Cisco Voice Switch Services (VXSM) Configuration and Command Reference Guide for MGX Switches, Release 5.3

August 31, 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-10284-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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, 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, 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, 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. (0601R)

Cisco Voice Switch Services Configuration Guide for MGX Switches and Media Gateways, Release 5.3
Copyright © 2006, Cisco Systems, Inc.
All rights reserved.

CONTENTS

About This Guide xi

Guide Revision History xi

Objectives xii

Audience xii

Document Organization xii

Obtaining Documentation xiii

Cisco.com xiii

Documentation DVD xiii

Ordering Documentation xiii

Documentation Feedback xiv

Cisco Product Security Overview xiv

Reporting Security Problems in Cisco Products xiv

Obtaining Technical Assistance xv

Cisco Technical Support Website xv

Submitting a Service Request xv

Definitions of Service Request Severity xvi

Obtaining Additional Publications and Information xvi

CHAPTER 1 **Cisco Voice Switch Service Module Introduction** 1-1

CHAPTER 2 **Cisco Voice Switch Service Module Description** 2-1

Voice Switch Service Module Physical Description 2-1

VXSM Firmware Images 2-6

VXSM Card Applications 2-7

Switching Operation—VoIP 2-7

Switching Features 2-8

Virtual Media Gateways 2-10

Support for H.248 Congestion and Overload 2-12

Backhauling Signaling Channels 2-12

VoIP Security Features 2-16

Communications Assistance for Law Enforcement Act Support 2-18

E911 Emergency Services Support 2-19

Announcements Feature 2-20

Voice Quality Monitoring Feature **2-21**
Busy Line Verification and Operator Interruption **2-24**
AAL2 Trunking Operation—Nonswitching **2-24**
Trunking Features—Nonswitching **2-25**
TDM Network Side **2-25**
Packet Network Side—Trunking **2-25**
Multiprotocol Service Module Interoperability **2-26**
Redundancy Support **2-27**
OC-3 Systems **2-27**
48 T1/E1 and 6 T3 Systems **2-31**
Processing Fax and Modem Traffic **2-33**
Fax/Modem/TTY Passthrough **2-33**
T.38 Fax Relay **2-35**
T.38 Fax Relay Statistics **2-36**
Network Bypass Feature **2-36**
Jitter Compensation **2-37**
Alarms and Statistics **2-38**
LED Indicator Alarms **2-38**
Software Alarms **2-39**
Statistics **2-39**

CHAPTER 3 **Configuring VoIP Switching Applications** **3-1**
Quick Start Procedure **3-1**
Configuring the PXM-45 Card **3-5**
Configuring AXSM or RPM-XF **3-7**
AXSM Card Configuration **3-7**
Configuring RPM-XF Cards **3-8**
Configuring VXSM Cards **3-10**
Configuring the TDM Interface **3-11**
Configuring MGC Interfaces for Call Control **3-21**
Gateways Using H.248 MGC Protocol **3-21**
Gateways Using XGCP MGC Protocol **3-30**
Configuring MGC Redundancy **3-34**
Configuring Backhaul **3-35**
Configuring the MGC Link **3-36**
Configuring the TDM Network Link **3-39**
Configuring E911 Emergency Services **3-43**
Configuring Bearer and Signaling Security Features **3-50**

Configuring More Features **3-57**

CHAPTER 4 **Configuring Switches for AAL2 Trunking Applications 4-1**

Multipurpose Service Module Alternative **4-1**

Quick Start Procedure **4-2**

Configuring the PXM-45 Card **4-3**

AXSM Card Configuration **4-4**

VXSM Card Configuration **4-5**

Create VXSM Resource Partition **4-5**

Configuring the TDM Interface **4-6**

Creating VXSM Trunks **4-12**

Configuring AAL2 Trunks **4-16**

Configuring HDLC Signaling AAL5 Trunks for Nx64 Format **4-18**

Configuring More Features **4-20**

CHAPTER 5 **Configuring VXSM Features 5-1**

Configuring T1/E1 and T3 Lines **5-1**

Configuring SONET Lines and Paths **5-1**

Configuring Clocking **5-5**

Connection Admission Control **5-7**

Configuring Redundancy **5-7**

Configuring PRI Backhaul **5-10**

Configuring Announcements **5-14**

Configuring Network Bypass **5-16**

Configuring Differentiated Services **5-17**

Configuring Fax and Modem Services **5-18**

Configuring the Voice Quality Monitoring Feature **5-30**

Configuring the Online Diagnostic Feature **5-45**

Configuring for Jitter Compensation **5-46**

DSP Resources under Mixed Codec Conditions **5-48**

CHAPTER 6 **VXSM as a Signaling Gateway 6-1**

Signaling Gateway Description **6-1**

Configuring a Signaling Gateway **6-4**

CHAPTER 7 **Loading and Upgrading VXSM Code Images 7-1**

Initial Considerations **7-1**

Loading a VXSM Image for the First Time **7-2**

Upgrade Procedure **7-3**

Interrupted Procedure Recovery **7-5**
Image Filenames and Revision Numbers **7-5**

CHAPTER 8 **VXSM Troubleshooting 8-1**
Collecting Troubleshooting Data **8-1**
Troubleshooting Procedures **8-2**
Obtaining Information on Current Voice Calls—H.248 **8-7**
Obtaining Information on Current Voice Calls—xGCP **8-11**
Bearer Tracing Feature **8-12**
Bearer Trace Operation **8-14**
Bearer Trace Types **8-15**
Bearer Trace CLI Requirements **8-18**
Considerations and Limitations **8-18**
Configuring the Bearer Tracing Feature **8-19**
Bearer Trace Configuration Examples **8-22**
Trace Files **8-24**
Troubleshooting a Bearer Trace Operation **8-25**
Bearer Trace Command Summary **8-26**
Troubleshooting Commands **8-27**

APPENDIX A **Media Gateway Clocking A-1**
Clocking Basics **A-1**
Clock Configuration **A-2**
Displaying Clock Configuration **A-4**
Clocking Guidelines **A-5**
Qualifying a Clock Source **A-5**
Switching to an Alternative Clock Source **A-6**

INDEX

FIGURES

Figure 1-1 MGX 8880 or MGX 8850 and VXSM as a Media Gateway **1-1**

Figure 2-1 Cisco MGX 8800 Series Chassis with VXSM Front Cards **2-3**

Figure 2-2 Cisco MGX 8800 Series Chassis with VXSM Back Cards **2-4**

Figure 2-3 Switching Operation Block Diagram **2-8**

Figure 2-4 VXSM with Four Virtual Media Gateways **2-11**

Figure 2-5 Virtual Gateway Redundancy—VXSM Card Level **2-12**

Figure 2-6 ISDN Backhaul Protocols Using RUDP **2-14**

Figure 2-7 ISDN Backhaul Protocols Using SCTP **2-15**

Figure 2-8 DPNSS Backback Protocols Using SCTP **2-16**

Figure 2-9 Signal and Bearer Security **2-17**

Figure 2-10 VXSM E911 Feature **2-19**

Figure 2-11 RTCP XR VoIP Metrics Method **2-22**

Figure 2-12 RTCP XR XNQ Metrics Method **2-22**

Figure 2-13 Trunking Block Diagram **2-24**

Figure 2-14 Media Gateway with MPSM Network Interface **2-27**

Figure 2-15 1:1 Front Card Redundancy **2-28**

Figure 2-16 1:1 Front and Back Card Redundancy **2-29**

Figure 2-17 1:1 Front and Back Card Redundancy after Switchover **2-30**

Figure 2-18 1:1 Front Card/Back Card Redundancy **2-32**

Figure 2-19 1:1 Front Card Redundancy **2-33**

Figure 2-20 PVC Mesh for Network Bypass—Example **2-37**

Figure 3-1 OC-3 Hierarchical Relationship **3-11**

Figure 3-2 SDH Hierarchical Relationships **3-13**

Figure 3-3 MGC, MGC Group, and VMG Arrangement—Example **3-22**

Figure 4-1 OC-3 Hierarchical Relationship **4-6**

Figure 4-2 SDH Hierarchical Relationships **4-8**

Figure 6-1 VXSM Signaling Gateway Protocol Stacks **6-1**

Figure 8-1 VoIP Call Leg Model **8-7**

Figure 8-2 TDM Hairpin Model **8-7**

Figure 8-3 xGCP Connection Model **8-11**

Figure 8-4 Bearer Tracing Major Elements **8-13**

Figure 8-5 VXSM Bearer Tracing High-Level Function **8-13**

Figure 8-6 Bearer Trace Probe Locations **8-13**

Figure A-1 PXM 45 UI S3 Back Card Connectors **A-2**

Table 2-1 Transmit Pin to Signal Assignments **2-4**
Table 2-2 Receive Pin to Signal Assignments **2-5**
Table 2-3 VXSM Supported Backhaul Protocols **2-12**
Table 2-4 TGCP Package MO Codes **2-19**
Table 3-1 Configuration for VoIP **3-2**
Table 3-2 Configure H.248 Commands **3-27**
Table 3-3 Configure H.248 Profile Commands **3-28**
Table 3-4 Configure Call Control Protocol Commands **3-31**
Table 3-5 Configure Call Control Profile Commands **3-33**
Table 3-6 RUDP Session Commands **3-37**
Table 3-7 LAPD Session Commands **3-41**
Table 4-1 Media Gateway Setup for a VoATM Trunking Application Commands **4-2**
Table 4-2 cnfpnportsig parameters **4-14**
Table 5-1 VTG/VT to DS1 Mapping **5-3**
Table 5-3 LAPD Session Commands **5-14**
Table 5-4 VQM Reference Ranges and Defaults **5-36**
Table 5-5 VQM Trigger Types **5-41**
Table 5-6 Voiceband Data Jitter Delay Parameters **5-47**
Table 7-1 Allowable VXSM Image Upgrades **7-1**
Table 8-1 Initial Troubleshooting Steps Using CLI Commands **8-1**
Table 8-4 PXM CLI Commands for Troubleshooting VXSM **8-12**
Table 8-5 VXSM CLI Commands for Troubleshooting VXSM **8-12**
Table 8-6 FTP Bandwidth and File Sizes **8-17**
Table 8-7 FTP Bandwidth and File Sizes **8-17**
Table 8-8 Trace Limitations **8-18**
Table 8-9 Generated Bearer Trace Filenames **8-21**
Table 8-10 Bearer Trace Troubleshooting **8-26**
Table 8-11 Troubleshooting VXSM—Commands **8-27**
Table A-1 Next Active Clock Source **A-6**
Table A-2 Clock Failure and Recovery: Primary Source Only **A-7**
Table A-3 Clock Failure/Recovery: Primary and Secondary—Revertive Enabled **A-8**

Table A-4 Clock Failure/Recovery: Primary and Secondary—Revertive Disabled **A-10**

About This Guide

This guide provides information about the features and functions of the Cisco Voice Switch Service Module (VXSM) Release 5.3.

Guide Revision History

This guide provides configuration procedures for Cisco VXSM features.

VXSM Release	Part Number	Publication Date
5.2	OL-7142-01	September 30, 2005
5.2	OL-7142-02	January 24, 2006
5.3	OL-10284-01	May 5, 2006
5.3.10	OL-10264-02	August 31, 2006

Description of Changes

- OL-7142-01 —This is the first revision of this document. However, this document is based upon the earlier VXSM document entitled *Cisco Voice Switch Services (VXSM) Configuration Guide and Command Reference for MGX Switches and Media Gateways, Release 5*.
- OL-7142-01 —This document includes all configuration procedures in the Release 5 document, plus new procedures for the features added to VXSM Release 5 to produce VXSM Release 5.2. Briefly, these added features are:
  - Packet cable compliance
  - E911 Emergency service
  - Bearer and IP security
  - T.38 Fax Relay
  - New VXSM-6T3 card set
  - Automatic detection of modem, fax, and TTY traffic with upspeed to pulse code modulation (PCM)
- OL-7142-02—Chapter 7, Troubleshooting, is updated to include the Bearer Trace feature.
- OL-10284-01 Rev. A0—This revision contains descriptions and configuration procedures for the following additional features

  - Ability of a VXSM card to perform as an SS7 Signaling Gateway in addition to its Media Gateway functions.
  - Voice Quality Monitoring
  - Ability of a VXSM card to act as a number of virtual media gateways
  - Call controlled T.38 Fax Relay
  - H.248 Congestion and Overload Handling
  - Expansion of the backhauling feature to include the following protocols

    DPNSS = Digital Private Network Signaling System
    DASS = Digital Access Signaling System
    SCTP = Streaming Control Transmission Protocol
    RUDP = Reliable UDP
    IUA = ISDN Q921-User Adaptation
    DUA = DPNSS/DASS User Adaptation Layer Protocol

- OL-10284-02—The procecure entitled "Setting Up XGCP Media Gateway Controllers and Media Gateway Controller Groups" in Chapter 3 has been improved.

Objectives

The *Cisco VXSM Configuration Guide* describes the use and configuration of VXSM in switching and nonswitching (trunking) applications.

Audience

The *Cisco VXSM Configuration Guide* is intended for experienced Cisco MGX users who are involved with the installation and configuration of the Cisco-based media gateway applications.

Document Organization

This installation guide has the following chapters:

- Chapter 1—Cisco Voice Switch Service Module Introduction
- Chapter 2—Cisco Voice Switch Service Module Description
- Chapter 3—Configuring VoIP Switching Applications
- Chapter 4—Configuring Switches for AAL2 Trunking Applications
- Chapter 5—Configuring VXSM Features
- Chapter 6—VXSM as an SS7 Signaling Gateway
- Chapter 7—Loading and Upgrading VXSM Code Images
- Chapter 8—VXSM Troubleshooting
- Appendix A—Media Gateway Clocking
- Index

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

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_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 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.

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

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

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
- Nonemergencies — 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

Cisco Voice Switch Service Module Introduction

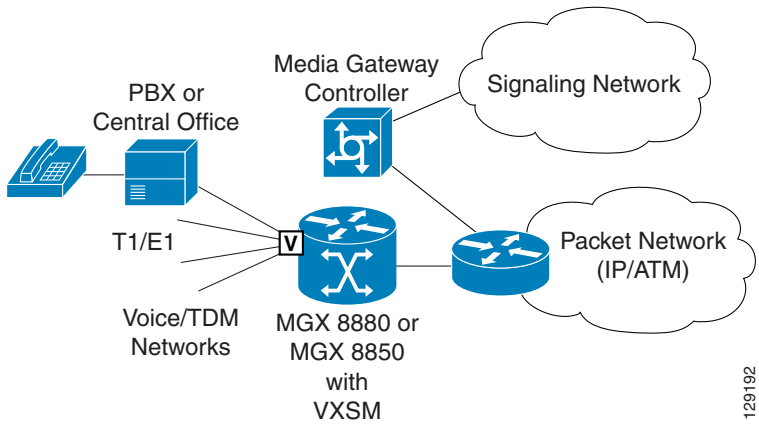
This chapter provides an overview of the Cisco Voice Switch Service Module (VXSM) Release 5.3 and the organization of this document.

VXSM is a front card/back card set that operates in either a Cisco MGX 8880 or a Cisco MGX 8850 /PXM-45 chassis. There are three such card sets, one supports 4 OC-3 ports, one supports 6 DS3 ports, and the other 48 T1 or E1 ports.

A Cisco MGX 8880 or Cisco MGX 8850 equipped with one or more VXSM card sets can function as a Media (Voice) Gateway in which voice traffic carried on conventional time-division multiplexed (TDM) voice circuits, including modem and fax data, is transported over IP or Asynchronous Transfer Mode (ATM) packet-switched networks (Figure 1-1). Each VXSM card can be configured as one or more virtual media gateways.

Further, a VXSM card can function as an Signaling System 7 (SS7) signaling gateway while also performing the functions of a media gateway.

Figure 1-1 MGX 8880 or MGX 8850 and VXSM as a Media Gateway



VXSM supports:

- Voice over IP (VoIP) switching applications
- Voice Trunking nonswitching applications
- Signaling gateway applications

VoIP Switching Applications

In VoIP switching applications, VXSM operates in conjunction with the PXM-45c card, along with either of the following:

- RPM-XF card—Used when the packet network side supports IP traffic (for example, an Ethernet network).
- AXSM card—Used when the packet network employs ATM to carry IP traffic.

  In these applications, voice traffic is switched between lines and trunks on the TDM and packet networks. The switching function is under the control of an external media gateway controller (often referred to as a call agent or softswitch). VoIP transmission of voice over a wide area packet network is often accomplished using an MPLS based network for routing the IP voice packets.

  In this application, a VXSM Card can be configured to backhaul Q.931 (using RUDP or SCTP) and DPNSS/DASS2 (using SCTP) layer 3 traffic to the call agent. VXSM card terminates layer 2 for both Q.931 and DPNSS/DASS2 protocols.

Trunking, Nonswitching Applications

In trunking, nonswitching applications, VXSM operates in conjunction with PXM-45c and AXSM cards. Voice traffic is routed onto pre-provisioned ATM trunks according to pre-configured parameters. A media gateway controller is not used in this application.

Using up-to-date semiconductor technology and a bank of digital signal processors, each VXSM card can support the following example capacities.

- A four OC-3 card set can support up to 8064 DS0s with 50 calls per second and an average call hold time of 161 seconds.
- A 48 T1 card set can support up to 1152 DS0s with 13 calls per second and an average call hold time of 90 seconds.
- A 48 E1 card set can support up to 1488 DS0s with 17 calls per second and an average call hold time of 90 seconds.

The Cisco MGX 8880 and Cisco MGX 8850 chassis provides 12 card slots that are shared between any installed VXSM, AXSM, and PRM cards.

Applications for a VXSM equipped Cisco MGX 8880 or MGX 8850 include:

- Wireless or wireline tandem switch replacement or offload.
- ATM trunks between distributed mobile switching centers (MSCs) in wireless networks.
- Wireless and wireline aggregation over ATM trunks.

Signaling Gateway Applications

A VXSM card can be configured to provide the functions of a signaling gateway between SS7 and IP networks. By this means, communication can be established between entities, such as Signaling End Points, on a SS7 network and Application Servers, such as a Media Gateway Controller, on an IP network.

Up to 16 DS0 lines on a VXSM card to be configured as SS7 signaling lines on which signaling messages to and from the SS7 network using the Message Transfer Part (MTP) 1, 2, and 3 layers of the SS7 protocol stack. Received messages have the MTP3 component extracted and relayed onto the IP network using the M3UA, SCTP, and IP protocol stack. The interworking at the MTP3 level is performed by a Nodal Interworking Function (NIF).

Using This Guide

This guide provides a general description of the features and functions of VXSM and describes how VXSM can be configured for switching and nonswitching applications. VXSM commands are explained in detail.

Use this document with the *Cisco Voice Switch Services (VXSM) Command Reference for MGX Switches and Media Gateways, Release 5.3*.

In addition to the VXSM card, the configuration sections of this guide cover other components such as PXM-45c, AXSM, and RPM-XF cards in some detail. For a more complete description of these components, how to configure them, and how to use their commands, refer to:

- *Cisco MGX 8850 Multiservice Switch Overview, Release 1.1.3*
- *Cisco MGX 8850 (PXM45/PXM1E), Cisco MGX 8950, and Cisco MGX 8830 Command Reference, Release 5*.2
- *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4*

In addition to the command line interface, you can perform many management and configuration tasks using the Cisco Media Gateway Manager (MGM) and Cisco WAN Manager (CWM). For details, refer to *Cisco Wide Area Network Manager User's Guide, Release 15*. and the *User Guide for Media Gateway Manager, Release 5*.

For the latest information on any of these products, refer also to the appropriate release notes.

Cisco Voice Switch Service Module Description

This chapter describes:

- The features and functions of the Cisco Voice Switch Service Module (VXSM) card set
- The VXSM application as a media gateway in a Cisco MGX 8880 or Cisco MGX 8850

Voice Switch Service Module Physical Description

VXSM consists of a full-height front card and a half-height back card or cards. The front card includes a large daughter card on which the digital signal processors (DSPs) are installed. The front card and daughter card are installed as one assembly and require only 1 slot. The complement of cards is as follows.

Voice Switch Service Module Front Cards

Three types of front card are supported (see Figure 2-1).

- MGX_VXSM_155—A full-height card used with OC-3 back card ports.
- MGX_VXSM_48_T1/E1—A full-height card used with T1/E1 back card ports.
- MGX_VXSM_6_T3/E3—A full-height card used with T3/E3 back card ports.

Note In Release 5.2, the MGX_VXSM_6_T3/E3 front card supports T3 only.

Voice Switch Service Module Back Cards

Four types of back card are supported (see Figure 2-2).

- VXSM_BC_4-155—A half-height card installed in the upper bay (for same card APS SONET line protection, a second back card can be installed in the lower bay). This card provides 4 OC-3 ports.
- VXSM_BC_3-T3—A half-height card. Two cards are used as a pair. One card is installed in the upper bay and one in the lower bay (providing a total interface for 6 T3/E3 lines).
- VXSM_BC_24-E1/T1—A half-height card. Two cards are used as a pair. One card is installed in the upper bay and one in the lower bay (providing a total interface for 48 T1/E1 lines).

Note Each 24 T1/E1 back card is equipped with two 50-pin connectors: one for transmit signals, and one for receive signals. Connect T1 and E1 lines through customer-supplied patch panels. Examples are:
Ortronics 24-port Patch Panel: Part Number 808-044990
Ortronics 48-port Patch Panel: Part Number 808-045368

- VXSM_BC_R—This is a redundant back card (no lines).

MGX Chassis

VXSM cards can be installed in either a Cisco MGX 8880 or a Cisco MGX 8850 chassis (Figure 2-1 and Figure 2-2). The differences between these chassis are as follows.

- Physically, the two chassis are card-compatible. The same control and service module cards can be installed in either chassis. However, the MGX 8880 supports only those cards that are used in media gateway applications. These are PXM-45c, VXSM, AXSM, and PRM-XF cards.
- The MGX 8880 chassis is smaller in height than the MGX 8850. Three MGX 8880 chassis can be installed in one 7-foot rack (as opposed to two for the MGX 8850).
- An RCON card is an integral part of the MGX 8880 chassis.
- The RCON card cannot be used in the MGX 8850 chassis.

Note The RCON card (Redundancy Connector) is a small assembly. It is installed in the top of the rear shelves spanning slots 1 to 6. An optional second RCON card can be installed in the bottom shelves and spans slots 7 to 12. Back cards connect to the RCON which in turn connects to the midplane of the MGX 8880 chassis. The RCON provides redundant paths for the back cards and its use is described in the Redundancy section of this chapter.

Figure 2-1 Cisco MGX 8800 Series Chassis with VXSM Front Cards

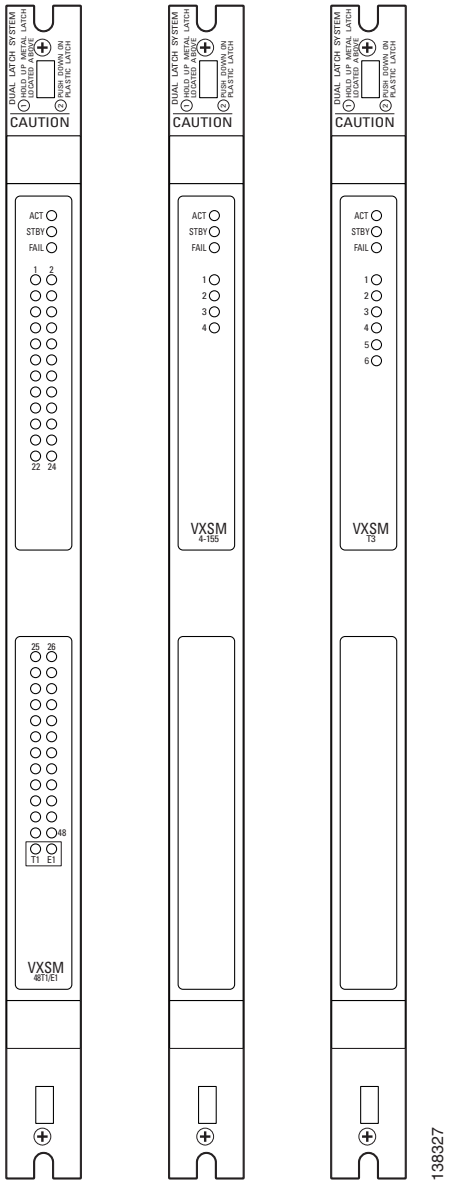
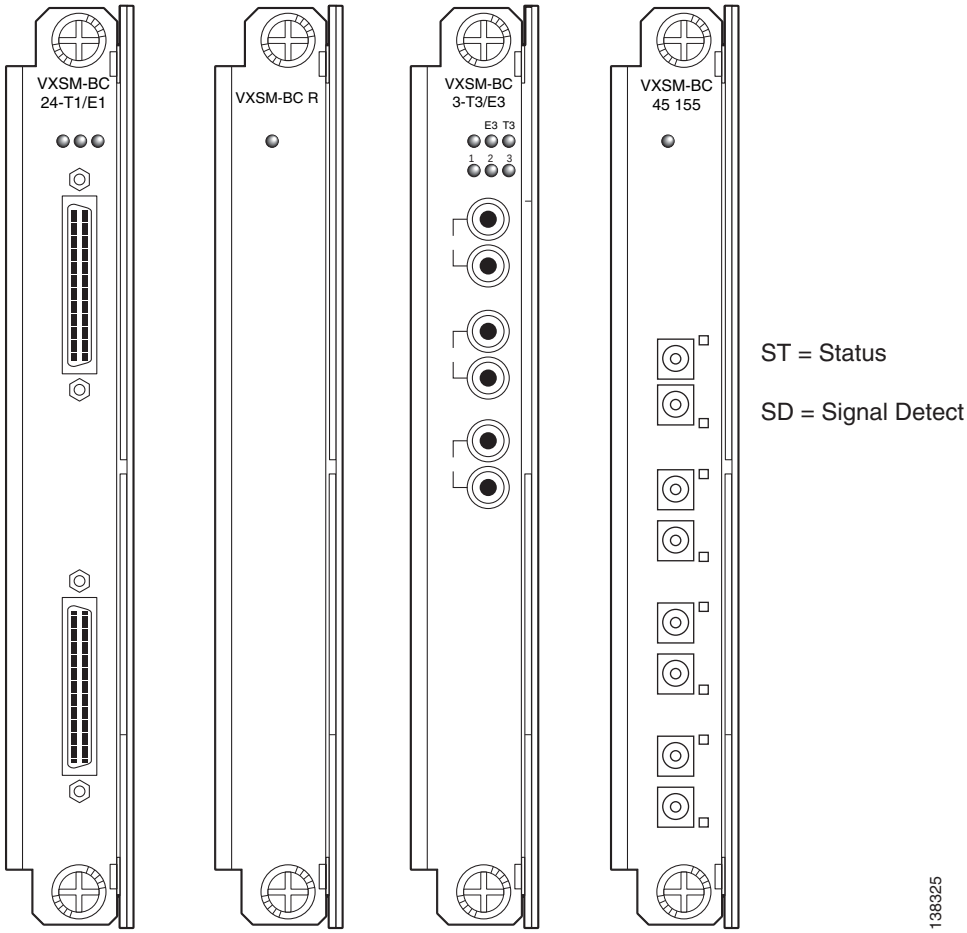


Figure 2-2 Cisco MGX 8800 Series Chassis with VXSM Back Cards



The pin assignments on the 24 T1/E1 back card appear in Table 2-1 and Table 2-2.

Table 2-1 Transmit Pin to Signal Assignments

Pin	Signal	Signal	Pin
1	TXRING1	TXTIP1	26
2	TXRING2	TXTIP2	27
3	TXRING3	TXTIP3	28
4	TXRING4	TXTIP4	29
5	TXRING5	TXTIP5	30
6	TXRING6	TXTIP6	31
7	TXRING7	TXTIP7	32
8	TXRING8	TXTIP8	33
9	TXRING9	TXTIP9	34
10	TXRING10	TXTIP10	35
11	TXRING11	TXTIP11	36

Table 2-1 Transmit Pin to Signal Assignments (continued)

Pin	Signal	Signal	Pin
12	TXRING12	TXTIP12	37
13	TXRING13	TXTIP13	38
14	TXRING14	TXTIP14	39
15	TXRING15	TXTIP15	40
16	TXRING16	TXTIP16	41
17	TXRING17	TXTIP17	42
18	TXRING18	TXTIP18	43
19	TXRING19	TXTIP19	44
20	TXRING20	TXTIP20	45
21	TXRING21	TXTIP21	46
22	TXRING22	TXTIP22	47
23	TXRING23	TXTIP23	48
24	TXRING24	TXTIP24	49
25	—	—	50

Table 2-2 Receive Pin to Signal Assignments

Pin	Signal	Signal	Pin
1	RXRING1	RXTIP1	26
2	RXRING2	RXTIP2	27
3	RXRING3	RXTIP3	28
4	RXRING4	RXTIP4	29
5	RXRING5	RXTIP5	30
6	RXRING6	RXTIP6	31
7	RXRING7	RXTIP7	32
8	RXRING8	RXTIP8	33
9	RXRING9	RXTIP9	34
10	RXRING10	RXTIP10	35
11	RXRING11	RXTIP11	36
12	RXRING12	RXTIP12	37
13	RXRING13	RXTIP13	38
14	RXRING14	RXTIP14	39
15	RXRING15	RXTIP15	40
16	RXRING16	RXTIP16	41
17	RXRING17	RXTIP17	42
18	RXRING18	RXTIP18	43

Table 2-2 Receive Pin to Signal Assignments (continued)

Pin	Signal	Signal	Pin
19	RXRING19	RXTIP19	44
20	RXRING20	RXTIP20	45
21	RXRING21	RXTIP21	46
22	RXRING22	RXTIP22	47
23	RXRING23	RXTIP23	48
24	RXRING24	RXTIP24	49
25	—	—	50

Card Slots

In an Cisco MGX 8880 chassis or an Cisco MGX 8850 chassis, VXSM cards can be installed in slots 1 through 6 and 9 through 14. Slots 7 and 8 are reserved for PXM-45c cards.

The 12 slots (1 through 6 and 9 through 14) are available for VXSM cards. However, all installed AXSM, MPSM, and RPM-XF cards also share these slots.

Slots 15 and 16 are reserved for SRM cards. These cards are typically not used in an Media Gateway application and the slots must remain empty.

When 1:1 redundant VXSM front cards are configured, the redundant pair must be installed in adjacent slots (for example, slots 1 and 2 or slots 9 and 10).

VXSM Firmware Images

VXSM is available with two versions of firmware: CALEA and non-CALEA:

- CALEA permits the user to configure support for the Communication Assisted Law Enforcement Act (CALEA)
- Non-CALEA does not permit the user to configure support for the CALEA

The user must specify either CALEA or non-CALEA at the time of order.

Both the CALEA and non-CALEA versions support MGCP and TGCP control protocols but only one at a time. Non-CALEA also supports H.248.

At the time of installation, user must:

- Choose between either the H.248, MGCP, or TGCP protocol
- Specify the codec template as either TGW/Wireline (default) or cable as appropriate

To execute these choices, use the **setrev** command on the PXM after the VXSM cards are installed. The user specifies the VXSM card (by slot number), the gateway controller protocol, and codec template. Then, the selected firmware and DSP images load onto the VXSM card. The nonselected protocol commands and codec functions are disabled.

VXSM Card Applications

Regardless of the firmware image that is installed, VXSM cards can be configured to perform the following three types of applications:

- Media gateway with VoIP switching
- Media gateway with nonswitching trunking
- Signaling gateway

One VXSM card can be configured to perform all three applications concurrently in which TDM lines are assigned to the specific applications.

The following sections describe the two types of media gateway applications. VXSM as a signaling gateway is described in Chapter 6.

Switching Operation—VoIP

VXSM support two methods for routing voice calls:

1. A switching method for VoIP applications
2. A nonswitching method for AAL2 trunking applications

The difference is how the internal and external connections are configured. VXSM can support AAL2 trunking, AAL5 trunking, and VoIP concurrently on the same VXSM card.

In switching operations, VXSM switches voice traffic between the conventional TDM voice network and the packet network under the control of a media gateway controller (MGC). VXSM and the MGC must have IP connectivity and use the H.248 (MEGACO) protocol, MGCP protocol, or the TGCP protocol to communicate.

Using one of these protocols, VXSM and the MGC communicate at each stage of the call setup and call tear down processes (on/off hook, dial tone, dialing, hang-up). At each stage, the MGC instructs VXSM how to perform the next step.

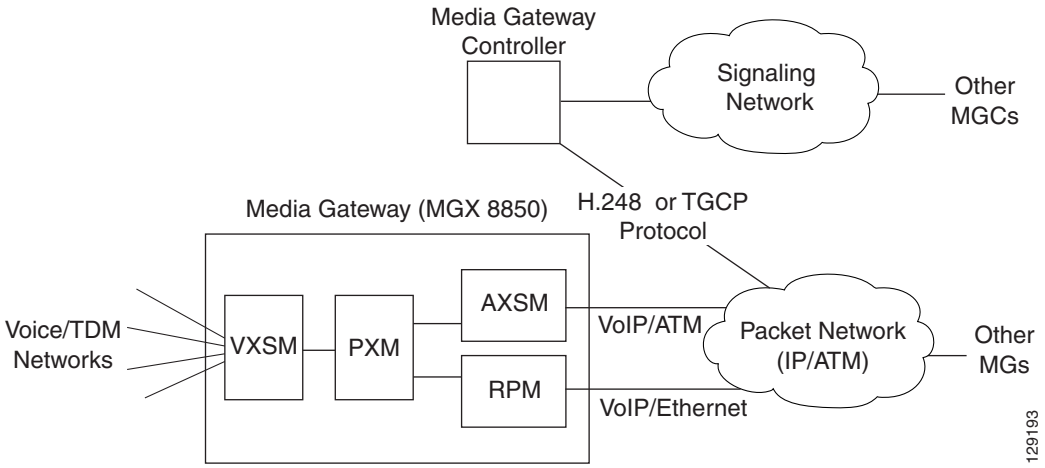
During call setup, a bearer circuit is set up across the packet network. This bearer circuit is used to establish IP connectivity for the voice traffic between the calling and called media gateways.

VXSM uses either an AXSM card or an RPM-XF card as its interface to the packet network:

- AXSM card—Communication between the gateways is voice over ATM communication using AAL5 PVCs.
- RPM-XF card—Communication between gateways is voice over IP communication using a gigabit Ethernet network.

Figure 2-3 shows the switching process.

Figure 2-3 Switching Operation Block Diagram



Switching Features

Switching operation supports the following features.

Time-Division Multiplexing Network Side

Interfaces

4 OC-3/STM-1, 6 T3/E3, and channelized 48 T1/E1

Companding

Mu law and A-law conversion

Configurable mu law and A-law endpoints on network side

Echo Cancellation

Echo removal on PCM samples using proprietary algorithm 8, 16,24,32,64, or 128 ms tails

Tones

Detects V.25 (with and without phase reversal) and V.8 signals or V.21 preamble or CNG tone to discriminate between voice, fax, and data calls

Upspeed to PCM upon fax/modem detection

The DSP module is capable of detecting DTMF tones while processing voice signals and transporting them in or out of band. (RFC 2833 and I.366.2 compliant)

Support for SS7 continuity tone for 2 and 4 wire circuits

PRI Backhaul

In applications where ISDN D channel signaling line are connected to VXSM, the VXSM can be configured to extract the layer 3 (Q.931) packets and backhaul them to the media gateway controller (this feature is described in Backhauling Signaling Channels, page 2-12 . PRI backhaul supports RUDP (Reliable UDP) and SCTP (Stream Control Transport Protocol) as transport protocols.

Network Bypass

For calls that originate and terminate on lines on the same VXSM card or the same media gateway, VXSM can be configured so that the call is routed within the media gateway and does not use IP or packet network resources. This feature operates with H.248 protocol only.

Busy Line Verification and Operator Interrupt

A caller can request that an operator check a called station to ascertain whether or not it is busy. This feature permits the operator to interrupt an ongoing call and relay a message to the called party.

Packet Network Side

ATM

Real-time protocol (RTP)
AAL 5 PVCs for bearer circuits

Codecs

G.711, G.726-(16K, 24K, 32K, and 40K), G.729a, G.729a/b, and G.clear (clear channel).

Connection Admission Control

For connection admission control (CAC), VXSM maintains information on available/used bandwidth on bearer virtual circuits. For PVC calls, before a call is admitted, a bandwidth check (based on code, packetization period, VAD) is made against the available PVC bandwidth. The result determines if the call is accepted or rejected.

Packetization Period

The codec packetization period is configurable up to 80 ms.

The VDB codec packetization period is configurable from 10 ms to 30 ms in 10 ms increments.

Jitter

Removes arrival time jitter from the incoming packet stream. Jitter buffer can manage up to 135 ms.

Silence Suppression

Uses voice activity detection (VAD) on bearer circuits to detect silence and suppress the transmission of cells containing silence. VAD is applicable on codecs G.711, G.723.1, G.723.1 Annex A, G.726, G729a, G.729b, and G.729ab

Differentiated Services

VXSM provides support for the quality of service (QoS) Differentiated Service feature known as DiffServ. DiffServ 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).

VoIP Security

VXSM provides a set of security features for the protection of bearer and signaling traffic in switching VoIP applications using TGCP. In particular, these features are designed to meet PacketCable standards.

E911 Emergency Services

VXSM supports an emergency services feature in which 911 dialed emergency calls are automatically directed to an E911 tandem switch and then onto a public safety answering point (PSAP).

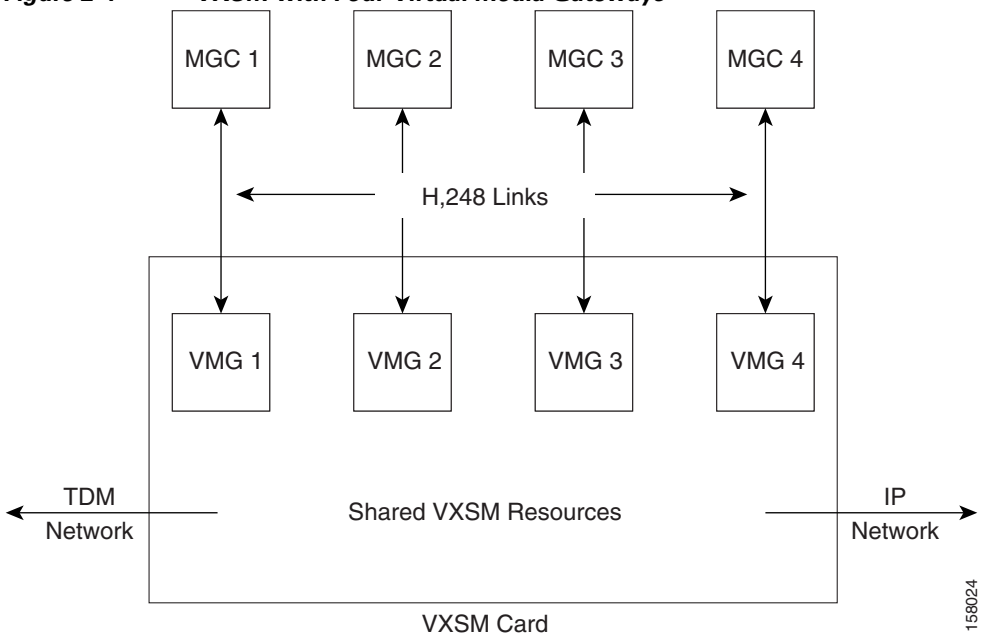
Virtual Media Gateways

For H.248 switched applications, a VXSM card can be partitioned into a number of Virtual Media Gateways (VMGs), where each VMG is a logical entity residing within a physical VXSM card. The VXSM Virtual Media Gateway feature permits a VXSM card to be partitioned into a maximum of 12 virtual gateways. This feature can be used in applications in which one media gateway controller (MGC) does not have the capacity to control one VXSM gateway. By partitioning the VXSM card into several VMGs, the control of VXSM's physical and ephemeral terminations can be distributed among several media gateway controllers .

Each of the virtual gateways appears to the MGC as a complete media gateway client. If one VMG goes out of service, the services provided by other VMGs are not affected. VXSM clears call-related data only for the VMG going out of service.

Figure 2-4 shows a VXSM card partitioned into four virtual gateways.

Figure 2-4 VXSM with Four Virtual Media Gateways



Virtual Gateways and H.248 Terminations

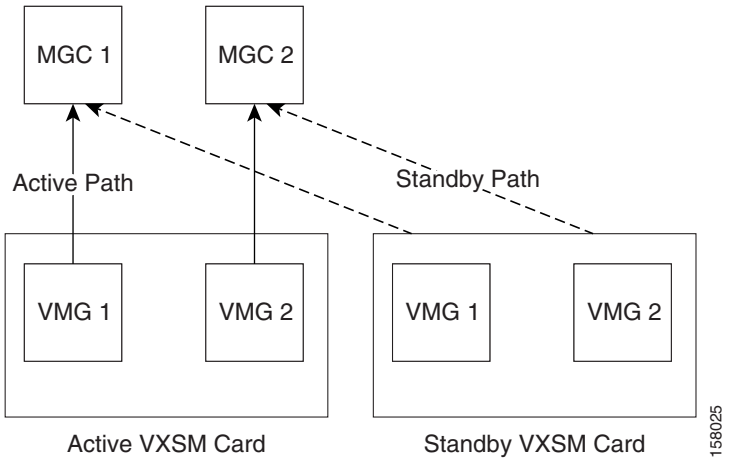
Physical terminations are statically partitioned among VMGs. Ephemeral terminations belong to the VMG whose controlling MGC creates them. One termination belongs to one, and only one, VMG. The finest granularity at which physical terminations are allocated to a VMG is at the T1/E1 level. Individual T1/E1 trunks may be added to a VMG, in any order.

The user must first create the required number of VMGs and then allocate terminations to their VMGs as they are provisioned. If VXSM is not to be partitioned, then the user creates only one VMG and associates all physical terminations with it.

Virtual Gateway Redundancy

VXSM supports redundancy at the physical gateway (VXSM card) level. One VXSM card acts as active for all of its VMGs, and another VXSM card acts as standby for all of its VMGs. In case of a failure, a physical gateway (VXSM card) level switchover is performed in which all VMGs on the active card are switched over to the standby card (Figure 2-5).

Figure 2-5 Virtual Gateway Redundancy—VXSM Card Level



Support for H.248 Congestion and Overload

VXSM supports the H.248.10 Congestion Control Package, and the H.248.11, Overload Control Package.

The H.248.10 MG Congestion Control Package is used to exchange congestion information between the MG and the MGC. VXSM reports congestion events to the MGC if congestion control has been enabled and MG detects a congestion event.

The H.248.11 MG Overload Control feature protects VXSM from processing overload that prevents the timely execution of H.248.1 transactions. MG Overload happens when the utilization of resources crosses a threshold and MG is close to being unable to respond to MGC transactions in a sufficiently timely manner to avoid the calling customer abandoning the call in setup.

When the H.248 overload feature is enabled, VXSM monitors and detects gateway overload condition. Upon detection of an overload condition, VXSM sends a Notify to the MGC when it receives an ADD command, in this way the MGC can adjust the calling rate to bring MG out of overloaded condition.

Backhauling Signaling Channels

For applications in which the signaling lines or channels are connected directly to VXSM, VXSM can be configured to relay the signaling messages to the Media Gateway Controller (MGC) for call control processing. This *backhauling* relay function consists of extracting the level 3 signaling message from the level 2 transport protocol, encapsulating it into the IP protocol stack, and relaying it onto the MGC.

To meet the requirements of various service provider networks, VXSM support a number of TDM network-side and the IP network-side protocol stacks for this purpose. VXSM supported backhaul protocols are shown in Table 2-3.

Table 2-3 VXSM Supported Backhaul Protocols

TDM Network Side	IP Network Side
ISDN D-channel (Q.931, Q.921	UDP, RUDP

Table 2-3 VXSM Supported Backhaul Protocols

TDM Network Side	IP Network Side
ISDN D-channel (Q.931, Q.921)	SCTP, IUA
DPNSS or DASS 2 trunks	SCTP, DUA

- DPNSS—Digital Private Network Signaling System
- DASS2—Digital Access Signaling System Version 2
- SCTP—Streaming Control Transmission Protocol
- RUDP—Reliable UDP
- IUA—ISDN Q921-User Adaptation
- DUA—DPNSS/DASS User Adaptation Layer Protocol

ISDN/RUDP Backhauling

When D channels of ISDN PRI lines are connected to the TDM side of the VXSM card, VXSM can be configured to extract the Layer 3 (Q.931) frames from the ISDN stream and pass (backhaul) them to the gateway controller. Likewise, Q.931 frames received from the gateway controller can be encapsulated into Layer 2 (LAPD Q.921) frames and transmitted over the appropriate D channel ISDN lines on the TDM side. This function is known as PRI Backhaul. Both T1 and E1 lines are supported.

The backhaul feature can be configured as either:

- Non-fault tolerant—Using one gateway controller, or
- Fault-tolerant—Using two gateway controllers; one active and one backup

Both configurations can be combined with 1:1 VXSM card redundancy. Automatic switchover is supported for both gateway controller and VXSM card failures.

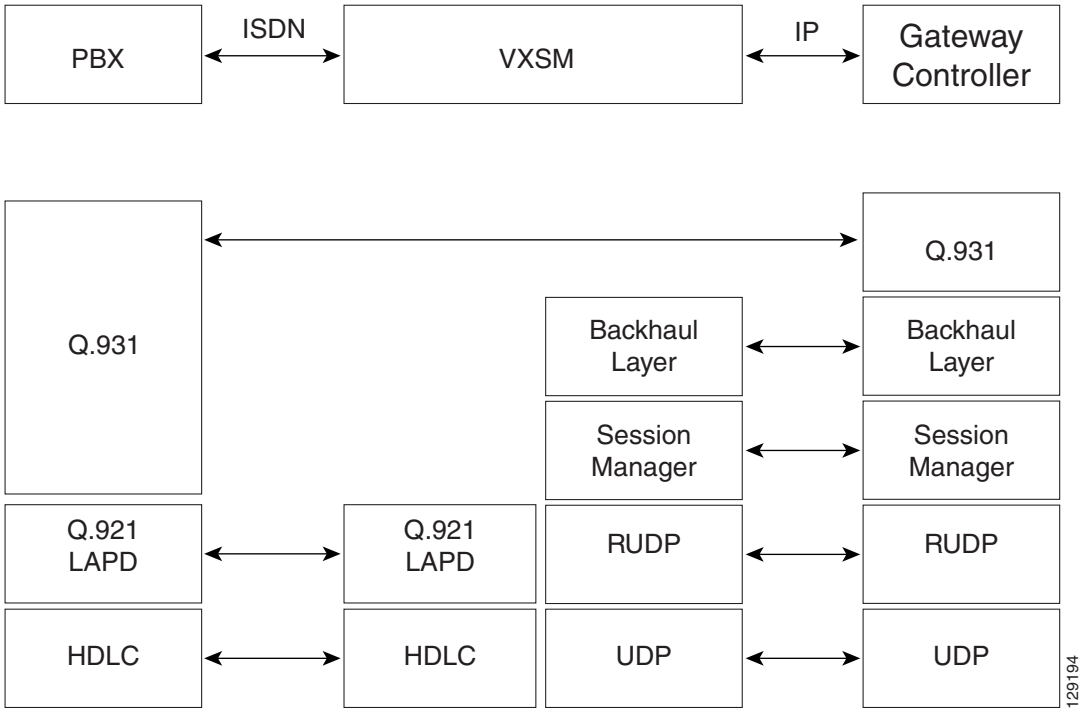
On the TDM side, ISDN PRI standards protocols are used. The Q.931 signaling frames are encapsulated in Q.921 (LAPD) frames and transported as High Level Data Link Control (HDLC) frames. The HDLC and Q.921 layers are terminated at the VXSM.

For communication between VXSM and the media gateway controller the protocol stack is based upon the Cisco proprietary session manager 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.

Figure 2-6 shows the protocol stacks for ISDN/ RUDP.

Figure 2-6 ISDN Backhaul Protocols Using RUDP



ISDN/SCTP Backhauling

When D channels of ISDN PRI lines are connected to the TDM side of the VXSM card, VXSM can be configured to extract the layer three (Q.931) frames from the ISDN stream and pass (backhaul) them to the gateway controller. Likewise, Q.931 frames received from the gateway controller can be encapsulated into Layer 2 (LAPD Q.921) frames and transmitted over the appropriate D channel ISDN lines on the TDM side. This function is known as PRI backhaul. E1 lines only are supported.

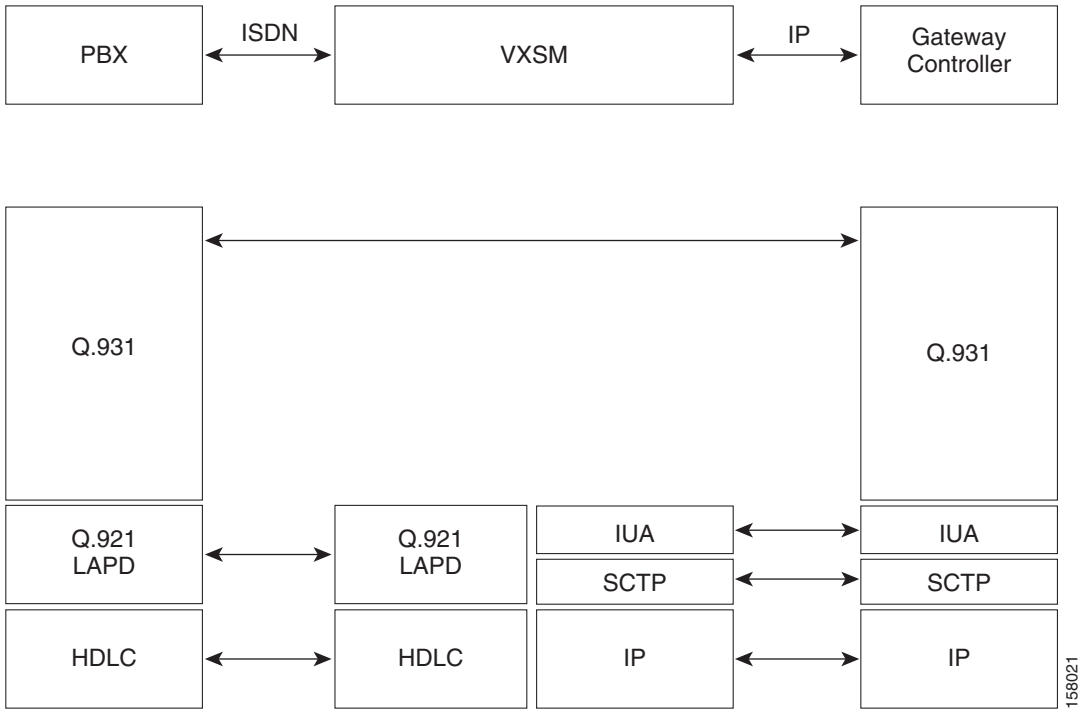
On the TDM side, ISDN PRI standards protocols are used. The Q.931 signaling frames are encapsulated in Q.921 (LAPD) frames and transported as High Level Data Link Control (HDLC) frames. The HDLC and Q.921 layers are terminated at the VXSM.

For communication between VXSM and the media gateway controller, the protocol stack is based upon the Streaming Control Transmission Protocol (SCTP) and the ISDN Q921-User Adaptation (IUA) layer.

SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers network-level fault tolerance through supporting of multihoming at either or both ends of an association, congestion avoidance, and resistance to flooding.

Figure 2-7 shows the protocol stacks for ISDN/ SCTP.

Figure 2-7 ISDN Backhaul Protocols Using SCTP



DPNSS/SCTP Backhauling

For applications in which DPNSS trunks are connected to the TDM side of the VXSM card, VXSM can be configured to extract the DPNSS layer 3 frames from the data stream and pass (backhaul) them to the gateway controller. Likewise, DPNSS layer 3 frames received from the gateway controller can be encapsulated into DPNSS layer 2 frames and transmitted over the appropriate trunks on the TDM side.

Note Both DPNSS and DASS 2 trunks are supported. For the purposes of this description, the term DPNSS refers to both DPNSS and DASS 2 unless otherwise noted.

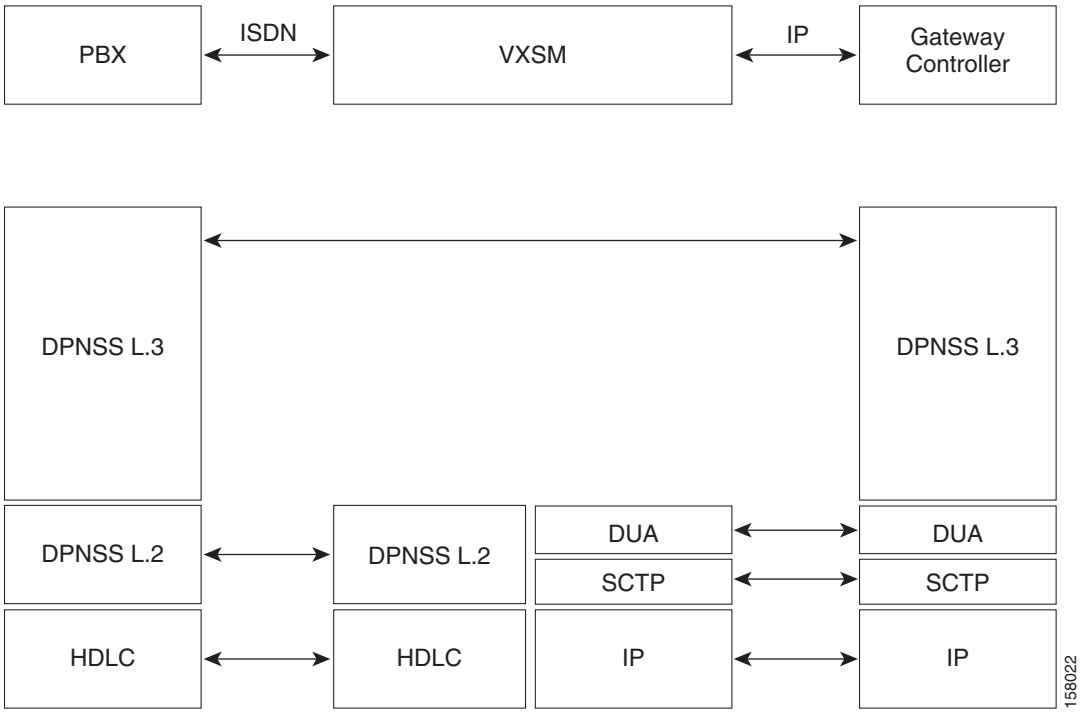
DPNSS trunks are supported on E1 lines only.

For communication between VXSM and the media gateway controller the protocol stack is based upon the Streaming Control Transmission Protocol (SCTP) and the DPNSS/DASS User Adaptation Layer (DUA).

SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers network-level fault tolerance through supporting of multihoming at either or both ends of an association, congestion avoidance, and resistance to flooding.

Figure 2-8 shows the protocol stacks for DPNSS/ SCTP.

Figure 2-8 DPNSS Backback Protocols Using SCTP



Note For backahuling using SCTP, VXSM supports multihoming (multiple IP addresses) associated with the MG (local) and the MGC (remote). Two IP addresses at the MGC end and two IP addresses at the MG end are supported.

VoIP Security Features

VXSM provides a set of security features for the protection of bearer and signaling traffic in switching VoIP applications using TGCP. In particular, these features are designed to meet PacketCable standards.

RTP and RTCP bearer streams can be protected across an IP network through the use of encryption and authentication algorithms that are applied to the bearer payloads.

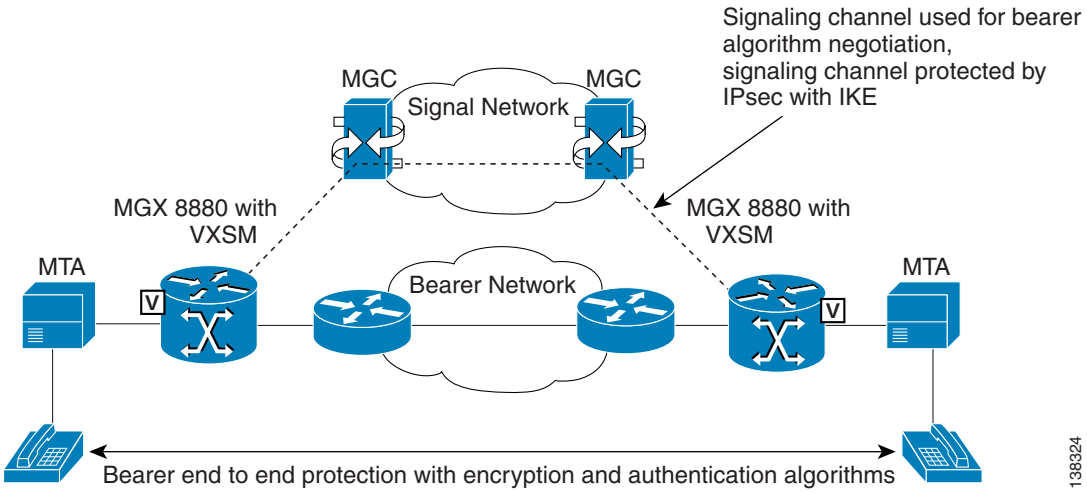
The specific security algorithms that are used for any particular call are negotiated during call setup (using TGCP) between the two ends (for example, media terminal adapters) with the media gateway controller acting as a mediator in the process. The signaling links between the media gateways and the media gateway controllers are protected using Internet Security (IPSec and IKE) protocols.

When the algorithms agree, they are used to secure the voice payload.

Note Signal and bearer security are supported on both the CABLE and TGW firmware images. Signal security (IPSec) operates with either H.248 or xGCP. Bearer security operates with xGCP only.

Figure 2-9 shows the protection in effect for a PacketCable call between two Media Terminal Adapters (MTA).

Figure 2-9 Signal and Bearer Security



Note For calls in which one end of the bearer path partially uses public switched telephone system (PSTN), the security extends only to the gateway entity that interfaces to the PSTN.

Signal Security

VXSM supports protection of the signaling channel through the use of IP Security (IPSec) and Internet Key Exchange (IKE) protocols.

The signaling channel (TGCP) is used to negotiate cipher suites (algorithms) that are to be used on the bearer channel. However, the signaling channel must be capable of protection.

1. IKE is used to exchange IPSec Security Associations (SA) and this function is performed in two phases. In the first phase the two IKE peers are authenticated.
2. The IPSec SAs are negotiated with keys derived from the first phase.
3. When the IPSec SAs are authenticated, the signaling stream can be encrypted. IPSec supports two protocols:
   - Authentication Header (AH)
   - IP Encapsulating Security Payload (ESP)

   IPSec supports two modes:
   - Transport mode—Protects the entire transport payload
   - Tunnel mode—Protects the IP packet by encapsulating it inside another IP packet

The following IPSec features are supported by VXSM:

- Protocols
- ESP
- Modes
- Transport and tunnel

Bearer Security

Each VXSM is configured by the user (CLI) to include a table of permissible cipher suites where a cipher suite is a record containing one encryption algorithm, one authentication algorithm and a preference.

When a call is originated, setting up security for the call is accomplished in two phases:

1. First, using TGCP, the MTAs and media gateways at each end of the call exchange their lists of permissible cipher suites.
2. An acceptable cipher suite is then negotiated. This negotiation is carried out for both RTP and RTCP bearer streams. The following algorithms are supported in VXSM:

   RTP encryption:

   - RTP_AES
   - RTP_ENCR_NULL

   RTP authentication:

   - RTP-MMH2
   - RTP_MMH4
   - AUTH_NULL

   RTCP encryption:

   - AES_CBC
   - RTCP_ENCR_NULL

   RTCP authentication:

   - HMAC-SHA1-96
   - RTCP_AUTH_NULL

Note If the negotiation results is one or both of the NULL algorithms, this effectively turns off the security function for each NULL algorithm.

3. When the cipher suites are agreed upon, the bearer path is set up and the call can be established. The negotiated algorithms are applied to the RTP and RTCP streams respectively.

   Encryption algorithms:

   - ESP_3DES
   - ESP_NULL

   Authentication algorithms:

   - HMAC_MD5-96
   - HMAC_SHA-1-96

Communications Assistance for Law Enforcement Act Support

VXSM provides support for Communications Assistance for Law Enforcement Act (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 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.

Note The VXSM firmware image is available in two versions: a CALEA version and a non-CALEA version. The version must be specified at the time of order.

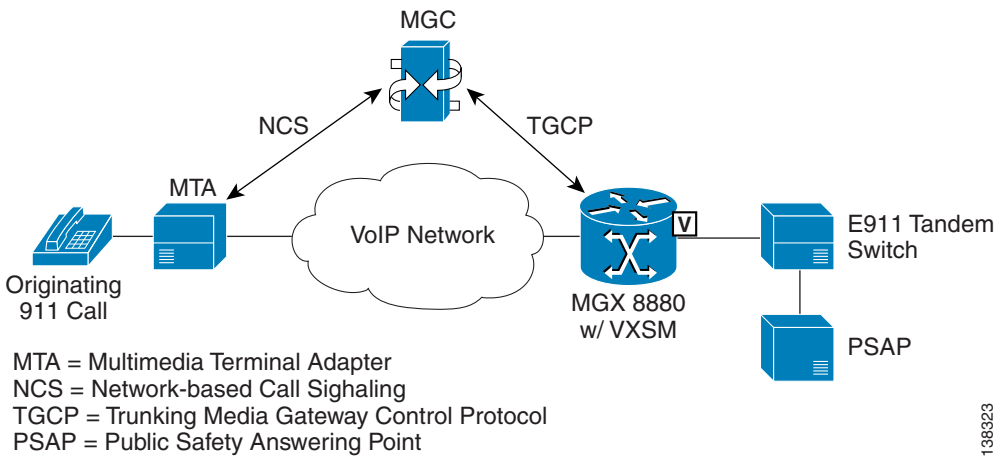
E911 Emergency Services Support

VXSM supports an emergency services feature in which 911 dialed emergency calls are automatically directed to an E911 tandem switch and then onto a Public Safety Answering Point (PSAP).

Enhanced 911 (E911) is a Federal Communications Commission (FCC) initiative to increase public safety by the deployment of a nationwide, seamless communications system for emergency services that includes the provision of location information for wireless 911 calls.

The E911 feature on VXSM primarily supports Packet Cable applications, and is implemented using the packet cable specified MO (MF OSS) package in the TGCP protocol. The E911feature is shown in Figure 2-10.

Figure 2-10 VXSM E911 Feature



1. When a 911 call is initiated by the caller, the MGC identifies the appropriate E911 Tandem switch and informs VXSM to set up a call to that switch. The communication between the MGC and VXSM is through TGCP (although MGCP is supported also) using the MF FGD operator services package (MO) protocol. The supported codes within this package are shown in Table 2-4.

Table 2-4 TGCP Package MO Codes

Code	Description	Event	Signal
Ans	Call answer	P	—
Oc	Operation complete	N	—

Table 2-4 TGCP Package MO Codes (continued)

Of	Operation failure	N	—
Sup<addr, id>	Setup	—	Timeout
OrBk	Operator ringback	N	—
Sus	Suspend call	—	Brief
Res	Resume call	—	Brief
Rel	Release call	N	Brief
Rlc	Release complete	N	—
Swk	Wink start	N	—

2. After the call is made, conversation between the caller and the PSAP operator takes place.
3. The call is then terminated.
4. The PSAP initiates a call back to establish the validity of the caller. When validated, the 911 process is complete.

The E911 feature is supported on all versions of VXSM cards, but only T1 circuits are supported.

If redundant hardware has been configured, active E911 calls are preserved during a switchover in the event of a failure.

Announcements Feature

In switching applications (H.248 media gateway control protocol only), VXSM includes an announcement feature in which pre-recorded announcements can be played on a voice channel under the control of the MGC. A set of announcement files is maintained on an announcement server:

1. When an announcement is to play, the MGC uses the announcement package in the H.248 protocol to instruct VXSM to play the announcement.

   If the announcement has:

   - Been previously cached by VXSM, the announcement is played out of cache.
   - Not been previously cached by VXSM, VXSM uses TFTP to download the file from the announcement server, cache it, and play the announcement.

   Announcement files:

   - Must be in PCM format and no more than 30 second in play-out duration (this represents a file size of approximately 240 kilobytes). When a file is downloaded from the announcement server, it is stored in a cache in the VXSM which can hold up to 136 announcements. When cache becomes full, any request for an announcement that is not in cache results in the requested file being downloaded and replacing an existing cached file on a “least recently used” basis.
   - Can be configured as permanent, in which case they remain in cache and are never replaced.
2. In addition to the announcement files and the VXSM cache, the user maintains a list of announcement files on VXSM. This list is in the form of a table, indexed by the announcement number, and it contains the name of the file (with directory path, if applicable) in the TFTP server. It also contains (associated with each file) the default values of the optional parameters that the MGC provides with the “play announcement” signal. The mapping of announcement index number to announcement filename must be maintained both in the VXSM and MGC. The MGC specifies the file index in the signal to indicate which announcement it wants to play.

3. The MGC can specify that the announcement be played in the direction of the caller, or the called party, or both.

   In the current implementation, no redundancy for announcement is supported.

Note Only the active VXSM card can communicate to the announcement server. All announcements are downloaded on the active card only.

4. When a switchover occurs, the newly active card downloads the permanent announcements from the announcement server as soon as it goes active. The dynamic announcements are downloaded on the newly active card on demand.
5. If a card switches over while playing an announcement, the announcement is not automatically continued on the newly active card. The MGC must explicitly restart the announcement on the newly active card.

Voice Quality Monitoring Feature

When configured for VoIP switched applications using the H.248 call control protocol, the VXSM Voice Quality Monitoring (VQM) feature provides the ability to monitor, collect, and report voice quality metrics to the Media Gateway Controller and/or the remote Media Gateway. Together, the values of the collected metrics represent a measure of the quality of voice calls transmitted across the network. Service providers can use these metrics to observe and diagnose quality problems and to provide a measure for Service Level Agreements between the provider and its customers.

VXSM supports two methods of performing VQM functions:

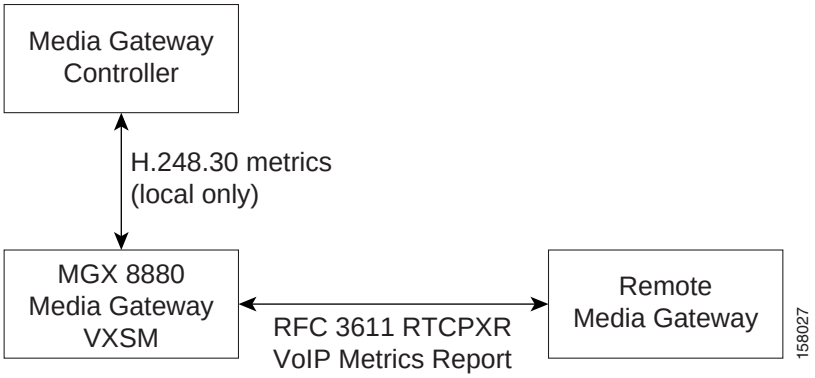
1. RFC3611 VQM—Based upon RFC 3611 metrics
2. XNQ VQM—Based upon Extended Network Quality (XNQ) metrics

VXSM can support either of these methods but not both simultaneously. These methods differ in the choice of protocols used to communicate with the remote MG and the MGC and the voice quality metrics that are reported.

RFC 3611 Voice Quality Monitoring

RFC 3611 voice quality monitoring (VQM) uses RTP control protocol extended reports (RTCP XR) VoIP metrics (Figure 2-11).

Figure 2-11 RTCP XR VoIP Metrics Method

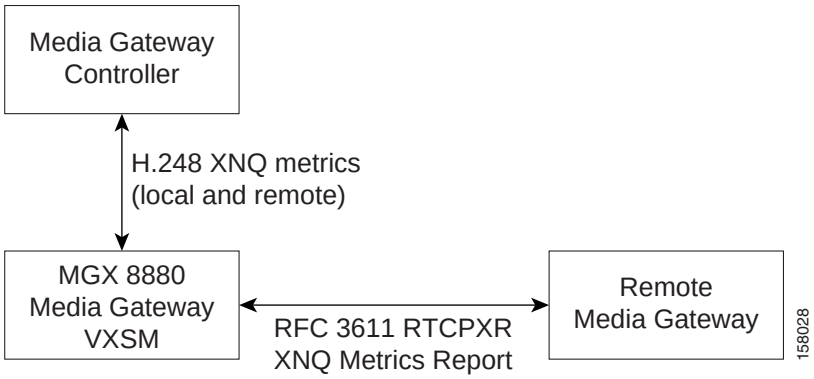


RTCP XR VoIP metrics use the RTP control protocol extended reports (RTCP XR) provision in RFC 3611 to append VoIP metrics reports to the normal RTCP packets. This method also involves the Media Gateway Controller (MGC) through the use of H.248 and the H.248.30 RTCP extended performance metrics packages. The two packages are the RTCP XR base package (rtcpxr) and the RTCP XR burst metrics package (xrbm). The voice metrics defined in these packages are consistent with those defined in the RTCP XR VoIP metrics report block. The media gateway controller is able to set up properties and retrieve statistics (voice-metrics) defined in these packages.

RTCP XR Extended Network Quality Metrics

XNQ voice quality monitoring (VQM) uses RTCP XR extended network quality (XNQ) metrics (Figure 2-12).

Figure 2-12 RTCP XR XNQ Metrics Method



This method uses the RTP control protocol extended reports (RTCP XR) provision in RFC 3611 to append XNQ metrics reports to the normal RTCP packets. This method also involves the media gateway controller (MGC) through the use of the H.248 RTCP extended network quality metrics package. The voice metrics defined in these two packages are consistent with those defined in the RTCP XR XNQ metrics report block. The MGC can set up properties and retrieve statistics (voice-metrics) defined in these packages.

Voice Quality History Reports

VXSM can maintain a history table to generate voice quality history reports to help service providers track their service level agreements. The history report tracks the minimum, maximum and average of the various voice metrics. History table entries are updated only if VQM feature is enabled.

The statistic upload function is used to retrieve the history table periodically. After the voice metric history table is retrieved, the history table is reset.

Voice Quality Alerts

VXSM has the capability of generating voice quality alerts that are reported to the Service Provider in real-time. Voice quality alerts are determined by comparing the measured value of a trigger voice metric to a threshold value. For each voice metric, the threshold values are determined by the following two parameters.

- Voice metric reference value
- Quality alert threshold percentage

When the measured value of a voice metric is worse than the reference value by more than the threshold percentage a voice quality alert is triggered.

VXSM supports one trigger per call at any one time. There is no support for multiple simultaneous triggers in a single call. Each T1/E1 interface can be configured with a different trigger metric. In addition, a default trigger metric can be configured for the whole gateway or a virtual gateway. If neither the gateway nor T1/E1 interface level trigger metrics are configured, no quality alert events or traps are generated and the MGC cannot enable quality alert events.

Voice Quality alert events are reported to the MGC and are based on the H.248 network package. This package allows for multiple thresholds, however, VXSM supports only one. Upon receipt of multiple thresholds, only the last threshold takes effect. If the MGC specifies the alert threshold percentage parameter when enabling a quality alert event, the MGC specified value overrides the threshold value provisioned on VXSM. If MGC does not enable a quality alert event, no alert event notification is sent to the MGC even though a quality alert trap may be generated to the SNMP Manager. After an alert notification is sent to the MGC, VXSM does not re-arm the quality alert event. Thus, a subsequent cross over of the alert threshold does not trigger another alert notification to the MGC.

SNMP voice quality alert traps are also supported. If the voice quality alert event is detected, VXSM can send SNMP quality alert traps to an SNMP Manager if the VQM trap is enabled.

Quality Alerts for Voice Band Data Calls

Upon detection of a modem tone (modem, fax, or TTY), upspeed takes place. Depending on the upspeed method, the Codec may be modified by the gateway or the Call Agent. Further, the jitter and a number of other parameters are reconfigured to better handle the VBD mode. After upspeed occurs, the call statistics are reset and the VBD and its associated thresholds trigger and thresholds are downloaded to the DSP.

The reason for resetting the statistics immediately after the upspeed is to avoid using the statistics collected during the voice-phase. VBD connections are usually more sensitive to frame-loss than voice connections. Consequently, the VBD trigger information might cause an instant quality alert alarm due to lost frames accumulated during the voice phase. These (old) statistics have no bearing on the quality of the VBD connection and should be discarded.

If traps/events are generated at a high rate, the VXSM performance may be affected. Thus, trap and event throttling may be required. The rate of trap and event-handling is configurable. Commands are provided to configure the number of trap/event to be processed in a specific time interval. The detected traps/events are placed into queues and processed at the rate configured in the system. Excess traps that cannot be buffered in the queue are lost.

Note Voice quality history reports and voice quality events are supported only if the VXSM RFC 3611 VQM feature is enabled.

Busy Line Verification and Operator Interruption

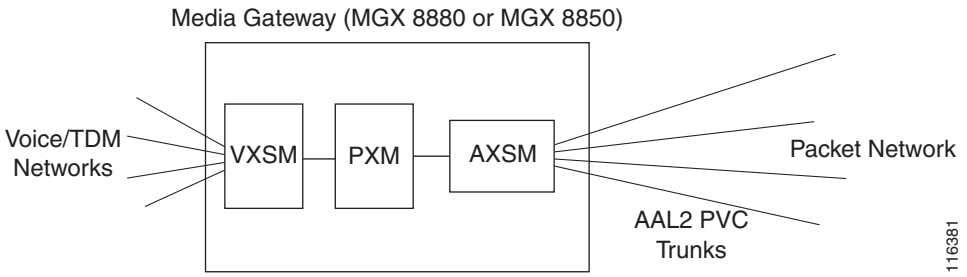
VXSM now supports Busy Line Verification and Operator Interruption (BLV/OI) through the MT package of the TGCP protocol under the control of a Call Agent. A caller can request that an operator check a called station to ascertain whether or not it is busy. This feature permits the operator to interrupt an ongoing call and relay a message to the called party.

AAL2 Trunking Operation—Nonswitching

VXSM support two methods for routing voice calls: a switching method for VoIP applications and a non-switching method for AAL2 trunking applications. The difference is how the internal and external connections are configured. A VXSM card can support only one or these methods at a time. However, the media gateway can support both methods by using different VXSM cards.

In a trunking operation, VXSM directs voice traffic between the conventional TDM voice network and one or more pre-provisioned AAL2 ATM PVC trunks on the packet network (Figure 2-13).

Figure 2-13 Trunking Block Diagram



As it name implies, this mode does not involve switching and does not involve a media gateway controller. Associations are made between the DS0 and DS1 circuits in the TDM network and AAL 2 CIDs in the ATM packet network. These associations determine which trunk a call uses.

Voice streams are identified by a Circuit Identifier (CID) and packed into AAL 2 cells. The mode supports subcell multiplexing in which partially filled cells can be filled with data from other CIDs thereby improving the bandwidth usage of the trunk.

In this mode, signaling is not terminated and is passed over the trunk. CCS (ISDN PRI) signaling is transported over HDLC/AAL5. SS7 uses AAL2 profile CUSTOM 200 (clear channel).

Upon detection of a fax or modem tone, this mode supports the upspeed feature.

Trunking Features—Nonswitching

Trunking operation supports the following features.

TDM Network Side

Interfaces

4 OC-3/STM-1 (channelized), 6 T3/E3, and 48 T1/E1

Companding

Mu law and A-law conversion

Configurable mu law and A-law endpoints on network side

Echo Cancellation

Echo removal on PCM samples using proprietary algorithm 8, 16, 24, 32, 64, or 128 ms tails.

Tones

Detects V.25 (with and without phase reversal) and V.8 signals or V.21 preamble or CNG tone to discriminate between voice, fax, and data calls.

Upspeed to PCM upon fax/modem detection. The upspeed codec is configurable.

The DSP module is capable of detecting DTMF tones while processing voice signals and transporting them. (RFC 2833 and I.366.2 compliant).

Packet Network Side—Trunking

Codecs

G.711 (mu-law and A-law), G.729a, G.729ab, and G.clear (clear channel).

Voice Activity Detection

Uses a voice activity detection (VAD) algorithm, provides updates for the remote end on the background noise level so that the comfort noise generator can sound natural.

AAL2 CPS Subsystem

ITU-T standard I.363.2 B-ISDN ATM Adaptation layer specification: Type 2 AAL, to multiplex/de-multiplex multiple low speed AAL2 connections over a single ATM VC.

Timer CU for subcell multiplexing timing

Sequence number protection checks for CPS-PDU

LI checks for each CPS-packet

Data transfers of CPS-Packets with CPS-INFO fields of up to 45 octets (no support for the 64 octet option)

CRC5 (HEC) generation/checking in the CPS-PH of the CPS-packet

OSF of the STF checking

Max_SDU_Deliver_Length checking (the length of the received CPS-Packet Payload exceeds the maximum length)

Odd parity checking for the STF octet of the CPS-PDU

CPS-PDU padding as needed.

Support up to 248 channels (CIDs) of AAL2 per ATM VC (8.255).

AAL2 SSCS—I.366.2

ITU-T standard I.366.2 "Service Specific Convergence Sublayer for the AAL type2."

- Audio service (voice, voice band data)
- Circuit mode data service (Annex J)
- Dialed digits service (Annex K)
- User State Control (Annex O)
- Frame mode data (I.366.1)
- Alarm handling

  VXSM supports the following standard based (I.366.2 annex P) ATM profiles: ITU 1,TU 2, ITU 3, ITU 7, ITU 8.

  In addition, the following Cisco custom profiles are supported: Custom 100, 101, 110, 200. Details on custom profiles appear in Chapter 5.

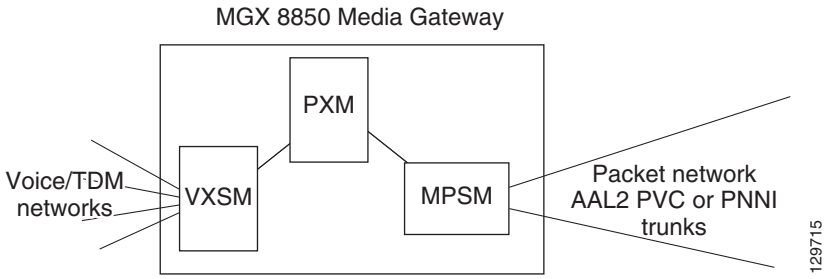
Note Fax demodulation/remodulation is not supported.

Multiprotocol Service Module Interoperability

For AAL2 trunking applications (MGX 8850 only), VXSM can now operate in conjunction with a Multiprotocol Service Module (MPSM) in which the MPSM provides the interface to the ATM network (Figure 2-14). In this way, the MPSM offers an alternative to the AXSM network interface. 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 **cnfclictx atm** command. After the context is set to ATM, provisioning is performed with the **upln**, **addport**, and **addcon** command sequence. For more details, refer to the MPSM user documentation.

Figure 2-14 Media Gateway with MPSM Network Interface



Redundancy Support

The Cisco MGX 8880 or Cisco MGX 8850 and the VXSM cards support a variety of redundancy schemes both at the card and line level. The details of each scheme depend upon whether the back cards support OC-3 or T1/E1 lines.

Note Some redundancy configurations require the use of the RCON card. Because the RCON card is not supported in MGX 8850 chassis, these configurations are not supported in the MGX 8850.

OC-3 Systems

OC-3 equipped systems support the following redundancy schemes.

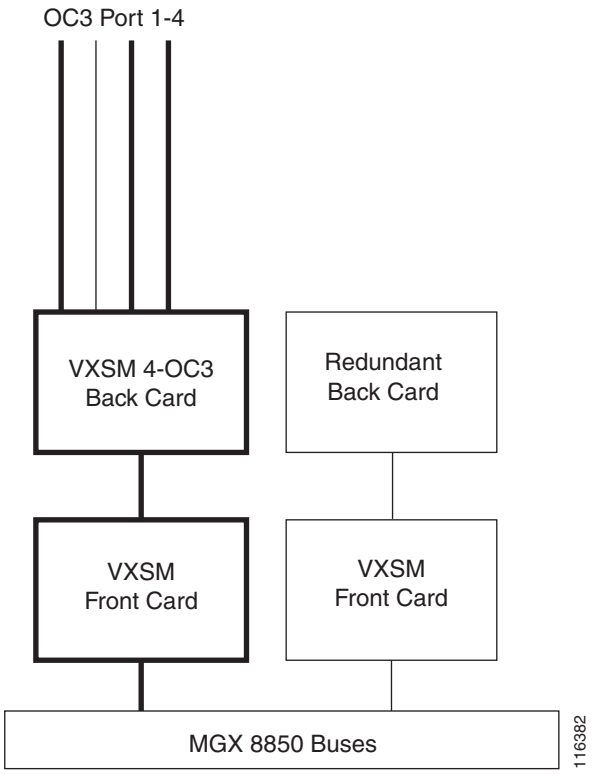
- 1:1 front card redundancy
- 1:1 front and back card redundancy
- 1+1 APS line redundancy
- 1:1 APS line redundancy

Card and line redundancy can be combined in one configuration.

1:1 Front Card Redundancy

In this scheme, the two VXSM front cards are installed in adjacent slots (slots 1 and 2, 3 and 4, 5 and 6, 9 and 10, 11 and 12, 13 and 14). The active card has the OC-3 back card and the standby card has a redundant back card (Figure 2-15). If a front card failure occurs, the redundant front becomes active. The lines in back card are connected through the redundant back card to the redundant (now active) front card.

Figure 2-15 1:1 Front Card Redundancy



1:1 Front and Back Card Redundancy

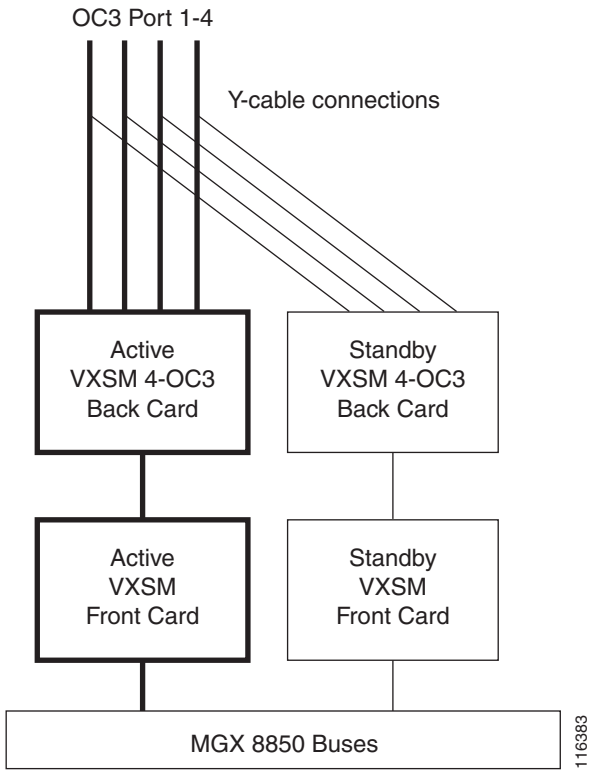
In this scheme, VXSM front and back card sets are installed in pairs: an active set and a standby set. For this feature to operate, the active and standby VXSM card sets must be in adjacent slots (slots 1 and 2, 3 and 4, 5 and 6, 9 and 10, 11 and 12, 13 and 14).

The VXSM 4-OC 3 back card provides a data path between the VXSM front card and the optical transceivers on back cards. It also provides the data path between the redundant front card and the optical transceivers on back card for front card redundancy. The VXSM back card also provides a data path between the adjacent front card and the optical transceivers on the back card for 1:1 legacy APS implementation.

The VXSM back card has an NVRAM on the board, which can be accessed through a local front card or through the redundant front card when redundant configuration is enabled or through the adjacent back card when 1:1 legacy APS is enabled.

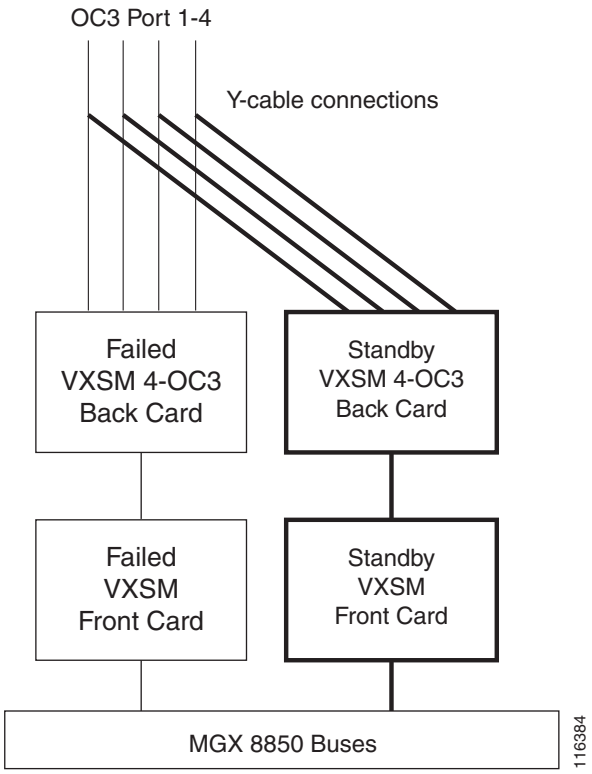
The 1:1 front and back card redundancy scheme is shown in Figure 2-16.

Figure 2-16 1:1 Front and Back Card Redundancy



If a failure occurs in either the active front card or the active back card, the entire standby card set automatically switches over and becomes the active card set. The new data path after switchover is shown in Figure 2-17.

Figure 2-17 1:1 Front and Back Card Redundancy after Switchover



Line Redundancy

SONET line APS redundancy can be set up either as same card or adjacent card.

In same card redundancy, a second, 4 OC-3 back card is installed in the lower bay providing lines 5 to 8 in addition to the lines 1 to 4 in the upper bay. One line in the upper bay is designated the working line and one line in the lower bay is designated the protection line.

In adjacent card redundancy, a VXSM front and back card set are installed in adjacent slots. Line redundancy is provided by designating one line on one back card and one line on the other back card as the working/protection set.

1+1 APS Line Redundancy

VXSM cards with SONET back cards also support 1+1 APS line redundancy in which there are two channels:

- Channel 1—*Working* channel
- Channel 2—*Protection* channel

In 1+1 APS architecture, the source node sends the data on both working and protection channel to the destination simultaneously. The destination chooses to receive the data from one of the two fiber channels, called the working channel.

If there is a failure in the working channel due to fiber cut or other reasons then the destination simply switches over to the protection channel. The destination continues to receive the data from the protection channel even after the other channel is fixed which is referred as nonrevertive mechanism.

1+1 APS line redundancy can operate on both same card and adjacent card redundant configurations.

1:1 APS Line Redundancy

VXSM cards with SONET back cards support 1:1 APS line redundancy

1:1 APS architecture is similar to 1+1 APS architecture in that there are also two fiber channels. Traffic is, however, transmitted only on the working channel. When the network is operating under normal conditions, the protection channel is unused or only used for carrying low priority traffic. The nodes switch the traffic to protection channel only when a failure occurs.

1:1 APS line redundancy can only operate on a same card redundant configuration.

48 T1/E1 and 6 T3 Systems

The 24 T1/E1 backcard and the 3 T3 backcard are designed to support:

- 1:1 front card/back card redundancy
- 1:1 front card redundancy

1:1 Front Card/Back Card Redundancy

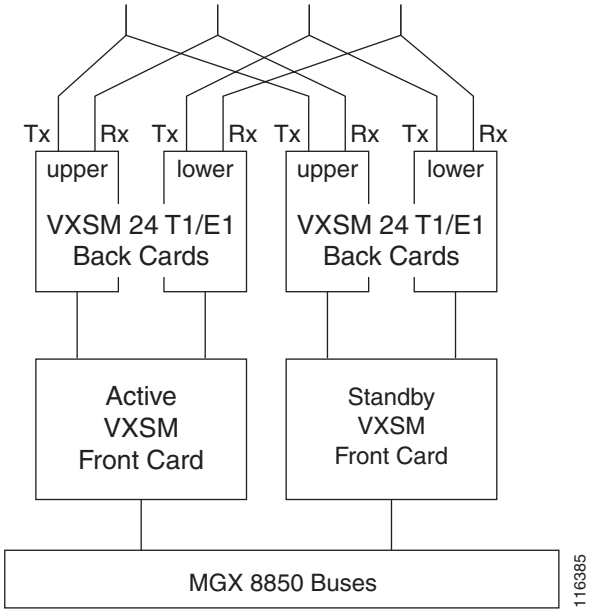
Two VXSM front cards are installed in adjacent slots. Each VXSM T1/E1 or VXSM T3 front card has two back cards installed, one in the upper bay and one in the lower bay.

For T1/E1 systems, each card has two 50-pin connectors, one for transmit and one for receive. Y-cables are used to connect lines to the corresponding connectors on each card set.

For T3 systems, each back card has two SMB connectors per port, one for transmit and one for receive, appropriate Y-cables can be used to connect lines to the corresponding connectors on each card set.

An example of a redundant arrangement for T1/E1 is shown in Figure 2-18.

Figure 2-18 1:1 Front Card/Back Card Redundancy



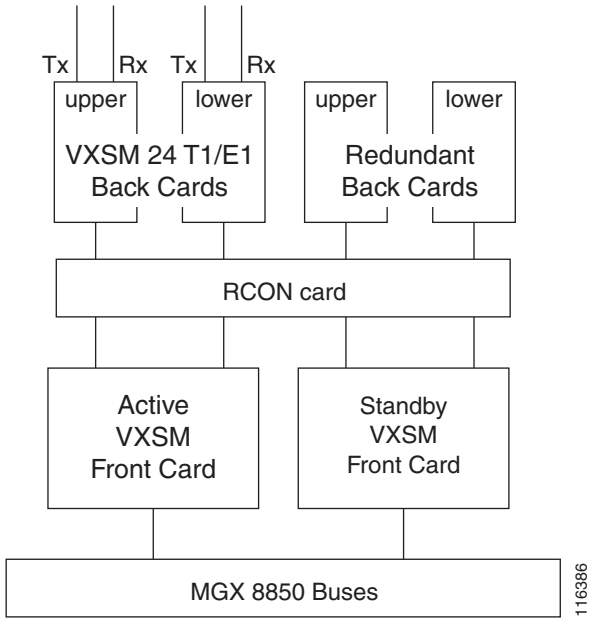
For this type of redundancy, one card set is the active set and the card set in the adjacent slot is the standby. During operation, both the card sets receive traffic, but only the active set transmits on the lines. If any failure occurs in the active front card, top back card, or bottom back card, the redundant card set becomes the active card set. The switchover is supported with the Y cables. Therefore, in the case of a switchover, complete traffic (on all 48 T1 or E1 lines) is transferred to the adjacent slot.

1:1 Front Card Redundancy

The 1:1 Front Card Redundancy scheme differs from the 1:1 Front Card Back Card scheme in that the redundant card set has redundant back cards (that do not have the lines connected to them) instead of 48 T1/E1 or 6 T3 back cards. In this scheme Y cable operation is not supported. A 1:1 front card redundancy is shown in Figure 2-19.

In this case, a RCON card (gang card) is needed and there is no back card redundancy. The redundant back card is required to switch traffic from the active front card to the redundant front card if a failure occurs. The 1:1 redundancy is achieved with the RCON (gang card used for 1:N redundancy but with N=1 only).

Figure 2-19 1:1 Front Card Redundancy



Processing Fax and Modem Traffic

VXSM supports the transmission of non-voice traffic such as clear channel, fax, and modem generated messages. VXSM can be configured such that, when a call is established, modem tones and fax preambles can be detected and acted upon accordingly. Nonvoice calls, when detected, can be handled by two methods, namely:

- Fax/modem passthrough
- T.38 fax relay

How the method is selected is user configurable. The user choices are:

- Select fax/modem passthrough only
- Select T.38 fax relay only
- Select T.38 first and, if that fails, select fax/modem passthrough

Fax/Modem/TTY Passthrough

Within a voice circuit call, VXSM supports the handling of voiceband data (vbd) such as fax, modem, and TTY transmissions. Upon detection of a voiceband tone, VXSM will perform the necessary upspeed procedure that may involve any of the following processes:

- Perform CAC calculations
- Codec manipulation
- Silence suppression

- Disabling echo cancellation
- Modify packetization period, gain, DC offset, and jitter parameters

Note Whether or not packetization period and VAD control are changed upon voiceband data detection can be controlled by the user. A voiceband data profile is maintained by VXSM that includes user configurable items that determine whether or not packetization period and VAD are enabled or disabled.

If either packetization control or VAD control is set to 'enable', the VBD module changes the values to the user configured values in VBD profile. If the packetization control and VAD control are set to 'disable', the values are not changed during upspeed.

Likewise, whether or not echo cancellation and NLP (non-linear processing) are changed upon voiceband detection can also be controlled by the user. Two parameters in the VBD profile (-ecan<EcanOverride> and -npl<NPLOverride>) can be enabled or disabled by the user. If ECANControl is set to enable, ECAN and NLP are both disabled upon detecting the first VBD tones for both high speed and low speed modems irrespective of the value of NLPControl. If ECANControl is set to disable, ECAN is not changed and NLP is changed based on the NLPControl value. If NLPControl is set to enable, NLP processing is disabled and if it is set to disable, NLP is not changed.

For upspeed to operate correctly, both ends of the connection must perform the upspeed procedure. For this reason, VXSM informs the other (remote) end of the connection when an upspeed procedure is to be performed. For fax/modem/TTY upspeed, there are two different methods by which upspeed at the remote end is triggered:

1. Passthrough with NSE—VXSM informs the remote end when it detects a voiceband tone on the voice TDM side of a call. This procedure involves a Cisco proprietary protocol in which a Named Signaling Event (NSE) is sent to the remote end. This method can be used for connections where both ends are VXSM cards or where one end is a VXSM card and the other end is a NSE compliant Cisco product.
2. Fax/modem passthrough with IP side tone detection—Relies on both ends of the connection being able to detect tones on both the TDM and IP sides. Thus both the originating and the terminating ends of the connection are able to detect the necessary tones and the need for any NSE type of message is eliminated. This method can be used with NSE compliant or none NSE compliant devices.For TTY upspeed, only the second method is supported.

Fax/modem/TTY passthrough features are as follows:

- Fax/modem/TTY passthrough with IP side tone detection is supported with TGCP, MGCP, or H.248 call setup
- FAX/modem/TTY provisioning redundancy
- Upspeed from voice codec to upspeed codec G.711u, G.711a, G.726-32 or clear channel
- Graceful upgrade for fax/modem/TTY provisioning
- Detection of the following tones, TTY (1400 Hz), CNG (1100 Hz), CED/ANS (2100 Hz), CED/ANS (2100 Hz with phase reversal) and V.21 fax preamble
- Detection of low speed modem tones, 2225 Hz (Bell modem), 2250 (USB1, V.22 bis), V.8bis, V.23-modem, and V.21-modem
- Bell low speed modem support for Bell 103/108/113, Bell 201, Bell 202,Bell 208, Bell 209, and Bell 212A
- Revert back to voice mode for fax/modem upspeed after silence detected for the configured inactivity duration..

- A TTY call does not revert back to voice mode as TTY devices may have genuine silence between character transmission

T.38 Fax Relay

The T.38 fax relay method supports fax transmissions from standard group 3 fax machines(G3FE) only. Initially, during call setup, both the MG and MGC do not know whether the call involves non-voice transmissions or not. However, once a call is setup and the tones and T.30 fax preamble indicate a group 3 fax transmission, the option of T.38 fax relay provides an alternative to the fax/modem passthrough method.

In general, fax relay offers smaller bandwidth demands on the packet network and provides greater security.

For gateway controlled T.38, switching to T.38 involves Modify or the use of Named Signaling Events (NSE) to handle the handshake between the originating and receiving gateways. Supported Named Signal Events are:

- 192—Detecting 2100 Hz ANS tone
- 193—Detecting 2100 Hz phase reversal/ANS tone
- 200—Switch to T.38
- 201—T.38 switch complete
- 202—T.38 switch fails.

In fax relay mode, the emitting gateway demodulates the T.30 transmission received from the calling terminal. The ITU-T.30 facsimile control and the image data are transferred as an octet stream structure using Internet Facsimile Protocol (IFP) packets, over the transport protocol (UDP) across the packet network.

The receiving gateway decodes the transferred information and establishes communication with the called facsimile terminal using normal T.30 procedures. The receiving gateway forwards all relevant responses from the called terminal to the emitting gateway.

For error protection, VXSM supports the “Use of Redundancy Messages” scheme as described in the ITU-T.38 recommendation, section 9.1.4.1.

Note The FEC scheme of error protection in ITU-T.38 is not supported.

The supported T30 INDICATOR types are:

- No signal
- V.21 Preamble Flags
- V.27 2400 modulation training
- V.27 4800 modulation training
- V.29 7200 modulation training
- V.29 9600 modulation training
- V.17 7200 modulation short training
- V.17 7200 modulation long training
- V.17 9600 modulation short training

- V.17 9600 modulation long training
- V.17 12 000 modulation short training
- V.17 12 000 modulation long training
- V.17 14 400 modulation short training
- V.17 14 400 modulation long training

The T.38 Fax Relay feature can be either Call Agent (CA) controlled or Gateway controlled. Both of which support MGCP, TGCP, and H.248 call control protocols.

However, the following four T.38 options are available with MGCP and TGCP call control only:

- T.38 Strict—In this option the MGC has control of the T.38 operation. This option requires an indication during call setup that the terminating end can support T.38.
- T.38 Loose—This option is the same as the T.38 Strict option except that no confirmation of T.38 support at the terminating end is required.
- Off—In this option no special procedure is invoked for fax traffic.
- Gateway—In this option the MG handles the fax calls without further involvement of the MGC

T.38 Fax Relay Statistics

VXSM accumulates two type of statistics fax calls:

- The RTP statistics which occurs in the beginning of the call before switching to T.38 mode.
- Fax specific statistics collected during T.38 operation.

Both the statistics types are maintained separately in the GWs.

The following fax relay statistics are available to users through the CLI. However, they are not be available through SNMP.

- Total number of FAX packets sent to network
- Number of FAX packets dropped due to the busy network
- Total number of valid FAX packets received from the network
- Number of lost network packets
- Number of invalid packets received from the network
- Count of out-of-sequence packets received from the network
- Most recent high-speed modulation
- Number of complete pages transferred

Network Bypass Feature

Network Bypass is a feature of a VXSM based media gateway for the efficient handling of calls that originate and terminate on the same gateway. This feature operates with H.248 media gateway control protocol only.

Depending upon the destination, incoming calls on a VXSM card can be routed in the following ways.

The call is for a ds0:

- On another gateway and is routed over the IP network to that gateway.

- On another VXSM card but in the same gateway.
- On the same VXSM card.

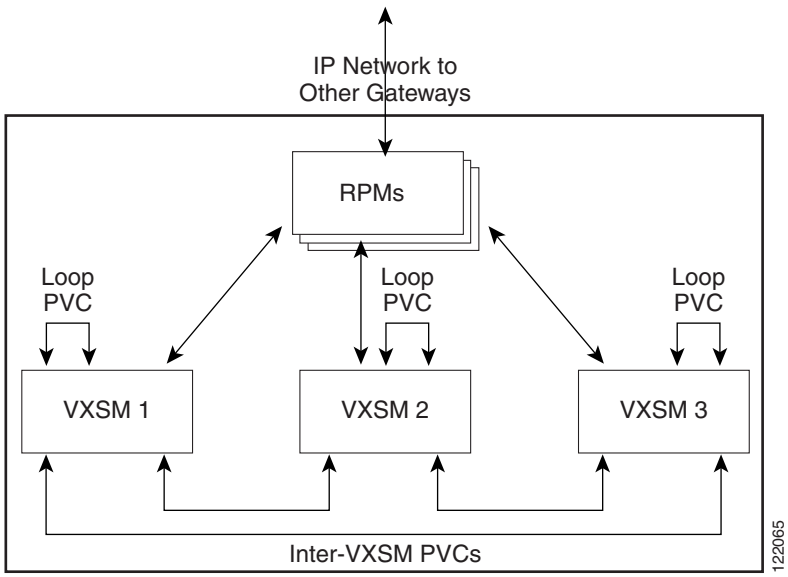
The VXSM network bypass feature, when enabled, examines the destination (NSAP address prefix) of each incoming call and makes a determination as to which of the three routing situations applies. If the incoming call is for a ds0 on the same or another VXSM card in the same gateway, the routing of the bearer circuit is made entirely within the VXSM cards in the gateway and does not involve the IP network. In this way the unnecessary use of network resources is eliminated.

Network bypass employs a mesh of user configured internal PVCs. The mesh consists of the following connections.

- Each VXSM card has PVC connections to all the other VXSM cards in the gateway. These connections provide direct inter-VXSM routing.
- Each VXSM card has a PVC connection that is looped back to itself. The looped connection provides direct intra-VXSM routing.
- Each VXSM card should have at least one external PVC (between VXSM and RPM or AXSM card) that is used to send the bearer traffic to an IP network.

Figure 2-20 shows an example of the PVCs for a three VXSM gateways.

Figure 2-20 PVC Mesh for Network Bypass—Example



Jitter Compensation

An inherent characteristic of packet networks is that the inter-arrival times of voice frames are subject to a certain amount of variation (inter-arrival jitter). The VXSM card uses a buffering mechanism to eliminate, or minimize, the amount of jitter passed from the packet network to the conventional telephone (TDM) network.

Voice frames received from the packet network are placed in a playout buffer where they experience a defined delay before being transmitted to the TDM network. In this way voice frames are transmitted in a more regular (synchronous) manner.

The amount of delay, in milliseconds, introduced by the buffer is determined by the values of three user configurable parameters known as nominal jitter delay, maximum jitter delay, and minimum jitter delay, respectively.

Nominal jitter delay is normally used to determine the delay and its value should be that of the expected average jitter experienced on the packet network (depends upon the network design, queuing delays, VAD on or off, codec frame size, and packetization period). Further, the value of the nominal jitter delay used by the buffer depends upon the buffer playout mode which can be either fixed or adaptive.

- Fixed mode—The value is a fixed delay explicitly configured by the user. Fixed mode is normally used for voice band data, fax, modem, and clear channel.
- Adaptive mode—The initial value is specified by the user but the actual value is derived from the jitter characteristics of the packet network. Adaptive mode is generally used for voice codecs.

The value used for the delay cannot be outside the range specified by user-configured minimum and maximum jitter delay values.

Alarms and Statistics

VXSM can monitor a large number of operational parameters and measure their values against configurable threshold values. When a parameter falls outside its valid threshold, an alarm is set. Likewise, VXSM maintains a large number of counters for the purpose of collecting and maintaining running statistics.

LED Indicator Alarms

The first level of alarm/status indicators are the LEDs located on the faceplate of the VXSM front card. Some of these LEDs refer to card level alarms and others to port level alarms.

Card Level LEDs

There are three card-level LEDs:

- Active LED (green)—Card is in the Active state.
- Standby LED (orange)—Card is in the Standby state, or the card's DSPs are being downloaded as part of card boot-up. Standby LED blinks orange when the card is in the boot state.
- Fail LED (red)—Card is in the Fail state.

Port Level LEDs

Port-level LEDs exist for each port supported by the front card: 4 LEDs for the OC-3 version, and 48 for the T1/E1 version.

The line LEDs are lit:

- Green—If the line is added and there is no alarm on the line.
- Orange—If the line is added and there is a Yellow alarm condition on the line.
- Red—If the line is added and a LoS condition exists (Red alarm condition) on the line.

Software Alarms

VXSM software is equipped to display a large number of alarm conditions through **display** commands. An equivalent set of **configure** commands permit the user to set threshold levels that, when exceeded, trigger individual alarms.

For example, alarms supported for OC-3 ports include.

- sonet line
- sonet section
- sonetpath ds1, ds3, E1, sts

Statistics

Statistics related to the network interfaces and ATM connections can be collected and stored locally on the card as statistics files. Users can see the value of the collected statistics either by executing certain display commands (for example, **dspsvccnt** to display SVC counters) or uploading the statistics files to a network management system such as Cisco WAN Manager.

The **cnfcdstat (**configure card statistics) command can be used to:

- Enable/disable statistics collection
- Configure the bucket interval (within the collection interval)
- Configure the collection interval
- Configure the level of statistics to be collected

Data for previous intervals can be uploaded to an NMS while a current interval of data is being collected. When the data for the current interval is collected, another statistics file is created with a filename based on the current timestamp. Statistics files for up to ten intervals can be maintained locally on the card. Older intervals are automatically purged, whether or not they have been uploaded

Some example commands for displaying statistics are:

- **dspbert**—display BERT counters
- **dspchancnt**—display channel counters

CHAPTER 3

Configuring VoIP Switching Applications

You can configure a Cisco MGX 8850 or 8880 switch equipped with VXSMs that functions as a media gateway to meet the requirements of many applications. In VoIP switching applications, the voice TDM interface, the packet network interface, and the interface to a call agent require configuration. The switching application uses VXSM cards, the PXM-45 card, and either the AXSM or the RPM-XF cards.

The interface to the packet network can be either:

- VoIP over Ethernet—An RPM-XF card is used, or
- VoIP over ATM—An AXSM card is used

These cards function together and must be configured accordingly.

VoIP switching configuration consists of the following tasks.

1. Initial PXM-45 card configuration to configure the gateway as a whole.
2. AXSM or RPM-XF card configuration to set up the interface to the VoIP/ATM or VoIP/Ethernet network.
3. VXSM card configuration to set up the TDM interface and to make the connection between the TDM and network interfaces.
4. Media Gateway Controller and associated protocol configuration to set up the interface between the gateway and the gateway controller.

Note A VXSM card supports three media gateway control protocols but only one at a time. The user must choose between either H.248, MGCP, or TGCP. The choice is made by executing the **setrev** command on the PXM. In this command, the user specifies the VXSM card (by slot number) and selects the MGCP protocol as one of the parameters. The effect of this command is to load a firmware image in the VXSM card with the "not selected" protocol commands disabled. Note that the CALEA images do not support H.248.

Quick Start Procedure

Table 3-1 shows an overview of tasks and commands required to set up the media gateway for VoIP switching application. In addition, the same procedure is presented later in this chapter in greater detail. For details on the commands used in this procedure, refer to the *Cisco Voice Switch Service Module (VXSM) Command Reference*.

Note VXSM does not support both AXSM and RPM-XF packet network interfaces on the same card. The following procedure is for gateways using either an RPM-XF or an AXSM card as the interface to the network. Use the RPM-XF or AXSM commands as appropriate for your application.

However, AXSM and RPM-XF cards can be configured in the same media gateway provided they are used on separate VXSM cards.

Table 3-1 Configuration for VoIP

Card Type	Major Task	Subtask/Commands
PXM-45	Basic gateway setup	Basic PXM-45 setup commands **cnfname** **cnfdate** **cnftmzn** **cnftmznmgt** **cnftime** **addcontroller** **ipifconfig** **addsct**
PXM-45	Select MGCP protocol	**setrev**

Table 3-1 Configuration for VoIP (continued)

Card Type	Major Task	Subtask/Commands
AXSM for VoIP over ATM or RPM-XP for VoIP over Ethernet	Set up interface to network using either the AXSM or RPM-XF cards	If using RPM-XF RPM-XF Setup Commands Logon **enable** **password** **config terminal** Create PNNI partition **interface switch1** **switch partition** **ingress_percentage-bandwidth** **egress-percentage-bandwidth** **vci** **vpi** **connection-limit** **end** Create ATM subinterface **interface** **ip** **pvc** **vbr_nrt** **encapsulation** **exit-vc** Create Gigabit Ethernet interface **interface gigabitethernet** **ip address** **negotiationauto** **no shutdown** **copy**

Table 3-1 Configuration for VoIP (continued)

Card Type	Major Task	Subtask/Commands
VXSM	Setup VXSM card	Create VXSM resource **partition** **addrscprtn** Bring up VXSM Lines **upln** **uppath** **-sts -ds1** (OC-3 only) Config Voice Interfaces **addvif** **cnfpath** **-sts** **-payload** (OC-3 only)
AXSM or RPM-XF	Create slave end of each connection at RPM-XF or AXSM: one for bearer and one for control. This task can be repeated for up to 8 bearer connections.	If using RPM-XF, setup slave end on RPM-XF **switch connection** **rmbs** **rpcr** **rscr** **cpmm-id** **pcr** **csr**
VXSM	Create master end of connections on VXSM: one for bearer and one for control. This task can be repeated for each of the slaves configured in the previous step.	VXSM connection command **addcon**
VXSM	Assign an IP address on VXSM for each connection.	**addconip**

Table 3-1 Configuration for VoIP (continued)

Card Type	Major Task	Subtask/Commands
VXSM	Configure MGC Interface on VXSM	If MGC protocol is H.248 Configure MGC **addmgcdn** **cnfmgc** **addmgcip** **addmgcgrpmgc** Configure H.248 Protocol **cnfprotocolport** **addh248assoc** **cnfh248rootpkg** **cnfh248param** **cnfh248mg** **addh248prof** **cnfh248nameschema** Configure VIF termination **addvif (if not already done)** **cnfvifterm** **addviftermtype**
VXSM	Bring gateway into service	**cnfh248is**

Configuring the PXM-45 Card

Log on to the PXM-45 card and perform the following steps to configure the PXM-45 card for VoIP using the VXSM. The PXM-45 has a large number of commands. These steps deal only with the minimum commands required to set up the MGX 8850 as media gateway.

Step 1 Use the **cnfname** command to give the MGX 8850 a node name.

```
unknown.7.PXM.a > cnfname <node name>
```

Enter up to 32 characters for the new node name, (node name is case-sensitive).

For example:

```
unknown.7.PXM.a > cnfname gateway1
```

After the user responds **Yes** to a confirmation request, the name is changed to gateway1

Step 2 Use the **cnfdate** command to set the date.

```
gateway1.7.PXM.a > cnfdate <mm/dd/yyyy>
```

Step 3 Use the **cnftmzn** command to set the time zone.

```
geteway1.7.PXM.a > cnftmzn <timezone>
```

Step 4 Use the **cnftmzngmt** command to set an offset if an offset from GMT is to be used.

```
geteway1.7.PXM.a > cnftmznmgt <timeoffsetGMT>Offset can be from -12 to +12.
```

Step 5 Use the **cnftime** command to enter the time.

```
geteway1.7.PXM.a > cnftime <hh:mm:ss>
```

Step 6 Use the **addcontroller** command to add a PNNI controller to the PXM card

```
geteway1.7.PXM.a > addcontroller <cntrlrId> i <cntrlrType> <slot> [cntrlrName
```

cntrlrId is the controller ID, enter 2 to specify a PNNI controller.

"i" stands for internal

cntrlrType is the controller type, enter 2 to specify a PNNI controller type.

slot is the PXM-45 slot in the MGX 8850, enter 7 or 8 as appropriate.

cntrlrName is an optional controller name, enter a text name is desired.

Step 7 Use the **ipifconfig** command to specify a LAN IP address for the node.

```
geteway1.7.PXM.a > ipifconfig lnPci0 <IP_Addr>[<netmask <Mask>]
```

Specify the values for the IP address and its associated netmask.

Step 8 Setup a Service Class Template (SCT) for the AXSM card. The SCT file name has the following format: AXSM_SCT.CARD.2.V1

The SCT file must have been ftp'd to the node's PXM-45 disk in the C:SCT/TEMP directory

Use the **dspsctchksum** command to display the checksum value of the file. Note the value of checksum

Note A Service Class Template (SCT) is a collection of ATM configuration parameter settings that are stored in a single file and can be applied to multiple lines or ports. SCT files include the following types of configuration data:

General link parameters
COSB (Class of Service Buffers) parameters
Virtual circuit threshold parameters
COSB threshold parameters

Step 9 Use the **addsct** to move the file to the F:SCT/AXSM directory on the PXM-45 disk. This has the effect of installing the SCT.

```
geteway1.10.AXSM.a > addsct <card type> <sct type> <sct ID> <Maj ver> <chksum>
```

cardtype is the card whose SCT you want to make available to the card by installing the SCT in the appropriate directory. Enter 1 for AXSM

scttype identifies either a port-level or a card-level SCT. Enter 2 for card level.

SCT ID refers to a specific service class template. The SCT is either provided by Cisco or created through CWM. Possible IDs are, Cisco-provided: 1-100 and User-created: 101-255. The default SCT ID is 0.

Maj ver is the major version number of the file. This number is assigned by Cisco.

checksum is the checksum for the file. Use the value obtained from the dspsctchksum command. The value is also published in the relevant release notes.

Step 10 Repeat Steps 8 and 9 for the port SCT to be used by the PXM-45. In the **addsct** command, specify 1 (port level) for the **scttype** parameter.

Step 11 Select the media gateway controller protocol for the card. Use the **setrev** command and select either H.248 or TGCP. This command force loads the image to the VXSM with only the selected MGCP commands enabled.

Configuring AXSM or RPM-XF

The following procedure configures the gateway's interface to the packet network. Use the AXSM card configuration procedure if the interface to the network is ATM. Use the RPM-XF card configuration procedure if the interface to the network is Ethernet.

AXSM Card Configuration

Log on to the AXSM card and perform the following steps to configure the AXSM card for VoIP/ATM using the VXSM. The AXSM has a large number of commands. These steps deal only with the minimum commands required to setup the MGX 8880 as a media gateway.

Step 1 Use the **upln** command to bring up the AXSM lines to be used by the gateway. This command establishes minimal connectivity over the line.

```
geteway1.10.AXSM.a > upln <bay.line>
```

For bay, enter 1 if the line on the back card is in the upper bay and enter 2 if it is in the lower bay. For line, enter the back card port number to which the line is connected.

Step 2 Use the **cnfln** command to configure a SONET lines.

```
geteway1.10.AXSM.a > cnfln -sonet <bay.line> -slt <LineType> -clk <clock source>
```

Enter the bay and line of the line being configured (see upln above). For LineType, enter 1 for SONET or 2 for SDH. For clockSource, enter 1 to use a clock received over the line from a remote node or 2 (the default) to use the local timing defined for the local node.

Step 3 Use the **addport** command to enable ATM communications over the line.

```
geteway1.10.AXSM.a > addport <ifNum> <bay.line> <guaranteedRate> <maxRate> <sctID>
<ifType>
```

For ifNum, enter a number from 1 to 60 to identify this interface. The interface number must be unique on the card to which it is assigned. For UNI and NNI ports, you can assign one logical interface per line.

For guaranteedRate and maxRate, enter an OC3 value in the range of 50 to 353207 cells per second.

For ifType, enter 1 for UNI, 2 for NNI

When AXSM is connected to an ATM router (ATM end devices), UNI is used. When AXSM is connected to core ATM NW devices, NNI is used

Step 4 Use the **addpart** command to create resource partition on the AXSM card. This command automatically creates a controller partition on the AXSM card. This command should be executed for each port that uses the controller.

```
geteway1.10.AXSM.a > addpart <ifNum> <partId> <ctrlrId> <egrminbw> <egrmaxbw> <ingminbw>
<ingmaxbw> <minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

For ifNum, enter the port number. For partId, enter 1 for PNNI. For cntrlid, enter 2 for PNNI.

The remaining parameters are used to specify maximum and minimum values for vpi/vci, bandwidth, connections, etc., see the Cisco MGX 8850 (PXM45 and PXM1E) Command Reference, Release 5 for details.

Configuring RPM-XF Cards

The object of RPM-XF card configuration is to:

- Create a PNNI resource partition
- Create an ATM subinterface
- Create a gigabit Ethernet interface

Creating a PNNI Resource Partition

Perform the following steps to create a PNNI resource partition for the RPM-XF.

Step 1 Use the cc command to switch to the RPM-XF card.

Step 2 Enter the **enable** command and password for the router.

```
Router>enable
Password:
```

Step 3 Enter the **config terminal** command.

```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Step 4 Enter the **interface** command

```
Router(config)#interface Switch1
```

Step 5 Enter the switch partition command.

```
(config-if)# switch partition {vcc | vpc} <partId> <ctrlrId>
```

For partId the range is 1 to 10; 1 is reserved for PNNI. Enter 1.

For ctrlrId, the range is 2to 255; 2 is reserved for PNNI. Enter 2.

Thus: (config-if)# **switch partition** *1 2*

Step 6 Enter the ingress-percentage-bandwidth command at the swpart prompt to specify the minimum and maximum ingress percentage bandwidth.

```
(config-if-swpart)# ingress-percentage-bandwidth <ingMinPctBw> <ingMaxPctBw>
```

For example, (config-if-swpart)#**ingress-percentage-bandwidth** 10 100

Step 7 Enter the egress-percentage-bandwidth command to specify the minimum and maximum egress percentage bandwidth.

```
(config-if-swpart)# egress-percentage-bandwidth <egrMinPctBw> <egrMaxPctBw>
```

For example, (config-if-swpart)# **egress-percentage-bandwidth** 10 100

Step 8 Enter the **vpi** command to specify the minimum and maximum vpi.

```
(config-if-swpart)# vpi <min_vpi> <max_vpi>
```

For example, (config-if-swpart)# **vpi** 20 240

Step 9 Enter the vci command to specify the minimum and maximum vci.

```
(config-if-swpart)# vci <min_vci> <max_vci>
```

For example, (config-if-swpart)# **vci** 50 65535

Step 10 Enter the connection-limit command to specify the minimum and maximum connection limits.

```
(config-if-swpart)# connection-limit <mincon><maxcon>
```

For example, (config-if-swpart)# **connection-limit** 1000 8000

Creating an ATM Subinterface

Perform the following steps to create an ATM subinterface. This procedure is in preparation for creating the master end of the connection to the VXSM card.

Step 1 Set up a switch subinterface

a. Enter the **interface** command.

```
Router(config)# interface switch 1<subinterface> <multipoint | point-to-point | mpls |
tag-switching>
```

Specify 1 for subinterface and point-to-point for the type of interface.

For example,

Router(config)#**interface switch 1**.1 point-to-point

b. Enter the **ip** command to add an IP address to the subinterface.

```
Router(config-subif)# ip address
 <ip_addr> <subnet_mask>
```

Enter the IP address for the subinterface and a mask of 255.255.255.0. The IP address should be the same as that used when setting up the slave end of the connection on the VXSM.

The following example adds IP address 1.1.1.1 to subinterface 1 and defines the network mask as 255.255.255.0

c. Enter the pvc command to add a PVC to the subinterface.

```
Router(config-subif)# pvc
<vpi>/<vci>
```

Note The VPI and VCI values you enter for the PVC must be within the ranges set for the PNNI controller when the PNNI partition was defined for the switch interface.

After you enter this command, the switch enters virtual circuit configuration mode for this PVC.

d. Specify the PVC variable bit rate parameters.

```
Router(config-if-atm-vc)# vbr-nrt pcr scr mbs
```

Enter values for PCR and SCR in kbps and MBS in cells.

e. Specify type of encapsulation to IP over AAL5.

```
Router(configu-if-atm-vc)#encapsulation aal5mux ip
```

f. When you have finished configuring the PVC, enter the exit-vc command to return to subinterface configuration mode.

```
Router(config-if-atm-vc)#exit-vc
```

Creating a Gigabit Ethernet Interface

Perform the following steps to configure the RPM-XF gigabit Ethernet interface to the network.

Step 1 At the Router> prompt enter the **enable** command and enter your password at the prompt. The router will enter the privileged EXEC mode.

Step 2 Use the config -t command to change to global configuration mode.

```
Router#config -t
```

Step 3 At the global configuration prompt, specify the new interface to configure by entering the **interface gigabitethernet** command

```
Router(config)# interface gigabitethernet <bay/port>
```

For example, Router(config)# **interface gigabitethernet** 1/0

Step 4 Assign an IP address and a subnet mask to the interface with the **ip address** command.

```
Router(config-if)# ip address <ip address><netmask>
```

For example, Router(config-if)# **ip address** 192.168.255.255 255.255.255.0

Step 5 Modify the MGX-1GE back card configuration.

a. Use the **negotiation auto** command to permit negotiation of the flow control parameter.

b. In configuration mode, use the **loopback** command to configure loopback testing

Step 6 Enter the **no shutdown** command to enable the interface.

```
Router(config-if)# no shutdown
```

Step 7 When all of the configuration subcommands are complete, press Cntl-Z to exit configuration mode.

Step 8 Write the new configuration to memory.

```
Router# copy running-config startup-config
```

The system displays an OK message when the configuration is stored.

Configuring VXSM Cards

Log on to the VXSM card and perform the following procedures to configure the VXSM card for VoIP. The VXSM card has a large number of commands. These steps deal only with the minimum commands required to set up the MGX 8880 as a media gateway for a VoIP switching application. Setting up other VoIP features such as CALEA, Bearer and Signaling Security, and Redundancy are included later in this chapter.

Depending upon the application, VXSM accesses the network either through RPM or AXSM cards. This is accomplished through PVC connections created between the VXSM and its network cards.

In switching applications, two connections types need to be made. The first type is a bearer connection for voice traffic over the packet network, up to eight such PVCs can be configured. The second type is a control connection for control messages to and from the media gateway controller (call agent), only one control connection per VXSM card can be configured.

Configuring the TDM Interface

Identifying Voice Circuits

The OC-3, 48 T1/E1, and 6 T3/E3 versions of the VXSM cards, support a variety of multiplexing schemes for interfacing to voice circuits. These schemes fall into four major categories:

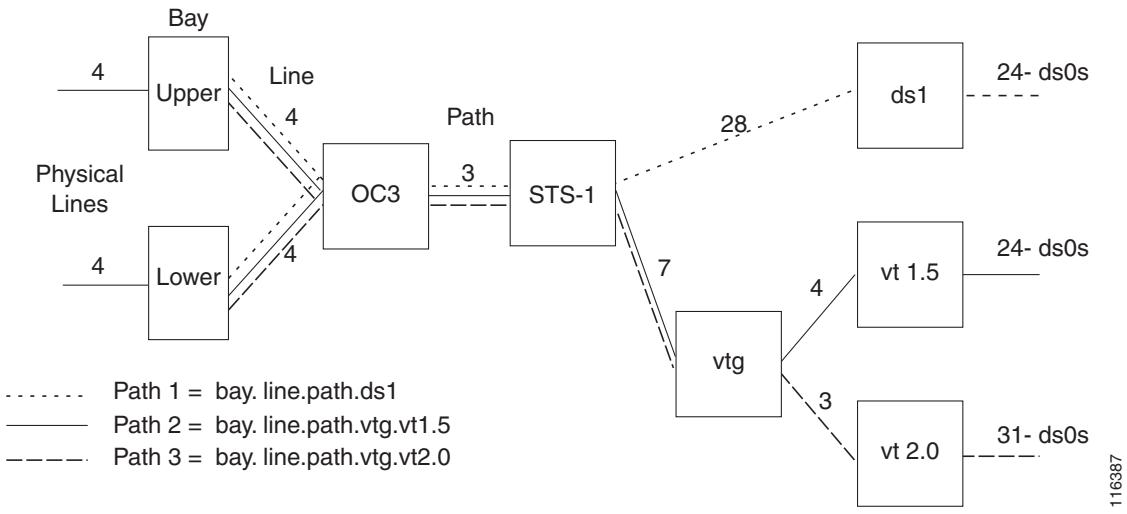
- Multiplexing under the OC-3 standards.
- Multiplexing under the SDH (Synchronous Digital Hierarchy) standards.
- Multiplexing under the T1 and E1 standards.
- Multiplexing under the T3 and E3 standards (T3 only in Release 5.2).

Many of the VXSM commands require the user to specify a line, a single voice circuit, or a group of voice circuits. The following paragraphs describe how these items are specified for the different multiplexing schemes.

OC-3 Systems

Specifying a DS0 stream from the highly multiplexed bit stream of OC3 is performed using the relationships (paths) shown in Figure 3-1.

Figure 3-1 OC-3 Hierarchical Relationship



The bit stream interfaces with VXSM via one of the four physical lines in the OC3 back card. This interface is usually in the upper bay (but, when a redundant back card is used and is active, it is in the lower bay).

For a particular line, the OC3 stream consists of three paths and, depending upon the format, a path consists of either 7 virtual tributary groups (vtg) or 28 DS1s. A vtg can be further divided into either four virtual tributaries (version 1.5) or three virtual tributaries (version 2.0). The DS1 and the virtual tributaries (vt) consist of 24 T1 DS0s for T1 or 31 DS0s for E1.

As shown in the diagram, the relationship between DS0s and physical ports can take one of three paths. The paths are common between the physical line and STS-1 level. From the STS-1 level to the DS0, one of three paths can be taken.

The path that a particular DS1/DS0 will use can be configured by the user with the **-payload** parameter in the **cnfpath -sts** command. This parameter can be set to:

- 3 = ds3 (not applicable to SDH interface)—The path is carrying a DS3 payload.
- 4 = vt15vc11—The path is carrying a SONET-VT1.5/SDH-VC11 payload.
- 5 = vt20vc12—The path is carrying a SONET-VT2/SDH-VC12 payload.

Note The vt1.5 path and the vt2.0 path also support SDH-VC11 and SDH-VC12 interfaces respectively.

Using the system described above, DS1 paths in VXSM commands are formatted as follows:

- **SONET path payload type VT1.5 or VT2.0**

  The DS1 is specified as: *bay.line.path.vtg.vt*

  bay = 1 (upper bay)
  line = the line number on the associated OC-3 card in the range 1 to 4.
  path = the path of the virtual tributary in the range 1 to 3.
  vtg = the virtual tributary groups applicable to the connection in the range 1 to 7.
  vt = virtual tributaries in the range 1 to 4 for vt1.5 or 1 to 3 for vt2.0.

Caution The combination of seven vtgs and four vts allows the specification of one of up to 28 DS1s. Be aware that VXSM supports two schemes for mapping a DS1 to a vtg/vt combination. These schemes are known as standard and Titan and are described in Table 5-1VTG/VT to DS1 Mapping, page 5-3.
vtg = the virtual tributary group.
vt = virtual tributary

- **SONET path payload type is ds3.**

The DS1 is specified as: *bay.line.path.ds1*

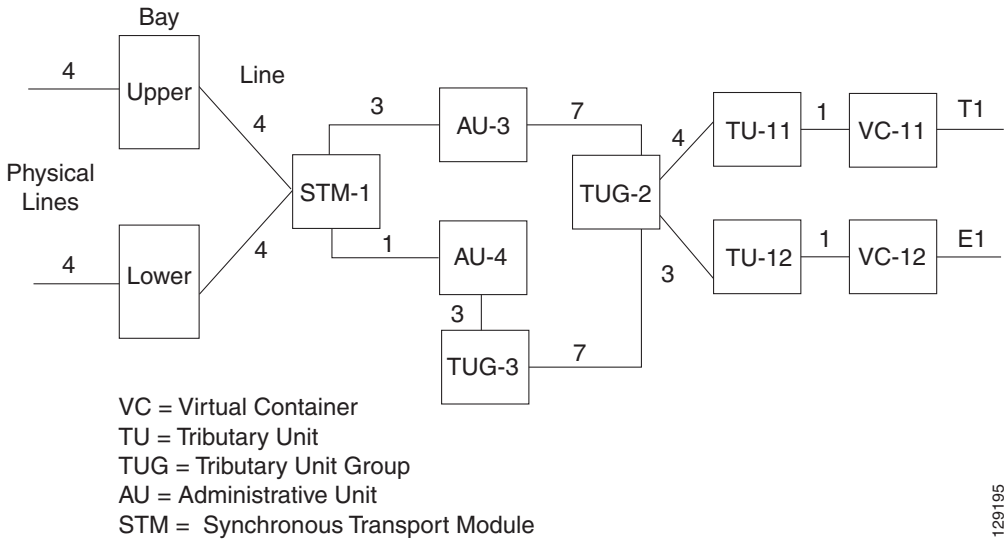
bay = upper of lower bay of the VXSM backcard.
line = the line number on the associated OC-3 card in the range 1 to 4.
path = the SONET (STS-1) path payload type as ds3 in the range 1 to 3.
ds1 = *the* ds1 channel within the ds3 interface in the range 1 to 28.

SDH Systems

The VXSM- 155 card supports voice circuits that are multiplexed according to the Synchronous Digital Hierarchy (SDH) standard. Each OC- 3 line presents the data stream as a 155.52 Mbps Synchronous Transport Module (STM-1).

Figure 3-2 shows the multiplexing paths between STM-1 at the physical line and the T1 or E1 voice circuits.

Figure 3-2 SDH Hierarchical Relationships



When using the SDH interface, the user must configure the path using the **cnfpath -sts** command. The format of this command is:

cnfpath -sts <*bay.line.path*> [**-payload** <*Path Payload*>] [**-tm** <*Tributary Mapping Type*>] [**-tg** <*Tributary Grouping*>] [**-txtrace** <*Transmit Trace*>] [**-extrace** <*Expect Trace*>]

<*bay.line.path*>, specifies the bay (1 = upper), the physical line number on the back card, the path number between the STM and the AU (1, 2, or 3 for AU-3, 1 for AU-4)

-payload <*Path Payload*>, specifies the TU/VC combination (TU-11/VC-11 for T1 or TU-12/VC-12 for E1).

-tm<*Tributary Mapping Type*>, specifies the mapping mode, 1 = asynchronous mode or 2 = byteSynchronous mode.

-tg <*Tributary Grouping*>, specifies the tributary grouping This is a choice between AU-3 or AU-4 (the default).

2 = au3Grouping—Applicable to SDH interfaces: STM1, -AU-3, -TUG-2, -TU-12, -VC12 or STM1, -AU-3, -TUG-2, -TU-11, -VC11.
3 = au4Grouping—Applicable to SDH interfaces: STM1, -AU-4, -TUG-3, -TUG-2, -TU-12, -VC12 or STM1, -AU-4, -TUG-3, -TUG-2, -TU-11, -VC11.

T1/E1 Systems

In T1/E1 systems, the front card supports up to 48 T1 or E1 lines. The back card supports up to 24 T1 or E1 lines. Depending upon the number of lines to be supported, one or two half high back cards are configured using 1 front card; one in the upper or lower bay and the other (if configured) in the remaining open bay.

A physical line or a DS1 service is specified simply as:
bay.line

where:
bay = 1 or *2*—1 for the upper bay, 2 for the lower bay.

line = 1 – 24, The physical T1 line on the back card in the range 1 to 24.

If the command requires the interface to be further specified down to the DS0 level, the DS0 is specified as:

bay.line ds0grp

where:

ds0grp = 0 - 23 or 30 — The DS0 group in the range of 0 to 23 for T1 or 0 to 30 for E1.

T3/E3 Systems

In T3/E3 systems, the front card supports up to 6 T3 or E3 lines. The back card supports up to 3 T3 or E3 lines. Depending upon the number of lines to be supported, one or two half height back cards are configured with a single front card; one in the upper or lower bay and other (if configured) in the remaining open bay.

A DS1 is specified simply as:

bay.line.path

where:

bay = *1* or *2*—1 for the upper bay, 2 for the lower bay.

line = 1 – 3—The physical T3 line on the back card in the range 1 to 3

path = 1 - 28—The DS1 circuit in the T3 line in the range of 1 to 28

If the command requires the interface to be specified down to the DS0 level, the DS0 is specified as:

bay.line.path ds0grp

where:

ds0grp = 0 - 23 or 30 — The DS0 group in the range of 0 to 23 for T1 or 0 to 30 for E1.

Note The VXSM T3/E3 card set is designed to support both T3 and E3 applications. However, in Release 5.2 only T3 services are supported.

Voice Interfaces

A voice interface (VIF) is a user configurable set of parameters that is applied to a group of DS0s within a DS1. The configuration settings of the VIF are used by the digital signal processors (DSPs) to determine how a voice payload is to be processed by VXSM. This is particularly true when the VXSM is operating in VoIP Switching mode.

A voice interface is created using the **addvif** command. With this command the user specifies a VIF number (DS0 group number) and its associated DS1, in addition, the type of signaling, the type of service (H.248 switching, trunking). Other bearer channel parameters such as echo cancellation and voice activity detection, are also specified, using **cnfvifec**, **cnfvifvad**, and other commands as listed below. These parameters are contained within a vif which, when the VIF is added, are assigned default values.

Once a VIF is created, its parameters can be discovered using the **dspvif** command. There are also display and configure commands for the user to see and configure the various parameters

To create and configure a VIF perform the following steps.

Step 1 Use the **dspvifs** command to check that the VIF exists. If it does not, use the **addvif** command to create the VIF.

Step 2 For a particular DS1, use one of the display VIF commands to display its associated VIF parameter values. Determine which parameter (if any) need to be modified.

dspvif [<*bay.line.path.vtg.vt* >] | [<*bay.line.path.ds1*>] <*ds0GroupId*> *for OC-3*

dspvif <*bay.line*> <*ds0GroupId*> *for 48 T1/E1*

dspvif <bay.line.ds1> <*Ds0GrpIndex*> *for T3*

dspvifvad <*bay.line.path.vtg.vt* > | <*bay.line.path.ds1*> <*ds0GroupId*> *for OC-3*

dspvifterms

dspvifterm [< *bay.line.path.vtg.vt* >] | [<*bay.line.path.ds1*>] <*ds0GroupId*> *for OC-3*

dspvifterm <*bay.line*> <*ds0GroupId*> *for 48 T1/E1*

dspvifterm <bay.line.ds1> <*Ds0GrpCfgIndex*> *for T3*

dspvifparam <*bay.line*> <*ds0GroupId*> *for 48 T1/E1*

dspvifparams

dspvifparam <bay.line.ds1> <*Ds0GrpCfgIndex*> *for T3*

dspviftoneplan <*bay.line*> <*ds0GroupId*> *for 48 T1/E1*

dspviftoneplan<*bay.line*> <*ds0GroupId*> *for 48 T1/E1*

dspviftoneplan <bay.line.ds1> <*Ds0GrpCfgIndex*> *for T3*

dspviftoneplans

dspvifgainattn <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*> *for OC-3*

dspvifgainattns *for OC-3*

dspviftd <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*> *for OC-3*

dspviftds *for OC-3*

Step 3 Use any of the following **configure vif** commands to modify VIF parameters.

H.248 Commands

cnfvifec<*bay.line.path.vtg.vt* > | <*bay.line.path.ds1*> <*ds0GroupId*> <*EchoCancelEnable*> <*EchoCancelCoverage*> <*Repetition*>

cnfvifeventmapping <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*> <*EventMappingIndex*>

cnfvifgainattn<*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*><*InputGain*><*outputAttn*><*repetition*>

cnfviftd <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*><*InitDigitTimeout*><*InterDigitTimeout*><*repetition*>**c**

cnfvifparam <*specified ds1*> <*ds0GroupId*> <*NoiseRegEnable*> <*NonLinearProcEnable*> <*MusicOnHoldThreshold*> <*ModemPassThru*> <*UpspeedCodec*> <*Repetition*>

cnfvifterm <*specified ds1*> <*ds0GroupId*> <*gatewayLinkId*> <*packageIds*> <*profileId*>

cnfviftoneplan <*specified ds1*> < *ds0GroupId*> <*tonePlanId*>

cnfvifvad<*bay.line.path.vtg.vt* > | <*bay.line.path.ds1*> <*ccasGrpCfgIndex*> <*VAD*> <*VadTimer*> <*Repetition*>

TGCP Commands

cnfvifec <*bay.line.path.vtg.vt* > | <*bay.line.path.ds1*> <*ds0GroupId*> <*EchoCancelEnable*> <*EchoCancelCoverage*> <*Repetition*>

cnfvifeventmapping <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*> <*EventMappingIndex*>

cnfvifgainattn<*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*><*InputGain*> <*outputAttn*><*repetition*>

cnfvifparam<*specified ds1*> <*ds0GroupId*> <*NoiseRegEnable*> <*NonLinearProcEnable*> <*MusicOnHoldThreshold*> <*Repetition*>

cnfviftd <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*ds0GroupId*><*InitDigitTimeout*><*InterDigitTimeout*><*repetition*>*(Only applicable when service is xgcp)*

cnfvifvad<*bay.line.path.vtg.vt* > | <*bay.line.path.ds1*> <*ccasGrpCfgIndex*> <*VAD*> <*VadTimer*> <*Repetition*>

cnfvifxgcpprof<*bay.line.path.vtg.vt* > | <*bay.line.path.ds1*> <*sd0GroupId*> <*XgcpProfileIndex*> <*Repetition*>

See the chapters entitled VXSM Commands for a description of the commands listed in steps 2 and 3.

Configuring TDM Lines

Use the following steps to configure the TDM lines on the VXSM.

Step 1 Use the **upln** command to bring up a VXSM line.

```
upln <bay.line>
```

For bay, enter 1 for upper bay or 2 for upper bay.

For line, enter a value in the range 1 - 4 for OC-3, 1 - 24 for 48T1/E1, 1 - 3 for T3.

Step 2 For OC-3 cards, use the **uppath** command to specify the STS-1 path within the OC-3

```
uppath -sts<bay.line.path>
```

For bay, enter 1 for upper bay or 2 for lower bay.

For line, enter a value between 1 and 4 to indicate the physical OC-3 interface on the back card.

For path, enter a value between 1 and 3 to indicate the DS3 path within the OC-3 interface.

Step 3 For OC-3 cards, use the -**payload** parameter in the **cnfpath** -**sts** command to specify the ds1 path with the OC-3. The choices are ds3, vt1.5, and vt2.0.

cnfpath -sts*<bay.line.path>[-payload <PathPayload>][-tm <TributaryMappingType>][-tg <TributaryGroupingType>][-txtrace <PathTraceToTransmit>][-exptrace <PathTraceToExpect]*
<bay.line.path>

bay: 1

line: 1 - 4

path: 1 - 3 or 1 (AU4 only)

[-payload <PathPayload>]

3 - ds3

4 - vt15vc11

5 - vt20vc12

[-tm <TributaryMappingType>]

1 - asynchronous

2 - byteSynchronous (NA for ds3)

[-tg <TributaryGroupingType>]

1 - notApplicable (Sonet)

2 - au3Grouping (SDH)

3 - au4Grouping (SDH)

[-txtrace <PathTraceToTransmit>]

trace-string: size 16(SDH) or 64(Sonet)

[-exptrace <PathTraceToExpect]

trace-string: size 16(SDH) or 64(Sonet)

Step 4 For OC-3 cards, use the **uppath** command to specify the DS1 path within the DS3

```
uppath -ds1<bay.line.path.vtg/ds3.vt/ds1>
```

For bay, enter 1 for upper bay or 2 for upper bay.

For line, enter a value between 1 and 4 to indicate the physical OC-3 interface on the back card.

For path, enter a value between 1 and 3 to indicate the DS3 path within the OC-3 interface.

Step 5 Use the appropriate **addvif** command to add a voice interface for a DS0 group within a DS1.

For OC-3 use, **addvif** <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*Ds0GrpIndex*> <*Ds0BitMap*> <*ServiceType*> <*Repetition*>

For T1/E1 use, **addvif** <*bay.line*> <*ds0GrpIndex*> <d*s0ChannelBitMap*> <*ServiceType*> <*Repetition*>

For T3 use, **addvif** <bay.line.ds1> <*ds0GrpIndex*> <d*s0ChannelBitMap*> <*ServiceType*> <*Repetition*>

LineNum for OC-3—(bay.line.path.vtg.vt or bay.line.path.ds1)

bay {1 - upper}

line (range=1..4)

path (range=1..3)

vtg (range=1..7)

vt (range=1..4)(ds1) (range=1..3)(e1)

ds1 (range=1..28)

LineNum for T1/E1—(bay.line)

bay {1 - upper, 2 - lower}

line (range=1..24)

LineNum for T3—(bay.line.ds1)

bay {1 - upper, 2 - lower}

line (range=1..3)

ds1 (range=1..28)

Ds0GrpIndex—DS0 group index

T1: (range=0..23)

E1: (range=0..30)

Ds0BitMap—DS0 channel number

For trunking Service or DS0Xconn: single bit input

For H248: multiple bits input (1-24 or 1, 5, 10-20)

T1: 1,2,3,..24

E1: 1,2,3,..31

ServiceType—service type

For H.248 Protocol, 8 = Trunking, 9 = H248, 10 =DS0Xconn

For xGCP protocol, 8 = Trunking, 10 = DS0Xconn, 11 = xGCP

BulkProvisionNumber—bulk provisioning number

Single DS0 configuration (range=1..8064(O-C3)/1152(T1)/1488(E1))(default=1)

Multiple DS0 configuration (range=1..336(OC-3)/48(T1E1))(default=1)

Setting Up VXSM Connections

Creating a VXSM Resource Partition

Step 1 Use the **addrscprtn** command to create a resource partition for the VXSM card.

```
geteway1.5.VXSM.a > addrscprtn <ifNum> <partId> <ctrlrId> <egrminbw> <egrmaxbw> <ingminbw>
<ingmaxbw> <minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

For *ifNum*, enter 1 for port number. For *partId*, enter 1 for PNNI. For *cntrlid*, enter 2 for PNNI.

The remaining parameters are used to specify maximum and minimum values for vpi/vci, bandwidth, connections, etc., see the *Cisco VXSM Command Reference, Release 5.3* for details.

Creating Slave End Connection on RPM or AXSM Card

Step 2 **For RPM Configurations Only**

For each connection, specify the slave end on the RPM-XF card and the master end on the VXSM card.

a. On the RPM-XF card, enter the interface command

```
Router(config)#interface Switch1
```

b. On the RPM-XF card, enter the switch connection command to define the slave connection endpoint.

```
Router(config-subif)# switch connection vcc <localVPI> <localVCI> master remote raddr
<ATMaddr> <remoteVPI> <remoteVCI>
```

Omit the <ATMaddr> <remoteVPI> <remoteVCI> parameters

The following example creates a master connection for the PVC labeled VPI 0, VCI 2001:

```
Router(config-subif)#switch connection vcc 0 2001 master remote
```

c. After you create the slave connection endpoint, the RPM-XF enters the switch connection configuration mode and displays the following prompt:

```
Router(config-if-swconn)#
```

On the RPM-XF card configure the switch connection using the switch connection configuration commands.

```
Router(config-if-swconn)rmbs 1024

Router(config-if-swconn)rpcr 860000

Router(config-if-swconn)rscr 860000

Router(config-if-swconn)cpmm-id 9

Router(config-if-swconn)pcr 860000

Router(config-if-swconn)csr 860000
```

Note This is the only time that you can configure the switch connection. If you need to change the configuration later, delete the subinterface and recreate the connection.

d. To display the ATM address assigned to the slave connection, switch to the active PXM45 card and enter the **dspcon** command to display connection information. For example, if the RPM-XF is in slot 9

```
Router#cc 7

(session redirected)

dspcon 9.1.2.2 0 2000
Port                    Vpi Vci                              Owner      State
------------------------------------------------------------------------------
Local  9:-1.1:-1        0.2000                               SLAVE      FAIL
       Address: 47.00918100000000036b5e2bb2.000001074b01.00
Remote Routed           0.0                                  MASTER      --
       Address: 00.000000000000000000000000.000000000000.00

-------------------- Provisioning Parameters --------------------
Connection Type: VCC          Cast Type: Point-to-Point
Service Category: UBR         Conformance: UBR.1
Bearer Class: BCOB-X
Last Fail Cause: N/A                              Attempts: 0
Continuity Check: Disabled    Frame Discard: Disabled
L-Utils: 0     R-Utils: 0     Max Cost: 0     Routing Cost: 0
OAM Segment Ep: Enabled

---------- Traffic Parameters ----------
Tx PCR:  353208         Rx PCR:  353208
Tx CDV:  N/A            Rx CDV:  N/A
Tx CTD:  N/A            Rx CTD:  N/A
```

The slave endpoint ATM address appears below the *Local* port identification. Note this value because this is the address you need to enter when you create a master connection endpoint at the VXSM card. The connection state is FAIL because the master endpoint has not been created.

e. Repeat Step 2 until all the bearer (up to 8) and the one control slave ends have been configured.

Step 3 **For AXSM Configurations Only**

Create PVC connections between VXSM and AXSM.

For each connection, the user needs to specify the slave end on the AXSM card and the master end on the VXSM.

Log on to the AXSM and use the **addcon** command to configure the slave end point for establishing a PVC between the VXSM and AXSM. Repeat this command for up to 8 bearer PVCs and 1 control PVC

a. **addcon** <ifNum> <vpi> <vci> <service type> <mastership>

```
[-casttype <value>] [-slave <NSAP.vpi.vci>] [-lpcr <local PCR>] [-rpcr <remote PCR>]
[-lscr <local SCR>] [-rscr <remote SCR>] [-lmbs <local MBS>] [-rmbs <remote MBS>]
[-cdvt <local CDVT>] [-lcdv <local maxCDV>] [-rcdv <remote maxCDV>] [-lctd <local
maxCTD>] [-rctd <remote maxCTD>] [-cc <OAM
CC Cnfg>] [-stat <Stats Cnfg>] [-frame <frame discard>]
[-mc <maximum cost>] [-lputil <local util>] [-rputil <remote util>] [-slavepersflag
<slavepers>] [-rtngprio <routingPriority>] [-prefrte
<preferredRouteId>] [-directrte <directRoute>]
```

For ifNum specify 1 as the interface number. For VPI and VCI, specify values in the ranges 0 to 255 and 0 to 65535 respectively. For service type, specify 1 (constant bit rate).

For pvc type, specify 1 (AAL5) for a control connection or a bearer connection.

For appication specify 1 for a control connection or 2 for a bearer connection.

For mastership specify 2 for False (slave).

Omit the -slave parameter. The gateway will assign a value and display it as NSAP.VPI.VCI. The user should note the value and use it when adding the master end of the connection on the VXSM.

Of the remaining optional parameters, enter values or accept the defaults. See the CLI chapter for details.

b. Repeat Step 3 until all the bearer (up to 8) and the one control slave ends have been configured.

Creating Master End Connections on VXSM Card

Step 4 Log on to the VXSM card

a. Use the **addcon** command to configure the master end point for establishing a PVC between the VXSM and RPM or AXSM.

```
addcon <ifNum> <vpi> <vci> <serviceType> <pvcType> <application> <mastership>
[-slave <NSAP.vpi.vci>] [-lpcr <local PCR>] [-rpcr <remote PCR>] [-lscr <local SCR>]
[-rscr <remote PCR>] [-lmbs <local MBS>]...
```

For ifNum specify 1 as the interface number. For VPI and VCI, specify values in the ranges 0 to 255 and 0 to 65535 respectively. For service type, specify 1 (constant bit rate).

For pvc type, specify 1 (AAL5) for a control connection or a bearer connection.

For appication specify 1 for a control connection or 2 for a bearer connection.

For mastership specify 1 for True (master).

For the -slave parameter, enter the NSAP.VPI.VCI that was noted when configuring the slave end of the connection.

Of the remaining optional parameters, enter values or accept the defaults. These parameters are best set from the master end. See the VXSM Command Reference for details.

b. Repeat step 4 for each bearer and control PVC configured in the previous step (step 2 or step 3).

Note PVC connections must be configured such that Connection Admission Control (CAC) mastership/slave follows that of the Connection Mastership/Slave.

Assigning IP Addresses

Step 5 For each connection (control and bearer), there must be an IP address assigned.

a. Use the **addconip** command to assign IP addresses to the VXSM connections.

```
addconip<IpIndex><PortNum><Vpi><Vci><IpAddr>
<PrefixLength><defaultGwIp>
```

For IpIndex assign a number in the range 1 to 16. Usually the user would assign 1 to the first IP address being assigned, 2 for the next and so on.

For PortNum, enter the value of 1.

For VPI and VCI, enter the values for the connection for which an IP address is being assigned.

For IPAddr, assign an IP address for the connection.

For PrefixLength, enter the length of the IP prefix.

For DefaultGwIp, specify whether this is to be the default gateway. Enter 1 for yes, or 2 for no.

b. Repeat step 5 for each bearer and control connection that was configured in step 4.

Configuring MGC Interfaces for Call Control

Perform one of the following procedures below to configure the interface between the Media Gateway (MG) and the Media Gateway Controller (MGC). VXSM supports the ITU H.248 and the xGCP protocols, select the procedure that applies to you application.

For each protocol type, the procedure consists of two basic phases. The first phase sets up MGCs and MGC Groups. The second phase configures the protocol and protocol profile details that are used for the VXSM and the MGC to communicate.

Note XGCP is a generic term for a family of similar MGC protocols. The protocols in the family are:

Simple Gateway Controller Protocol (SGCP)
Media Gateway Controller Protocol (MGCP)
Trunking Gateway Controller Protocol (TGCP).

Gateways Using H.248 MGC Protocol

Setting Up H.248 MGCs and MGC Groups

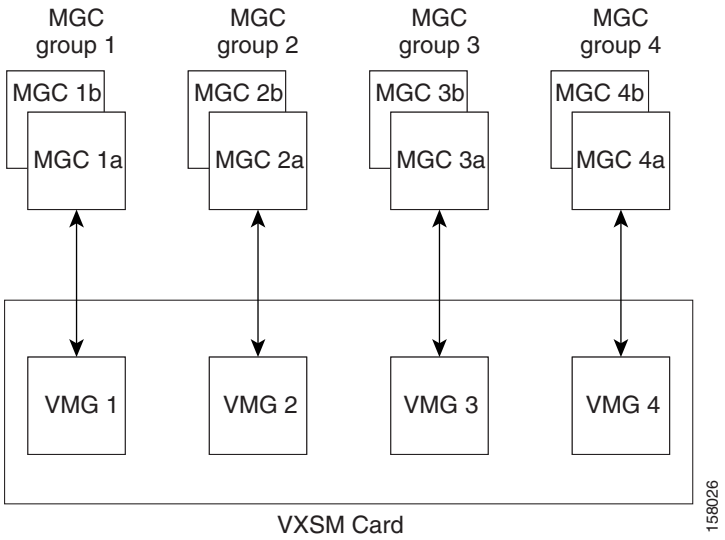
The following procedure establishes Media Gateway Controller and Media Gateway Controller Group identities, properties, and relationships. Because H.248 applications support up to 12 virtual media gateways (VGWs), this procedure supports the configuration of multiple MGC Groups associated with one physical VXSM board.

Step 1 Determine the number of VGWs, MGCs, and MGC Groups to be setup. Determine their relationships. The rules are:

- A VXSM card can have up to 12 VGWs (it must have at least one)
- There must one, and only one, associated MGC Group for each VGW
- Each MGC Group can up to 4 MGCs (it must have at least one)

Figure 3-3 shows a sample arrangement is which VXSM is partitioned into 4 virtual media gateways with 4 corresponding media gateway groups.

Figure 3-3 MGC, MGC Group, and VMG Arrangement—Example



Step 2 Provide a domain name for the MGC, and specify how it is to be resolved.

a. Use the **addmgcdn** command to add am MGC domain name.

addmgcdn *<MGC Index> <Domain Name>*

For MGC Index, enter an integer in the range 1 to 4 to identify the MGC within a group.

For Domain Name, enter and name up to 64 characters.

b. Use the **cnfmgc** command to specify the resolution method for the MGC domain name.

cnfmgc *<MGC Index> <Resolution>*

Note Use the **cnfmgc** command only if the MGC group is not already in an H.248 association (see later)

MGC Index specifies which MGC is being configured in the range of 1 to 4.

For Resolution, specify 1 for internal resolution or 2 for external (DNS) resolution.

If internal resolution is specified, use the **addmgcip** command to specify an IP address for domain resolution.

addmgcip <*MGC Index*> <*MGC IP Index*> <*MGC IP Address*> <*Preference*>

MGC Index specifies the MGX for which the IP address is being configured.

For MGC IP Index, enter a integer in the range 1 to 4 to uniquely identify the IP address.

For MGC IP Address, enter the IP address to be used for resolving domain names.

For Preference, enter an integer in the range 1 to 8 to indicate the order of preference of IP addresses for the MGC (1 is the highest).

If resolution is external is specified, use the **adddnsdn** command to specify the domain name of the server.

adddnsdn <*Domain Name*>

Step 3 Use to **addmgcgrpmgc** command to add the MGC to an MGC group. This command adds an MGC to an MGC Group identified by the MGC Group Index. If no such group exists, one is created.

The syntax for this command is:

addmgcgrpmgc *<MGC Group Index> <MGC Index> <Preference> <TCP/UDP Port>*

Where:

MGC Group Index—MGC group index (range=1..12)

MGC Index—MGC index (range=1..4). This identifies the MGC within the group.

Preference—Preference (range=1..4) (default=1)

TCP/UDP port—Port (range=1024..16383) (default=2944)

Note Specifying 0 (zero) as the value of this parameter means that there is no specific UDP port, in which case, the UDP port contained in the protocol table will be used.

Step 4 Repeat steps 2 and 3 for each MGC Group to be set up.

Configuring H.248 Protocol

Use this procedure it the VXSM is to communicate with the MGC(s) using the H.248 protocol

H.248 protocol configuration consists of:

- Adding an MGC protocol
- Configuring an association between a virtual gateway and a media gateway controller group
- Configuring a protocol (H.248) profile
- Configuring Switch Circuit Network (SCN) termination
- Configuring Packet Data Network (PDN) termination
- Bringing up the association

Step 1 Use the **addh248assoc** command to add an association of a VGW with an MGC group. The syntax for this command is:

addh248assoc <*GatewayLinkId*> <*MgcGroupIndex*> <*GatewayIpIndex*><*PortNumber*> <*TransportProtocol*><*MgHeaderAddrType*><*SrvChgProfile*><*SrvChgProfileVer*> <*MsgTokenType*> <*dynamicTpktVersion*><*maxCommandMsgSize*> <*maxReplyMsgSize*>

GatewayLinkId—The gateway link ID is an integer in the range 1 to 12. GatewayLinkId unique identifies the MG-MGC association or Virtual MG.

MgcGroupIndex—MGC group index (range=1..12)

GatewayIpIndex—gateway IP index (range=1..16)

PortNumber—gateway port number (range=1024..16383)

TransportProtocol—transport protocol {1 | 2 |3 | #}

1—tcp (default)

2—udp

3—sctp

#—default value

MgHeaderAddrType—MG header address type

{(range=1 to 16) | #=current value} (default=1)

SrvChgProfile—Profile name in ServiceChange message (16 chars)

(default=CISCO_TGW)

For example, CISCO_TGW, BT_TGW

SrvChgProfileVer—Profile version (range=1..99)(default=1)

MsgTokenType—Message Token Type {1 | 2 | #}

1—short (default)

2—long

#—default value

DynamicTpktVersion—This object specifies the TPKT header version that is dynamically assigned based on the size of the packet presented to TCP layer.

1 = Enabled

2 = Disabled

Note The **dsph248assoc** and **dsph248state** commands can be used to display the association parameters. The **cnfh248rootpkg** and **cnfh248delay** commands can be used to modify the association parameters. See the CLI chapter for details.

Step 2 Use the **cnfh248param** command to configure H.248 protocol related parameters.

cnfh248param <*GatewayLinkId*> <*RespRetentionTime*> <*InitialRtt*> <*InactivityTime*>
GatewayLinkId—The gateway link ID is an integer in the range 1 to 12. GatewayLinkId unique identifies the MG-MGC association or Virtual MG.

RespRetentionTime—Specifies the time in seconds that an H.248 transaction response should be retained before being sent if the gateway receives a repetition of an H.248 transaction that is still being executed.

The value for this parameter is a number in the range from 0 – 65535, with a default value of 30.

InitialRtt—Defines the initial round-trip time in milliseconds for the response to an H.248 transaction. In effect, this parameters reflects the network delay time.

The value for this parameter is a number in the range from 0 – 65535, with a default value of 1000

InactivityTime—Specifies the allowable period of silence in milliseconds between messages from the media gateway controller (MGC) to the media gateway.

The value for this parameter is a number in the range from 0 – 65535, with a default value of 1000.

Step 3 Use the **cnfh248mg** command to configure the H.248 protocol. This command is used to modify the gateway port to be used for the VMG.

cnfh248mg *<gatewayLinkId> <portNumber>*

GatewayLinkId—Gateway link ID is an integer in the range 1 to 12. GatewayLinkId unique identifies the MG-MGC association or Virtual MG.

For portNumber, this parameter is the TCP/UDP port number that the MGC uses to communicate with the MG.

The permissible value of this parameter is an integer in the range from 1024 – 16383.

Step 4 Use the **addh248prof** command to add an H.248 profile.

An H.248 profile contains a set of configurations consisting of SCN and PDN termination types. Each profile is identified by a profile ID (ID = 0 is the default).

addh248prof *<Index>*

Index -- profile index (range=1..25)

Step 5 If an H.248 name schema for terminations is to be used, it should be configured now and before any terminations are added.

Use the cnfh248nameschema command to configure the name schema. The configuration consists of enabling/ disabling the name schema feature and, if enabled, specifying prefix names for DS, RTP, and AAL2/SVC termination types.

cnfh248nameschema <*DescriptiveName> <DsNamePrefix> <RtpNamePrefix>*

DescriptiveName is a parameter that specifies whether the media gateway is to support the descriptive suffix of the name schema for H.248 terminations in the media gateway.

The permissible values of this parameter are:

- *1*—Enables the descriptive name suffix for the termination.
- *2*—Disables the descriptive name suffix (default value) for the termination.

The parameters DsNamePrefix, RtpNamePrefix are characters strings (length depends upon card type) specifying the prefixes for DS, RTP, AAL1/PVC, and AAL2/PVC respectively.

The default values for these prefixes are DS, RTP, AAL1/PVC, and AAL2/PVC respectively.

Step 6 Configure the terminations for the switch circuit network (SCN) side of VXSM. It is this step that links the VIFs to the H.248 profiles

a. Check that the **addvif** command has already been executed to add a DS0 group. If not, use the **addvif** command to create a DS0 group.

b. Use the **cnfvifterm** command to configure SCN terminations.

The syntax for this command is:

cnfvifterm *<LineNum> <Ds0GrpIndex> <GatewayLinkId> <H248PkgIds><ProfileIndex> <Repetition>*
Where:

LineNum for OC-3—(bay.line.path.vtg.vt or bay.line.path.ds1)

bay {1 - upper}

line (range=1..4)

path (range=1..3)

vtg (range=1..7)

vt (range=1..4)(ds1) (range=1..3)(e1)

ds1 (range=1..28)

LineNum for T1/E1—(bay.line)

bay {1 - upper, 2 - lower}

line (range=1..24)

LineNum for T3—(bay.line.ds1)

bay {1 - upper, 2 - lower}

line (range=1..3)

ds1 (range=1..28)

Ds0GrpIndex—DS0 group index

T1: (range=0..23)

E1: (range=0..30)

GatewayLinkId—Gateway link ID an integer in the range 1 to 12. GatewayLinkId unique identifies the MG-MGC association or Virtual MG.

H248PkgIds—H248 package IDs {(multiple IDs) | #=current value}

0 - G
4 - DG
5 - DD
6 - CG
8 - CT
11 - TDMC
12 - AN
13 - BCG
15 - SrvTn
19 - Lltr
20 - BCAS
21 - RBS
22 - OSES
23 - AMET
24 - BCASAddr
25 - CASB
26 - GRI
31 - EriTermInfo
33 - CTYP

- current packagesProfileIndex—profile index

(range=0..25)(default=0)

- current value}

Repetition—bulk provisioning number

Single DS0 configuration (range=1..8064(OC-3)/1152(T1)/1488(E1)/4032 (T3). (default=1)

Multiple DS0 configuration (range=1..336(OC-3)/48(T1E1))/168 (T3))(default=1)

Step 7 Configure the terminations for the packet data network (PDN) side of VXSM

Use the **addtermtype -rtp** command to add an RTP terminal type.

The syntax for this command is:

addtermtype -rtp *<termTypeId> <termTypePkgIds> <termTypeProfileId>*

termTypeId is a unique identifier in the range of 2 to 3.

For termTypePkgIds, enter a 6 hexadecimal value (representing a 3-byte bitmap) to specify the packages to be supported.The supported packages are:

pkgG	(0)–Generic
pkgDG	(4)–Basic DTMF (Dual Tone Multi-Frequency) generator
pkgCG	(6)–Call progress tones generator
pkgNT	(9)–Network
pkgRTP	(10)–RTP (Real-time Transport Protocol)
pkgAN	(12)–Generic announcement
pkgSrvTn	(15)–Basic services tones generation
pkgLltr	(19)–

Step 8 When the H.248l profile has been created, it can be further configured using one or any of the following commands. The details of these commands are included in Chapter 6. Use the relevant configure H.248 commands one at a time to configure the parameter values.
These commands are shown in Table 3-2.

Step 9 Use the **cnfh248is** command to bring the MG to MGC H.248 link into service.

cnfh248is <*GatewayLinkId*>

GatewayLinkId—Gateway link ID is an integer in the range 1 to 12. GatewayLinkId unique identifies the MG-MGC association or Virtual MG.

Table 3-2 Configure H.248 Commands

Command	Parameter(s)	Default
cnfh248delay	Configures various retry and delay parameters.	
	• gateway link ID	• -
	• number of retries (0 - 100)	• 11
	• max. waiting delay (0 - 600000)	• 3000ms
	• restart delay (0 - 600ms)	• 60ms
cnfh248oos	Configures the gateway to out-of-service	
	• gateway link ID	• -
	• gateway shutdown type	• forced

Step 10 Use the relevant display commands (for example, **dsph248rootpkg**) to check for the correct parameter values.

Configuring MGC H.248 Profile

An H.248 profile is a set of parameter values that can be applied (as a set) to SCN terminations and PDN termination types. The parameters are applied by specifying the particular profile when SCNs and PDNs are created using the **cnfvifterm** and **addtermtype** commands (see Chapter 3). When the VXSM is operating in VoIP switching mode, the H.248 profile that is selected largely determines the processing that the DSPs perform on the voice payload.

To create and configure an H.248 profile, perform the following steps.

Step 1 If the profile has not already been created, use the **addh248prof** command to create the profile and assign it an ID (between 1 and 25).

```
addh248prof <profileIndex>
```

Step 2 Use the **dsph248prof** command to display the parameter values of the profile to be configured.

Step 3 Determine which parameters need to be modified.

Step 4 Use the relevant configure H.248 commands in sequence to modify the parameter values. These commands are shown in Table 3-3.

Table 3-3 Configure H.248 Profile Commands

Command	Parameter(s)	Default
cnfh248profcot -term	Configure continuity test parameters • profileIndex • RespondMethod	 • - • 1
cnfh248profcot -orig	• profileIndex • Duration • TxFrequency • RxFrequency	• - • 500 • 2010 • 2010.
cnfh248profcptone	Configure CP tones • profileIndex • [InterCPToneDuration] • [DetectLongCPToneDuration]	 • - • 60 • *70000*.
cnfh248profdtmf	Configure DTMF tones • profileIndex • DigitOnDuration • DtmfPauseDuration • DetectLongDigitDuration • SuppressBearerDigit	 • - • 100 • 100 • 1000 • 2.
cnfh248profec	Configure echo cancelation parameters • profileIndex • [EchoCancelEnabled] • [EchoCancelTail]	 • - • true • 128ms
cnfh248profgainattn	Configure gain/attenuation parameters • profileIndex • InGainControl • OutAttnControl	 • - • *0* dB • *0* dB.

Table 3-3 Configure H.248 Profile Commands (continued)

Command	Parameter(s)	Default
cnfh248profvad	Configure voice activity detection parameters	
	• profileIndex	• -
	• VoIpVad	• *1 (enable)*
	• VoIpVadTimer	• *250*
cnfh248rootpkg	Configure root package parameters	
	• gatewayLinkId	• -
	• maxContexts	• *8064/1488*
	• maxTermsPerContext	• *2*
	• mgExecTime	• *5000*.
	• mgcExecTime	• *5000*.
	• provisionRspTime	• *2000*.

ConfiguringH.248 Congestion and Overload

To configure Congestion and Overload Thresholds, perform the following steps.

Step 1 Use the **cnfrmrsrc** command to configure the CPU interval or the CPU threshold for the call admission control (CAC) processing resource in the media gateway, the format of this command is:

cnfrmrsrc -interval <*rsrc_id*> **-interval** <*ResourceInterval*>

For *rsrc_id* (resource identifier), enter the number 2 for cpuAvg, 12 for CPS, and 14 (call setup delay).

For *interval* (resource interval), enter an interval, in seconds, in the range or 10 to 300

Step 2 The previous step can be verified by executing the **dsprmrsrc** command.

To configure H.248 Congestion Control, perform the following steps.

Step 1 Use the **cnfcrrparam** command to enable the congestion control feature. The format of this command is:

cnfcrrparam <*enable*> <*interval*>

For *enable*, enter 1. The H.248 congestion package is enabled and call reduce functions for the VXSM card are activated.

For *interval*, enter an interval value in the range from 0 – 100 milliseconds, with a default value of 0.

This parameter defines the call renotification interval (in seconds) for the VXSM card to notify the media gateway controller (MGC) of a congestion condition in the gateway. In the event of congestion, the media gateway generates an event notification to the MGC, requesting a percentage reduction in the rate of calls that the MGC attempts to make to the gateway.

A default value of 0 for this parameter means that the media gateway controller (MGC) does not require renotifications.

Step 2 The previous step can be verified by executing the **dspcrrparam** command.

To configure H.248 Overload Control, perform the following steps.

Step 3 Use the **cnfovrldparam** command to enable H.248 overload control, the format of this command is:

cnfovrldparam <*overloadEnable*>

For *overloadEnable*, enter a value of 1 to enable the overload feature.

Step 4 The previous step can be verified by executing the **dspovrldparam** command.

Gateways Using XGCP MGC Protocol

This section refers to the generic protocol name of XGCP (or xGCP), note that in VXSM Release 5.3 the protocols supported in this generic family are MGCP and TGCP.

Setting Up XGCP Media Gateway Controllers and Media Gateway Controller Groups

The following procedure establishes Media Gateway Controller and Media Gateway Controller Group identities and properties. It also configures MGC and MGC Group relationships.

Step 1 Provide a domain name for the MGC, and specify how it is to be resolved.

a. Use the **addmgcdn** command to add a MGC domain name. Repeat for each MGC.

addmgcdn *<MGC Index> <Domain Name>*

For *MgcIndex*, enter an integer in the range 1 to 4 to identify the MGC.

For *DomainName*, enter and name up to 64 characters.

b. Use the **cnfmgc** command to specify the resolution method for the MGC domain name. Repeat for each MGC.

cnfmgc *<MGC Index> <Resolution>*

MGC Index specifies which MGC is being configured in the range of 1 to 4.

For Resolution, specify 1 for internal resolution or 2 for external (DNS) resolution.

c. If internal resolution is specified, use the **addmgcip** command to specify an IP address for domain resolution.

addmgcip <MGC Index> <MGC IP Index> <MGC IP Address> <Preference>

MGC Index specifies the MGX for which the IP address is being configured.

For MGC IP Index, enter a integer in the range 1 to 4 to uniquely identify the IP address.

For MGC IP Address, enter the IP address to be used for resolving domain names.

For Preference, enter an integer in the range 1 to 8 to indicate the order of preference of IP addresses for the MGC (1 is the highest).

d. If external resolution is specified, use the **adddnsdn** command to add a Domain Name Server (DNS) domain name and the **adddnssrver** command to add a DNS IP address. The format of these command is:

adddnsdn <domain name>
adddnssrvr <index><ipaddr>

Step 2 Use the **addmgcgrpmgc** command to add an MGC to an MGC group. Repeat for each MGC to be included in the group.

The syntax for this command is:

addmgcgrpmgc *<MGC Group Index> <MGC Index> <Preference> <TCP/UDP Port>*

MGC Group Index—MGC group index (range=1..12)

MGC Index—MGC index (range=1..4)

Preference—Preference (range=1..4) (default=1)

TCP/UDP port—Port (range=1024..16383) (default=2944)

Step 3 Use the **cnfxgcpmgcgrp** command to configure an MGC group.

The syntax for this command is:

cnfxgcpmgcgrp*<MgcgroupNumber>*

MgcGroupNumber specifies which MGC Redundant Group will be used in XGCP. An integer in the range 0 to 12.

Two conditions exist for an MGC group:

1. At least one MGC is associated with the MGC group
2. At least one protocol is associated with the MGC group

XGCP Protocol Configuration

When an MGC is created, the XGCP protocol can be configured using one or any of the following commands (Table 3-4). The details of these commands are included in Chapter 6. Each of the commands has an equivalent display command for displaying the current parameter values.

Table 3-4 Configure Call Control Protocol Commands

Command	Parameters	Default
cnfxgcpretry	Configure retry parameters for the call control protocol	
	• CmdTimeout	• 500ms
	• MaxExpTimeout	• 4000ms
cnfxgcpsdp	Configure session descriptor parameters for the call control protocol	
	• SimpleSdp	• 2 (disabled)
	• UndottedNotation	• 2 (disabled)
	• AckSdp	• 2 (disabled)
cnfxgcpldtmr	• LongDurationTimer	• 3600)

Table 3-4 Configure Call Control Protocol Commands (continued)

Command	Parameters	Default
cnfxgcpgwprof	• ProfileIndex	• 0
cnfxgcprsip	• Connection OOS RSIP behavior	• 1 - Send DLCX
cnfxgcpquarantine	Configure quarantined persistent event handling for the call control protocol	
	• QuarantineProcess	• 1 (Discard0
	• QuarantineLoop	• 2 (Step)
	• QuarantinePersist	• 2 (Disable)
cnfxgcpmgs	Configure message parameters for the call control protocol	
	• profileIndex	• -
	• TcritTimeout	• *4*
	• TparTimeout	• *16*
cnfxgcpdtmf	Configure DTMF relay parameters for the call control protocol	
	• DtmfRelay	• 1 (Enable)
cnfxgcpprofdtmf	• ProfileIndex	
	• SuppressBearerDigit	• 2 (Disable)

Configuring an MGC XGCP Profile

An xGCP call control profile contains the call control information that an MGC uses to establish a call. A call control profile contains information such as call agent details (address, port, type, and so on), retry parameters and timeout values.

A voice interface (DS0 group in TDM side) can be associated with a call control profile, in which case all the calls set up in the voice interface will use the call control parameters from the profile.

The following procedure configures a call control profile.

Step 1 Use the **addxgcpprof** command to establish a call control profile.
The command has the following syntax:

addxgcpprof *<ProfileIndex><profileName>*

ProfileIndex uniquely identifies the call control profile. An integer in the range 1 to 30.

profileName is a unique name for the profile. Profile name is a character string of 1 to 30 characters.

Once the profile name is configured it cannot be modified. If a user wants to modify the name. The original profile has to be deleted and another profile created with the new designated name.

Step 2 When the call control profile has been created, it can be further configured using one or any of the following commands. The details of these commands are included in Chapter 6.

Each of the commands listed in Table 3-5 has an equivalent display command for displaying the current parameter values.

Table 3-5 Configure Call Control Profile Commands

Command	Parameters	Default
cnfxgcpprofretry	Configure retry parameters for the call control profile • profileIndex • DnsLookupMax1 • RetryMax1 • DnsLoopupMax2 • RetryMax2	 • • - • 1 • 5 • 1 • 7
cnfxgcpprofttone	Configure tone timer parameters for the call control profileIndex • ProfileIndex • MwiTimeout • RtTimeout • RbkTimeout • CgTimeout • BzTimeout • DlTimeout • S1Timeout • RgTimeout • RoTimeout	 • - • 16 • 180 • 180 • 180 • 30 • *16* • 16 • 180 • 30
cnfxgcpproftsmax	Configure retransmission removal timer parameters for the call control profileIndex • ProfileIndex • TsMaxTimeout	 • - • 20
cnfxgcpprofthist	Configure this timer parameters for the call control profileIndex • ProfileIndex • ThistTimeout	 • - • 30
cnfxgcpproftd	• Configure disconnect timers parameters for the call control profileIndex profileIndex • ProfileIndex • TdinitTimeout • TdminTimeout • TdmaxTimeout	 • - • 15 • 15 • 600

Table 3-5 Configure Call Control Profile Commands (continued)

Command	Parameters	Default
cnfxgcpproftdmap	Configure digit map timers parameters for the call control profileIndex	
	• profileIndex	• -
	• TcritTimeout	• *4*
	• TparTimeout	• *16*
cnfxgcpprofcot	Configure COT timers parameters for the call control profileIndex	
	• *P*rofileIndex	• -
	• Cot1Timer	• *3*
	• Cot2Timer	• *3*

Configuring CALEA

The VXSM card can be ordered with a firmware image that has the CALEA feature either enabled or disabled. Further, the CALEA features function only in switching VoIP mode using TGCP as the media gateway control protocol.

Step 1 Check that the CALEA version of the firmware is ordered and installed. Execute the **dspcalea** command.

If the response is Unknown Command, the CALEA version is not installed and the feature does not function. If the CALEA version is installed, the **dspcalea** command shows whether the feature is enabled or disabled.

Step 2 If the CALEA version of the firmware is installed but is disabled, use the **cnfcalea** to enable the CALEA feature.

Other CALEA commands are:

dspxgcpcalea, this command displays the current status of the CALEA feature (enabled or disabled).

dspxgcpcaleacalls, this command displays details of calls subject to CALEA surveillance.

Configuring MGC Redundancy

MGCs configured in an MGC group form a set of redundant MGCs (up to a maximum of 4). The order in which MGCs are added to the group is the order of preference for selecting the MGC to use. Besides having up to 4 MGCs in a group, each MGC can have up to 4 IP addresses.

The procedure used by VXSM for selecting an MGC is as follows:

1. VXSM selects the MGC that was first added to the group and uses the highest preference IP address to communicate with the MGC.
2. If the communication fails, VXSM retries a number of times determined by the value of the xgcpretry parameter.

3. If communication still fails after the retries, VXSM repeats the attempts with the next highest preference IP address.
4. If this IP address fails, the next address is attempted, this process continues until all IP addresses are exhausted.
5. If none of the IP addresses are able to communicate with the MGC, VXSM repeats the whole process with the second MGC to be added to the MGC group.
6. The process continues using the remaining MGCs to establish a connection.

To configure MGC redundancy perform the following steps.

Step 1 Use the **addmgcdn** (H.248) command to create an MGC. Create an MGC for each one to be included in the redundant group. Configure them in the order of preference. The first one configured will be the first one used for an MGC. If the first one fails, the second MGC to be configured will be attempted, and so on to a maximum of four.

Step 2 Use the **addmgcip** to specify the IP address or addresses for each MGC.

Note MGCs can be provided with up to four IP address. They should be configured in order of preference. The first address will be tried first, if it fails, the second is attempted, and so on up to four IP addresses.

Step 3 Use the **addmgcgrpmgc** command to add the MGCs to the MGC group. This command also contains the MGC preference parameter.

Configuring Backhaul

In switching applications, VXSM is able to extract layer 3 signaling frames from a TDM signaling channels and backhaul them to the media gateway controller for processing (this feature is described in Chapter 2).

When backhauling is employed, two distinct communication channels exist between the media gateway and the media gateway controller. The first is used for the normal call control functions and the second is used for backhauling.

Configuration of a backhauling channel consists of the following major steps:

Step 1 Establishing a communication link between the VXSM and the media gateway controller. This communication link can is based upon a RUDP (Reliable UDP) session set or RTCP.

Step 2 Establishing communication link between VXSM and the voice TDM network. This link can be configured for ISDN Q.931 or DPNSS

Configuring the MGC Link

Two configuration procedures, one for RUDP and one for SCTP/DUA, follow. Only one procedure can be used for any media gateway or virtual media gateway. Select the appropriate procedure for the gateway being configured.

Configuring RUDP (for PRI only)

To configure an RUDP session between VXSM and the media gateway controller, perform the following steps.

Step 1 Establish IP connectivity with the media gateway controllers (see Chapter 2 for details).

Step 2 Use the **addsesset** command to create a session set.

```
addsesset <set number> <fault tolerant>
```

set number
Integer value of 1 (currently only session set is supported)

fault tolerant
Integer value
1 = fault tolerant
2 = non-fault tolerant

Step 3 Use the **adddnsdn** command to add the domain server domain name

```
adddnsdn <Domain Name>
```

Step 4 Use the **adddnssrvrip** command to add the IP address of the domain server

```
adddnssrvrip 1 172.29.66.35
```

Step 5 Use the **addmgcdn** command to ass the domain name of the media gateway controller

```
addmgcdn 1 mgc7
```

Step 6 Use the **addsesgrp** command to create each session group

```
addsesgrp <group number> <set number> <mgcname>
```

group number
Integer value of 1 or 2 (specify 1 for non-fault tolerant mode or 2 for fault tolerant mode).

set number
Integer value of 1(only 1 is supported)

mgcname
Domain name of the call agent (a text string of 1-64 characters.

Step 7 Use the **addses** command to create each RUDP session. Each session group can have up to four sessions.

```
addses <session number> <group number> <priority> <local port> <remote port>
```

session number
Integer value (1 to 8)

group number
Integer value (1 or 2)

priority
Integer value in the range of 1 to 4. A lower number means higher priority.

local port
Integer value in the range of 1124 to 65535

remote port
Integer value in the range of 1124 to 65535

Step 8 For each session that has been created, the session parameters can be further configured using the commands in Table 3-6 (see VXSM Command Reference for CLI details).

Table 3-6 RUDP Session Commands

Command	Configures …
cnfsesport	The local port/remote port values. The <local port, remote port and Remote IP address> combination must be unique across the group.
cnfsesmaxwindow	The maximum number of segments that can be sent without getting an acknowledgement for a specific RUDP session.
cnfsessyncatmpts	The maximum number of attempts to synchronize with MGC for a specific RUDP session.
cnfsesmaxseg	The maximum number of octets to synchronize with VSC for a specific RUDP session.
cnfsesmaxreset	The maximum number of auto resets performed before a connection is reset.
cnfsesretrans	The timeout value for retransmission of unacknowledged packets in millisecondes and the maximum number of times consecutive retransmission is attempted before the connection is considered broken.
cnfsesack	The timeout value to send out an acknowledgment and the maximum number of acknowledgments that will be accumulated before sending an acknowledgment.
cnfsesoutofseq	The maximum number of out of sequence packets that will be accumulated before sending an EACK segment is sent. A value of 0 indicates an DACK is sent immediately if an out of order segment is received.
cnfsesnullsegtmout	The number of milliseconds of idle time before sending a null segment.
cnfsesstatetmout	The number of milliseconds of idle time before sending a null segment.

Configuring H.248 over SCTP (for PRI and DPNSS)

To configure an SCTP session between a VXSM virtual gateway and the media gateway controller, perform the following steps.

Step 1 Establish IP connectivity with the media gateway controller(s) (see Chapter 2 for details).

Step 2 Use the **addh248assoc** command to add an association of a VGW with an MGC Group. Make sure to specify the gateway to MGC transport protocol as **sctp** (<*TransportProtocol*> =3).

The syntax for this command is:

addh248assoc <*GatewayLinkId*> <*MgcGroupIndex*> <*GatewayIpIndex*><*PortNumber*> <*TransportProtocol*><*MgHeaderAddrType*><*SrvChgProfile*><*SrvChgProfileVer*> <*MsgTokenType*> <*dynamicTpktVersion*><*maxCommandMsgSize*> <*maxReplyMsgSize*>

- GatewayLinkId—An integer in the range 1 to 12. GatewayLinkId unique identifies the MG-MGC association or Virtual MG.
- MgcGroupIndex—MGC group index (range=1..12)
- GatewayIpIndex—gateway IP index (range=1..16)
- PortNumber—gateway port number (range=1024..16383)
- TransportProtocol—transport protocol {1 | 2 |3 | #}
  - 1—tcp (default)
  - 2—udp
  - 3—sctp
  - #—default value
- MgHeaderAddrType—MG header address type

  {(range=1 to 16) | #=current value} (default=1)
- SrvChgProfile—Profile name in service change message (16 characters)

  (default=CISCO_TGW)

  For example, CISCO_TGW, BT_TGW
- SrvChgProfileVer—Profile version (range=1..99)(default=1)
- MsgTokenType—Message Token Type {1 | 2 | #}
  - 1—short (default)
  - 2—long
  - #—default value
- DynamicTpktVersion—Specifies the TPKT header version that is dynamically assigned based on the size of the packet presented to TCP layer.

  1 = Enabled

  2 = Disabled

Step 3 Use the **cnfh248sctpparams** command to configure the SCTP parameters. The format is:

cnfh248sctpparams <*SctpIdx*>[-**rto** <*InitRto*>][-**ret** <*MaxInitRetrans*>]
[-**minrto** <*MinRto*>][-**maxrto** <*MaxRto*>][-**asret** <*MaxAssocRetrans*>]
[-**ipalive** <*IPKeepalive*>][-**ipret** <*IPPathRetrans*>][-**tos** <*TOS*>][-**instr** <*InStreams*>]
[-**outstr** <*OutStreams*>]

For *SctpIdx*—Enter an SCTP config index number. An integer in the range of 1 to 12.

Enter the following optional parameters as necessary.

For -**rto** <*InitRto*>—Enter a maximum initial retransmit timeout in the range of 2000 to 20000 ms. (default=3000)

For -**ret** <*MaxInitRetrans*>—Enter a max initial retransmit in the range of 1 to10) (default=8)

For -**minrto** <*MinRto*>—Enter a min retransmit timeout in the range of 300 to 60000ms (default=300)

For -**maxrto** <*MaxRto*>—Enter a max retransmit timeout in the range of 300 to 60000ms. (default=900)

For -**asret** <*MaxAssocRetrans*>—Enter a max association retransmit in the range of 2 to 20. (default=5)

For -**ipalive** <*IPKeepalive*>—Enter a heart beat interval in the range of 500 to 60000ms. (default=3000)

For -**ipret** <*IPPathRetrans*>—Enter the IP path retransmit in the range of 2000 to 20000ms(range=2..10) (default=3)

For -**tos** <*TOS*>—Enter the IP precedence level for PDUs in the range of 0 to 255) (default=0)

For -**instr** <*InStreams*>—Enter the number of inbound streams for negotiation in the range of 1 to 336) (default=1)

For -**outstr** <*OutStreams*>—Enter the number of outbound streams for negotiation in the range of 1 to 336) (default=1)

Configuring the TDM Network Link

Two configuration procedures, one for ISDN layer 2 (LAPD) and one for DPNSS, follow. Only one procedure can be used for any media gateway or virtual media gateway. Select the appropriate procedure for the gateway being configured.

Configuring LAPD

To configure LAPD parameters for a DS0 used for ISDN D channel, perform the following steps.

Step 1 Use the **addlapd** command to create an LAPD session on a specified DS0.

```
addlapd <bay.line.path.vtg.vt:ds0>|<bay.line.path.ds1:ds0>|<bay.line>:<ds0>[-side
<LAPDside>][-type <Type>][-window <WindowSize>]{-n200<n200>}[-t200 <Timer200>][-t203
<Timer203>][-ds0 <Ds0Format>][-profile <IsdnHdlcProfile>][-as <AS Name>][-appltype
<AppType>]
```

OC-3/SDH	bay.line.path.vtg.vt:ds0 or bay.line.path.ds1:ds0	bay {1 - upper} line (range=1..4) path (range=1..3) vtg (range=1..7) vt (range=1..4)(ds1) (range=1..3)(e1) ds1 (range=1..28) ds0 (range= 1..24 for T1 1..31 for E1)
T1/E1	bay.line:ds0	bay {1 - upper, 2 - lower} line (range=1..24) ds0 (range= 1..24 for T1 1..31 for E1
T3	bay.line.ds1:ds0	bay {1 - upper, 2 - lower} line (range=1..3) ds1 (range=1..28) ds0 (range= 1..24 for T1 1..31 for E1

side <LAPDsid>

Specify whether the LAPD stack is at user side or network side

1 - network

2 - user

-type <Type>

Specify the switch type at the remote end of the ISDN line.

1 - CCITT

3 - AT&T 5ESS PRA

4 - AT&T 4ESS

6 - NT dms100 PRA

7 - VN 2 or VN 3

8 - INS Net

9 - tr6 MPC

10 - tr6 PBX

12 - Austel Primary

13 - National ISDN-1

14 - ETSI

15 - NT dms250

16 - Bellcore

17 - National ISDN-2

-window <WindowSize>

Specify the maximum number of sequentially numbered I-frames that may be outstanding

1..128 (default=7)

-n200 <n200>

Specify the maximum number of retransmissions of a frame

1..10 (default=3)

-t200 <Timer200>

Specify the maximum time to wait for acknowledgment of a transmit frame

100..1023000 ms (default=1000)

-t203 <Timer203>

Specify the maximum time in milliseconds allowed without frames being exchanged. This value should be greater than that for -t200

100..1023000 ms (default=1000)

-ds0 <Ds0Format>

Specify the DS0 format. 56k(1) is robbed-bit for T1.

1—ds056k

2—ds064k}

-profile <IsdnHdlcProfile>

Specify the HDLC profile which contains a list of HDLC attributes for the PRI backhaul connection

1..128

-as <AS Name>

Specify the LAPD application server (AS) name. An AS is a logical entity serving LAPD D-channel.Zero length string (size 0) means there is no AS association with this LAPD D-channel

255 chars. This parameter is used for PRI backhaul using SCTP only and is not configurable for RUDP.

-appltype <AppType>

Specify the PRI backhaul application protocols as 1 or 2.

1 = sctp

2 = rudp

Step 2 When an LAPD session has been created, the session parameters can be further configured using the following commands (see Chapter 6 for CLI details).

Table 3-7 LAPD Session Commands

Command	Function
cnflapd	Modify an existing Lapd entry. The applType can not be modified in this command. The line must be deleted and then added back again to change the applType.
dsplapdcnt	Display LAPD statistics counters
dsplapdhdlccnt	Display LAPD HDLC statistics counters

Configuring DPNSS

To configure a DPNSS channel, perform the following steps.

Step 1 Create an level 2 application server using the addl2as command.

addl2as <*AS Index*> <*AS Name*> <*Primary IP*> [**-ip2** <*Secondary IP*>]
[-**port** <*SCTP Port*>]

For *ASIndex, AsName,* and *PrimaryIP* provide a index number, an application server name, and an IP address for the AS.

For -**ip2**<*SecondaryIP*>, the user can provide an optional secondary IP address.

For -**port**<*SCTP Port*> assign an port number for use at the SCTP level. If not specified, the default value of 9900 is used.

Note Up to 12 application servers can be added for each virtual media gateway.

Step 2 Create a level 2 application server process using the addl2asp command.

addl2asp <*ASP Index***> <***ASP Name***> <***Primary IP***> <***ASP AS Name***>**
[-ip2 <*Secondary IP***>][-port <***SCTP Port***>]**

Specify the index, ASP name, primary IP and (if specified) the -ip2 and -port values. For ASP AS Name, enter an Application Server Process Application Server name.

Note Up to 2 application server processes can be added for each application server.

Step 3 Configure an IAU application server process IP address, using the cnf2laspip command.

cnfl2aspip <*ASP Index***> <***IP Type***> <***ASP IP***> [-pre <***IP Precedence***>][-alive <***Keep Alive***>][-prtx <***Retrans***>][-flag <***IP HB Flag***>]**

For *ASP Index*, use the value created in step 3.

IP Type should be 1 for ipv-4

For *ASP IP*, enter an IP address for the application server process.

For -**pre**<*IP Precedence*>, enter a value in the range of 1 to 7. The default value is 0 and entering a value of -1 will disable this parameter (in which case, SCTP will determine the service type).

For **-alive, -prtx**, and **-flag**, these are optional parameters. See the cnfl2aspip command in the VXSM Command Reference, Release 5.3.

Note Once the AS, and the ASP have been added, they can be modified using the cnfl2as, cnfl2asp, and cnfl2aspip commands

Step 4 To create a DPNSS entry, use the

adddpnss <*ifIndex*> <*SigSystemType*> [-**as** <*AsName*>][-**ps** <*PbxSide*>][-**hp** <*HdlcProfile*>][-**ft** <*L2FrameTimer*>][-**tft** <*TestFrameTimer*>][-**rmc** <*RetryMaxCnt*>]

For *ifIndex*, use the format appropriate to the VXSM card being configured.

OC3/SDH	bay.line.path.vtg.vt:ds0 or bay.line.path.ds1:ds0	bay {1 - upper} line (range=1..4) path (range=1..3) vtg (range=1..7) vt (range=1..4)(ds1) (range=1..3)(e1) ds1 (range=1..28) ds0 (range= 1..24 for T1 1..31 for E1)
T1/E1	bay.line:ds0	bay {1 - upper, 2 - lower} line (range=1..24) ds0 (range= 1..24 for T1 1..31 for E1

Only E1 is supported.

For *SigSystemType* - enter the Signaling System Type

1 - dpnss
2 - dass

For -**as** <*AsName*> enter the DPNSS application server name, a character string of up to 12 characters.

For -**ps** <*PbxSide*> enter which pbx side is being configured

1 - pbxA, only applicable with DPNSS trunk

2 - pbxB, only applicable with DPNSS trunk

3 - et, only applicable with DASS trunk

4 - pbx, only applicable with DASS trunk

For -**hp** <*HdlcProfile*> enter the HDLC profile number, an integer in the range of 1 to 128. (default=1)

For -**ft** <*L2FrameTimer*> enter the layer 2 frame timer in the range of 50 to 10000 ms) (default=500) This parameter is the timer value at the expiry of which the DPNSS/DASS layer 2 frame would need to be retransmitted if unacknowledged.

For -**tft** <*TestFrameTimer*> enter the test frame timer in the range of 0 to 60 minutes (default=5)

A value 0 indicates test frame timer is disable

For -**rmc** <*RetryMaxCnt*>] enter the number of retransmissions of a command frame which must take place from the media gateway if the correct acknowledgement is not received from the PBX/PSTN. An integer in the range of 0 to 64.(default=4)

Step 5 The previous step can be verified by executing either the **dspdpnss** or **dspdpnsss** command.

Step 6 Repeat steps 1 and 2 for each DPNSS channel to be created.

Configuring E911 Emergency Services

Configuration of the E911 feature consists of the following tasks:

- Setting up a CAS variant file for use with the MGC protocol
- Modify the line signal values (if required)
- Setting up CAS general configuration parameters (if required)
- Setting up the CAS line signal timers (if required)
- Setting up a CAS profile (if required)
- Setting up a path and DS1 for E911
- Associating a CAS variant file with a DS1 line and Voice Interface (VIF)

To configure the E911 feature, perform the following procedure.

Step 1 Set up the CAS variant file

a. Use the **dspcasbuiltinvars** command to display the available built-in CAS variant files. For example.

```
M8850_NY.3.VXSM.a > dspcasbuiltinvars
=====================================================
=====================================================
    Built-in CAS Variants (dspcasbuiltinvars)
=====================================================
 File Name:    fgd_os_e911
 File Name:    fgd_os_psap
 File Name:    mf_wink_start_incoming
 File Name:    mf_wink_start_outgoing
 File Name:    dtmf_wink_start_incoming
 File Name:    dtmf_wink_start_outgoing
```

Verify that the var file for E911, fgd_os_e911, is present.

Note The only other variant file supported by VXSM is **mf_wink_start_incoming.o**. This file is used for lines that support the Busy Line Verify/Operator Interrupt (BLV/OI) feature.

b. Use the **addcasvar** command to add an E911 variant file. The command has the following format:

addcasvar<*CasVarIndx*><*FileName*>[**-source**<*SourceFile*>]

For *CasVarIndx* enter an integer in the range of 1 to 25, use a number to uniquely identify the variant file being added.

For *FileName*, enter **fgd_os_e911**. This is the name of the E911 variant file.

For **-source** <*SourceFile*>, enter **-source** 1 for internal.

This instructs VXSM to look for the file as a built-in file in the firmware. Actually, this parameter can be omitted because "internal" is the default value.

The other possible value for this parameter is 2 for external. If this is specified, VXSM looks for the file on the PXM hard disk. External is normally used for testing purposes.

The **dspcasvar** or **dspcasvars** commands can be used to verify that the variant file has been added successfully. For example:

```
M8850_NY.3.VXSM.a > dspcasvars
================================================================================
                              CAS Variants
================================================================================

VarIndx  Variant File Name  Source File  Variant State     Num of Associated
                                                          DS0 Group
=======  =================  ===========  ================  =================
   2     fgd_os_e911        internal     initSuccessfully          0
   3     mf_wink_start_incoming     internal     initSuccessfully          0
```

Step 2 Verify and configure (if necessary) the incoming and outgoing line signal values. The **addcasvar** command in the previous step populates the default values in the VXSM card for the incoming and outgoing line signals.

a. Use the **dspcasinclnsigs** and **dspcasoutlnsigs** commands to display the current values of these parameters. For example:

```
M8850_NY.3.VXSM.a > dspcasinclnsigs
================================================================================
                        Incoming Lines Signal
================================================================================

Var   Sig   Signal Name    New   Old   CurTx MinMake MaxMake MinBreak MaxBreak
Index Name                Match Match       Time    Time    Time     Time
      Index               Rx    Rx          (ms)    (ms)    (ms)     (ms)
===== ===== ============== ===== ===== ===== ======= ======= ======== ========
   2    1   rx_on_hook     00xx  xxxx  xxxx  300     300     0        0
   2    2   rx_off_hook    11xx  xxxx  xxxx  50      50      0        0
   2    3   rx_wink        11xx  xxxx  1111  100     350     70       0
   2    4   rx_flash       00xx  11xx  xxxx  200     700     0        0

M8850_NY.3.VXSM.a > dspcasoutlnsigs
====================================================================
                        Outgoing Lines Signal
====================================================================

Var    Signal      Signal Name     Tx       Make        Break
Index  Name Index                 Pattern  Time (ms)   Time (ms)
=====  ==========  ==============  =======  ==========  ==========
```

```
2       1       tx_on_hook      0000       50          0
2       2       tx_off_hook     1111       50          0
2       3       tx_wink         1111       210         50
2       4       tx_flash        0000       400         50
```

b. If these line signal values need to be changed, use the **cnfcasinclnsig** and **cnfcasoutlnsig** commands.

The format of the **cnfcasinclnsig** command is:

cnfcasinclnsig <*CasVarIndx*> <*ILSigIndex*> [**-minmt** <*MinMakeTime*>] [**-maxmt**<*MaxMakeTime*>][**-minbt** <*MinBreakTime*>] [**-maxbt** <*MaxBreakTime*>]

For *CasVarIndx* enter an index number to the relevant cas variant entry. The cas variant must have already been added (see previous step).

For *ILSigIndex* enter an integer in the range of 1 to 25 that uniquely defines the particular set of incoming line signal parameters.

[**-minmt** <*MinMakeTime*>] [**-maxmt**<*MaxMakeTime*>][**-minbt** <*MinBreakTime*>] [**-maxbt** <*MaxBreakTime*>] are the minimum and maximum make and break times. Enter a value for each parameter to be configured as follows:

-minmt—A number in the range of 50 to 1000 ms in increments of 10
-maxmt—A number in the range of 20 to 2000 ms in increments of 10
-minbt—A number in the range of 0 to 200 ms in increments of 10
-maxmt—A number in the range of 0 to 200 ms in increments of 10

The format of the **cnfcasoutlnsig** command is:

cnfcasoutlnsig <*CasVarIndx*> <*OLSigIndex*> [**-mt** <*MakeTime*>] [**-bt** <*BreakTime*>]

For *CasVarIndx* enter an index number to the relevant cas variant entry The cas variant must have already been added (see previous step).

For *OLSigIndex* enter an integer in the range of 1 to 25 that uniquely defines the particular set of outgoing line signal parameters.

[**-mt** <*MakeTime*>] [**-bt** <*BreakTime*>] are the make and break times. Enter a value for each parameter to be configured as follows:

-mt—A number in the range of 50 to 2000 ms
-bt—A number in the range of 0 to 200 ms

Step 3 Verify and Configure (if necessary) the Line Signal Timers.

An entry with default line signal timers is created automatically with an index number of 1. This default set of timers cannot be modified or deleted by the user. However, the user can create a new set of timers with a new index number.

a. Use the **dspcaslnsigtimer** command to display the default Line Signal Timer values. The format of this command is:

dspcaslnsigtimer <*LineSigTimerIndex***>**

For example:

```
M8850_NY.3.VXSM.a > dspcaslnsigtimer 1
============================================================
                  CAS Line Signal timer
============================================================
Line Signal Timer Index                    :    1
Idle Guard Timer (ms)                      :    10000
Clear Forward Timer (ms)                   :    120000
Clear Backward Timer (ms)                  :    120000
```

```
Release Guard Timer (ms)                      :    800
Glare Timer (ms)                              :    4000
Answer Meter Delay Timer (ms)                 :    600
Debounce Timer (ms)                           :    50
Seize Ack Response Timer (ms)                 :    6000
Delay Between Register and Line Answer (s)    :    90
Seize Ack Wait Timer (s)                      :    15
```

b. If any of the values of the Line Signal Timers need to be changed, use the **addcaslnsigtimer** command to create a new Line Signal Timers entry with a new index number.

The format of this command is:

addcaslnsigtimer <*LineSigTimerIndex***> [-ig <***IdleGuardTimer***>][-cfw <***ClearFwdTimer***>] [-cbw <***ClearBwdTimer***>][-rg <***ReleaseGuardTimer***>][-gl <***GlareTimer***>] [-am <***AnswerMeterDelayTimer***>][-db <***DebounceTimer***>][-srsp <***SeizeAckRspTimer***>] [-drl <***DelayBetRegAnsAndLineAns***>][-sdig <***SeizeAckToDigitTimer***>]**

For example:

```
M8850_NY.3.VXSM.a > addcaslnsigtimer 2 -ig 10000 -cfw 140000 -cbw 140000
```

The **addcaslnsigtimer** command adds and configures the CAS timers with index 2, idle guard timer of 10000 ms, clear forward timer of 140000 ms, clear backward timer of 14000 ms. The remaining unspecified timer values are assigned their default values.

Note Although the default set of timers with index = 1 cannot be modified or deleted, any other sets of timers created by the user can subsequently be modified or deleted using the **cnfcaslnsigtimer** and **delcaslnsigtimer** commands.

Step 4 Verify and Configure (if necessary) the CAS General Configuration values.

An entry with default CAS general configuration values is created automatically with an index number of 1. This default set of values cannot be modified or deleted by the user. However, the user can create a new set of values with a new index number.

a. Use the **dspcasgencfg** command to display the default CAS general configuration values. The format of this command is:

dspcasgencfg <*GenCfgIndex***>**

For example:

```
M8850_NY.3.VXSM.a > dspcasgencfg 1
================================================================================
                           CAS General Configuration
================================================================================
CAS General Config Index                      :   1
Glare Policy                                  :   rptSzOnGlareTmrExp
Parmameter Source                             :   mib
Register Signaling Mode                       :   compelled
Line Signaling Type                           :   digital
Ring Back Signal Type                         :   wink
Incoming Call High Frequency Power (dBm)      :   0
Incoming Call Low Frequency Power (dBm)       :   -30
Incoming Call Negative Twist Power (dBm)      :   7
Incoming Call Positive Twist Power (dBm)      :   7
Incoming Call Break Threshold  (dBm)          :   -32
Outgoing Call High Frequency Power (dBm)      :   -7
Outgoing Call Low Frequency Power (dBm)       :   7
Outgoing Call Cadence On Time (ms)            :   65
```

```
Outgoing Call Cadence Off Time (ms)          :   65
Country Code                                 :   000
Echo Cancellation                            :   2
Subscriber Category                          :   subscriberWithoutPriority
Nature Of Circuit                            :   notIncluded
Compelled Signaling Type                     :   enbloc
Tx Digit Order                               :   dnisAni
Digit Detect Mode                            :   2
Metering Report Interval Threshold (ms)      :   10
Start Timer (s)                              :   16
Long Timer  (s)                              :   16
Short Timer (s)                              :   4
Long Duration Timer  (s)                     :   100
MGC Timer (ms)                               :   1000
Digit Type                                   :   mf
End Point Directional                        :   bidirectional
Receive Timeout  (s)                         :   0
Initial Delay (s)                            :   0
Maximum Number Call Party                    :   0
```

b. If any of the values must be changed, use the **addcasgencfg** command to create a CAS general configuration entry with a new index number. The format of this command is:

addcasgencfg <*GenCfgIndex***> [-gp <***GlarePolicy***>][-ps <***ParmSource***>]**
[-rsig <*RegSigMode***>][-lsig <***LineSigTyp***][-rb <***RingBackType***>][-ihf <***IncHiFreqPower***>]**
[-ilf <*IncLoFreqPower***>][-int <***IncNegTwist***>][-ipt <***IncPosTwist***>]**
[-bkth <*IncBreakThreshold***>][-olf <***OutLoFreqPower***>][-opt <***OutPosTwist***>]**
[-cadon <*OutCadenceOntime***>][-cadoff <***OutCadenceOfftime***>]**
[-ccode <*CountryCode***>][-ecan <***EchoCancellation***>]**
[-subcat <*SubscriberCategory***>][-natcir <***NatureOfCircuit***>]**
[-compsig <*CompelledSigType***>][-tdo <***TxDigitOrder***>][-digdect <***DigitDetectMode***>]**
[-dmp <*MeteringRepIntThresh***>][-start <***StartTimer***>][-long <***LongTimer***>]**
[-short <*ShortTimer***>][-longdur <***LongDurationTimer***>][-mgctimer <***MGCTimer***>]**
[-digtype <*DigitType***>][-enptdir <***EndPointDirectional***>]**
[-rxtmout <*ReceiveTimeout***>][-initdelay <***InitialDelay***>][-mxnum <***MaxNumCallParty***>]**

For example:

```
M8850_NY.3.VXSM.a > addcasgencfg 2-gp 2 -ps 2 -lsig 2 -digtype 1
```

The **addcasgencfg** command adds and configures the CAS general features with an index =2, all default values are accepted with the exception of glare policy = 2 (OnGlareDetect), parameter source is 2 (MIB), line signaling type is 2 (ring back), and digit select mode is 1 (dtmf):

Note Although the default CAS general configuration values with index = 1 cannot be modified or deleted, any other sets of values created by the user can subsequently be modified or deleted using the **cnfcasgencfg** and **delcasgencfg** commands.

Step 5 Setup a CAS Profile.

A CAS profile is a table entry that specifies which CAS Line Signal Timer entry and which CAS General Configuration entry are to be used. A default CAS profile entry is created automatically that itself has

an index of 1 and specifies the CAS Line Signal Timer entry index of 1 and the CAS General Configuration entry index of 1. Thus the default profile specifies the default Line Signal Timers and default CAS General Configuration values.

a. Use the dspcasprof command to display the default profile.

```
M8850_NY.3.VXSM.a > dspcasprof 1
================================================
                  CAS Profile
================================================
CAS Profile Index             :    1
Line Signal Timer Index       :    1
General Config Index          :    1
```

If the user has created new Line Signal Timer or CAS General Configuration entries (as defined in the previous steps), the user can specify the use of these new entries by creating a new CAS profile.

Note Because the default profile cannot be modified or deleted, the only way to change which Line signal timers and which CAS general configuration values are to be used is to create a new profile.

To create a new profile, use the **addcasprof** command. The format of this command is:

addcasprof<*ProfIndex*> **-lstidx**<*LineSigtimer*> **-gcidx**<*GeneralCfg*>

Enter a new profile index number for the profile in the range of 2 to 25.

Note Although the default CAS profile with index = 1 cannot be modified or deleted, any profiles created by the user can subsequently be modified or deleted using the **cnfcasprof** and **delcasprof** commands.

Step 6 With the E911 files setup, the next step is to configure one or more DS1 lines as CAS lines for use with E911.

Note This step describes how to configure a DS1 line for CAS E911 purposes. The user can repeat this procedure to configure one or several lines for this purpose but the total (maximum) number of 20 CAS T1 lines per VXSM card (for all applications) must be observed.

a. Use the **upln** command to bring up a physical line, the format of this command is:

upln <*bay.line*>

For example:

```
upln 1.1.
```

This command brings up line 1 in bay 1 (upper).

b. Use the **uppath -sts** command to bring up a SONET path on the upped line, the format of this command is:

uppath -sts <*bay.line.path*>

For example:

```
uppath 1.1.1
```

This command brings up SONET path 1 on line 1 in bay 1 (upper).

c. Use the **uppath -ds1** command to bring up a DS1 line in the SONET path, the format of this command is:

uppath -ds1 <*bay.line.path.vtg.vt* >

For example:

```
uplath 1.1.1.1.1
```

This command brings up DS1 line 1 on the SONET path 1.

d. Use the **cnfpath -ds1** command to configure the DS1 line for CAS robbed bit signaling, the format of this command is:

cnfpath -ds1 <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> [**-lt** <*LineType*>] [**-sc** <*SendCode*>] [**-lpb** <*Loopback*>] [**-signal** <*SignalMode*>] [**-detect** <*LoopbackCodeDetection*>] [**-trkcnd** <*TrunkConditionEnable*>] [**-rep** <*Repetition*>]

The **-signal** parameter is used to set the signal mode to robbed bit (2), for example:

```
cnflath 1.1.1.1.1 -signal 2
```

The DS1 is now configured for CAS robbed bit signaling.

Step 7 This step creates a voice interface (VIF) for the E911 service and applies the CAS E911 configuration values to that voice interface.

a. Use the addvif command to create a VIF for the CAS E911 service. The format of this command is:

addvif <*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*Ds0GrpIndex*> <*Ds0BitMap*> <*ServiceType*> <*Repetition*>

For *bay.line.path.vtg.vt* |*bay.line.path.ds1* specify the same path that has been upped in the previous step.

For *Ds0GrpIndex* enter a new index number for the Ds0 group. An integer in the range 2 to 23.

For *Ds0BitMap* enter 1-24 to include all 24 T1 channels in the DS1.

For *ServiceType* enter the value 11 to indicate the MGC protocol as tgcp.

For *repetition* enter the value 1.

b. Use the **cnfvifcas** command to apply the configured CAS E911 values to the voice interface. The format of this command is:

cnfvifcas <<*bay.line.path.vtg.vt*> | <*bay.line.path.ds1*> <*Ds0GrpIndex*> <*CasVariant*> <*CasProfile*>

For <*bay.line.path.vtg.vt* >|<*bay.line.path.ds1*><*Ds0GrpIndex* specify the path and Ds0 group index of the VIF created in the previous sub step.

For *CasVariant*, enter the index number of the CAS Variant entry to be used. The index number that is specified must already exist.

For *CasProfile*, enter the index number of the CAS Profile entry to be used. The index number that is specified must already exist.

For example:

```
cnfvifcas 1.1.1.1.1 1 1 2
```

This example associates the VIF for path 1.1.1.1.1 Ds0 group 1 with the CAS Variant Index 1 and the CAS Profile index 2

Note If the application uses H.248 as the media gateway control protocol, the user should follow the **cnfvifcas** command with the **cnfvifterm** command. This command sets up the necessary CAS packages for CAS terminations.

Configuring Bearer and Signaling Security Features

Configuring the security features consists of the following major steps.

- Setting up security policies.
- Configuring phase 2 signaling security.
- Configuring phase 1 signaling security.
- Configuring the bearer channel.
- Enable security features.

Note Bearer and signal security are supported on both the CABLE and TGW firmware images. Bearer security operates with TGCP only. Signal security (IPSec) operates with either H.248 or TGCP.

Setting Up Security Policies

Step 1 Use the **addipsecsp** command to create a security policy database table and configure its parameters. The security policy contains a number of selectors that can be matched with those contained in the SDP from the MGC. The matching process determines whether a packet is treated as secure, not secure, or to be discarded.
The format of this command is:

addipsecsp <*SP Index*> <*Src Addr Prefix Len*> <*Src Addr*> <*Dst Addr Prefix Len*> <*Dst Addr*> <*SP Protocol*> <*SP Src Port*> <*SP Dst Port*> <*SP Directionality*> <*SP Mirroring*> <*SP Action*>

For *SP Index* enter a number in the range of 1 to 12, this number is then used to identify the item in the security policy database table.

For *Src Addr Prefix Len* enter a number in the range of 1 to 32. This specifies the length of the mask to be used for the source address selector (see below).

For *SrcAddr* enter an IP (dotted decimal) for the source address selector.

For *Dst Addr Prefix Len* enter a number in the range of 1 to 32. This specifies the length of the mask to be used for the destination address selector (see below).

For *dst Addr* enter an IP (dotted decimal) destination address selector.

For *SP Protocol* enter the transport layer protocol selector.
0 = Any protocol
1 = TCP,
2 = UDP
3 = RAW

For *SP Src Port* enter the source port selector in the range 1 to 65535. A 0 implies ‘any port’.

For *SP Dst Por*t enter the destination port selector in the range 1 to 65535. A 0 implies ‘any port’.

For SP Directionality, enter the inbound (in) or outbound (out) direction for Security Policy Database entries.

1 = In

2 = Out

For *SP Mirroring* enter whether mirroring or non-mirroring is to be applied.

1 = mirrored

2 = non-mirrored

If mirrored, an entry in the SPD applies to both the inbound and outbound databases with the source, destination addresses and ports reversed.

If nonmirrored, an entry added to the SPD applies in the specified direction only.

If mirrored is specified, then it applies to both inbound and outbound databases regardless of the directionality value.

For *SP Action* enter the action to be taken when a packet matches this policy

1 = secure - Apply IPSec on the packet which matches this policy.

2 = bypass - Do not apply IPSec processing on the packet which it matches this policy.

3 = discard - Drop the packet which matches this policy

The action applicable to a packet after it is selected for one of the three processing modes based on IP and transport layer header information (electors) matched against entries in the SPD.

Note For signal security to take effect, at least one policy must specify an action of ‘secure’.

Step 2 Create a separate “Bypass” policy to allow the flow through of DNS traffic.

Use the **addipsecsp** command entering the Media Gateway IP address as the source address and the DNS IP address as the Destination address. Specify the upper layer protocol as UDP (2). This policy stops DNS traffic from being dropped.

Step 3 Repeat step 2 for any other policies that will be required for the application.

Configuring Phase 2 Signaling Security

Protecting the signaling link between the MG and MGC involves configuring a number of security parameters such as encryption and authentication algorithms.

Follow the procedures below to configure signal security.

Step 1 Use the **addipsecxform** command to enter an item in the IKE Phase 2 Transform table and configure the encryption and authentication algorithms to be supported.

The format of this command is:

addipsecxform *<IPSec Transform Index> <IPSec Authentication Header> <IPSec ESP Encryption> <IPSec ESP Authentication> <IPSec Encapsulation Mode>*

For I*PSec Transform Index*, enter the index number to be used in the Phase Transform table. An integer in the range of 1 to 20.

For IPSec Authentication Header (AH), specify the AH Transform applicable to the proposal. Both AH and ESP Transforms cannot be null at the same time.

1 = none

2 = sha196 - SHA1 authentication, first 96 bits used for authentication

3 = md596 - MD5 authentication, first 96 bits used for authentication

For *IPSec ESP Encryption*, specify the ESP Transform applicable to the proposal.

3 = esp3Des - 3-DES encryption

8 = espNull - ESP encryption in cleartext

Only the parameter values of 3 = 3-DES and 8 = NULL are supported.

For *IPSec ESP Authentication*, specify the Authentication Algorithm for ESP Transform applicable to the proposal.

2 = sha196 - SHA1 authentication - first 96 bits used for authentication

3 = md596 - MD5 authentication - first 96 bits used for authentication.

For *IPSec Encapsulation Mode*, specify the encapsulation type for the transform enter the value of 1.

1 = transport - IPsec in Transport encapsulation mode

Only the1 = transport mode is supported.

Step 2 Use the **addipsecprop** command to add an entry to the IPSec Phase 2 Proposal Table. With this command the user can specify the Diffie Hellman group, the lifetime of the Phase 2, and the lifetime unit.

The format of this command is:

addipsecprop <*Proposal Index*> <*End Point IP Address*> [**-antiReplay** <*Anti Replay*>][**-pfsEnable** <*Pfs Enable*>][**-dhgrp** <*Diffie Hellman Group*>][**-unitoftime** <*Unit of Time*>][**-hardlifetime** <*Hard Lifetime*>][**-select** <*Use Select*>]

For *Index* enter a number in the range of 1 to 20, this number is then used to identify the item in the Phase 2 Proposal table.

For *EndPointIPAddress* enter an IP address of the MGC in dotted decimal format. In the case of a Tunnel, the IP Address is that of the router between two end hosts (Gateway).

For **-antiReplay**<*AntiReplay*> This parameter specifies whether the Anti-Replay (partial sequence integrity) service to help counter Denial of Service (DoS) attacks is enabled or not. Specify:

1 = Disabled
2 = Enabled

For **-pfsEnable**<*PfsEnable*>, this parameter specifies if Perfect Forward Secrecy is enabled or not. Specify:

1 = Enabled
2 = Disabled

For -**dhgrp** <*Diffie Hellman Group*>, this parameter. Both Diffie-Hellman groups 1 and 2 are supported for the key exchange process. Specify:

1 = Group 1
2 = Group 2

For **-unitoftime**<*Unit of Time*>, this parameter that specifies the units of time for the Phase 2 Lifetime parameter.

1 = seconds

2 = minutes

3 = hours

For **-hardlifetime**<Hard*Lifetime*>, this parameter specifies the time interval when the current SA ends. The unit of this object is dependent on the UnitOfTime parameter.

Enter a number in the range:

60..86400 (seconds)

1..1440 (minutes)

1..24 (hours)

For **-select**<*UseSelect*>, this parameter specifies whether the selector parameters are obtained from policy or copied from incoming packet.

1 = Packet
2 = Policy

Step 3 Repeat step 2 for each other MGCs that VXSM uses for signaling.

Step 4 Use the **addipsecprxfassoc** command to make an association between a proposal entry and a transform entry.

The format of this command is:

addipsecprxfassoc <*Index*> <*IKE Transform Idx*>

For *Index*, specify the index number in the IKE Phase 2 Proposal Table for the proposal entry to be associated. An integer in the range of 1 - 20.

For *IKE Transform Idx*, specify the index number in the IPSec Ike Phase 2 Proposal Transform table. An integer in the range of 1 - 72.

Step 5 Use the **addipsecspkm** command to add an entry to the Policy Database Key Manager Association table. This table contains the mapping between the SPD Table and the Key Manager Table. With this command the user can specify an association between a Security Policy and a Key Manager.

The format of this command is:

addipsecspkm <*SP Index*> <*SP Key Mgr Assoc Key Type*> <*SP Key Mgr Assoc Key Index*>

For *SP Index*, enter the index number to be used in the Policy Database Key Manager Association table. An integer in the range of 1 - 20.

For *SP Key Mgr Assoc Key Type*, to specify whether IKE or MKM is used for key management for the SPD entry specified. Enter the value of 1 (IKE).

1 = ike - Dynamic method of Key Management through Internet Key Exchange (IKE) protocol.

manual - Manual method of key management (not supported).

For *SP Key Mgr Assoc Key Index*, to specify the index of the Key Manager table with which the corresponding SPD entry is associated. The index belongs to IKE or MKM tables is determined on the basis of the parameter SP Key Mgr Assoc KeyType An integer in the range of 1 - 72.

Step 6 Repeat step5 for each other MGCs that VXSM uses for signaling.

Configuring Phase 2 Signaling Security

Step 1 Use the **addipsecikexform** to enter an item in the IKE Phase 1 Transform table and configure the encryption and authentication algorithms to be supported.

The format of this command is
:
addipsecikexform <*IKE Transform Idx*> <*IKE Encryption Algo*> <*IKE Auth Algo*>

For I*KE Transform Idx* enter a number in the range 1 to 10 to identify this record in the IKE Phase 1 Transform table.

For *IKE Ecnryption Algo* enter the encryption algorithm to be used:

1 = DES
2 = DES3

For *IKE Auth Algo* enter the authentication algorithm to be used

1 = MD5
2 = SHA.

Step 2 Use the **addipsecikeprop** command to enter an item in the IKE Phase 1 Proposal table and to configure proposal parameters.

The format of this command is:

addipsecikeprop <*Index*> [-**dhgrp** <*Diffie Hellman Group*>][-**lifetimeunit** <*Lifetime Unit*>][-**lifetime** <*Lifetime*>]

For *Index* enter a number in the range of 1 to 10, this number is then used to identify the item in the Phase 1 Proposal table.

For -**dhgrp** <*Diffie Hellman Group*>, this is an optional parameter. Both Diffie-Hellman groups 1 and 2 are supported for the key exchange process. Specify:

1 = Group 1
2 = Group 2

For **-lifetimeunit**<*Lifetime Unit*>, an optional parameter that specifies the units of time for the Phase1Lifetime parameter.

1 = seconds

2 = minutes

3 = hours

For **-lifetime**<*Lifetime*>, an optional parameter that specifies the time interval when the current IKE Phase 1 Proposal ends. An integer in the range 1 - 65535. The unit is the unit specified in the lifetime unit parameter.

Step 3 Use the **addipsecikeprxfassoc** command to make an association between a proposal entry and a transform entry.

The format of this command is:

addipsecprxfassoc <*Index*> <*IKE Transform Idx*>

For *Index*, specify the index number in the IKE Phase 1 Proposal Table for the proposal entry to be associated. An integer in the range of 1 - 10.

For *IKE Transform Idx*, specify the index number in the IPSec Ike Phase 1 Proposal Transform table. An integer in the range of 1 - 10.

Step 4 Use the **addipsecikepeer** command to add an entry to the Ike Peer authentication Table. This command also specifies a remote IKE peer, authentication pre shared key information, the proposal to be used, and the authentication method.

addipsecikepeer *<IP Config Index> <Remote IP Index> <Remote IP Addr Type> <Remote IP Addr> <Auth Pre Shared Key> <Proposal Index> <Auth Method>*

This command. With this command the user can.

For *IP Config Index,* specify the index for the Ike Peer authentication Table. An integer in the range of 1 - 16

For *Remote IP Index*, specify the index number of the remote IKE peer. An integer in the range 1 - 16

For *Remote IP Addr Type* and *Remote IP Addr*, specify the value 1 (Ipv4) for address type and the address (dotted decimal notation) of the remote peer.

For *Auth Pre Shared Key*, specify any authentication information in the form of an SNMP admin string of 1 - 64 characters.

For *Proposal Index*, specify the index in the phase 1 proposal table that defines the proposal to be used to communicate with the peer. An integer in the range 1 - 10.

For *Auth Method*, specify the authentication method to be used. Enter the value 1 for PSK (Pre Sharing Key).

Configuring Bearer Security

Step 1 Use the **cnfciphersuite -rtp** command to configure an entry to the RTP Cipher Suite table. With this command the user can specify the RTP encryption and authentication algorithms available for use with bearer security and the usage preference of those algorithms

The format of this command is:

cnfciphersuite -rtp *<Encryption Algorithm> <Authentication Algorithm> <Preference>*

For *Encryption Algorithm,* specify an encryption algorithm that may be used for bearer traffic.

1 = Null (no encryption)
2 = AES-128

For *Authentication Algorithm,* specify an authentication algorithm that may be used for bearer traffic.

1 = Null (no authentication)
2 = MMH2
3 = MMH4

For *Preference,* specify the preference for the algorithms in this cipher suite.

The entry with the highest preference will be selected first. The entry with '0' preference is not applicable. An integer in the range of 0 to 18.

Note A combination of null RTP encryption and non-null RTP authentication algorithms is invalid. For example, cnfciphersuite -rtp 1 2 2 would not be valid.

Step 2 Repeat step 1 as necessary to configure additional RTP cipher suites.

Step 3 Use the **cnfciphersuite -rtcp** command to configure an entry to the RTCP Cipher Suite table. With this command the user can specify the RTCP encryption and authentication algorithms and the usage preference of those algorithms.

The format of this command is:

cnfciphersuite -rtcp <*Encryption Algorithm*> <*Authentication Algorithm*> <*Preference*>

For *Encryption Algorithm,* specify an encryption algorithm that may be used for bearer traffic.

1 = Null (no encryption)
2 = AES-CBC

For *Authentication Algorithm*, specify an authentication algorithm that may be used for bearer traffic.

1 = Null (no authentication)
2 = HMAC SHA1-96

For *Preference,* specify the preference for the algorithms in this cipher suite.

The entry with the highest preference will be selected first. The entry with '0' preference is not applicable. An integer in the range of 0 to 18.

Note A combination of null RTCP encryption and non-null RTCP authentication algorithms is invalid. For example, cnfciphersuite -rtcp 1 2 2 is not valid.

Step 4 Repeat step 3 as necessary to configure additional RTCP cipher suites.

When the ciphersuite configurations have been performed, they can be verified using the **dspciphersuite** and **dspciphersuites** commands.

Enable Security Features

Step 1 Use the **addipsecnwif** command to add an entry to the Network Interface Table. With this command the user can specify the IP DF (Don't fragment) bit and a PMTU timeout value. These parameters are used for configuring Tunnel mode during IKE phase 2.

The format of this command is:

addipsecnwif <Local *IP Index*> [**-dfbit** <*DF Bit*>][**-pmtuage** <*PMTU age*>]

For *Local IP Index*, enter the index number to be used in the Network Interface Table. An integer in the range of 1 - 16

For **-dfbit**<*DF Bit*>, specify whether to clear, set or copy the inner IP header DF (Don't fragment) bit for the Network Interface.

1 = clear - DF bit is not set in the Tunnel IP header (default)

2 = set - DF bit is set in the Tunnel IP header

3 = copy - DF bit is copied from inner IP header to the Outer Tunnel IP header.

For **-pmtuage**<*PMTU age*>, specify a timeout value in seconds for PMTU Information for an SA. An integer in the range of 1 - 65535. Default is 10.

Step 2 Use the **cnfbearersec** to enable security on the IP bearer traffic.

The format of this command is:

cnfbearersec<*Security Enable*>

For *Security Enable*, specify:

1 = Enable
2 = Disable

Configuring More Features

In addition to the features described so far in this chapter, there are more VXSM features that can be configured by the user. Refer to Chapter 5 in this guide to see configuration details of these additional features. Some features include:

- Clocking
- Connection Admission Control (CAC)
- Network Bypass
- Differentiated Services
- Fax/Modem Services
- Jitter Compensation

Configuring Switches for AAL2 Trunking Applications

Cisco MGX 8880 and 8850 switches equipped with VXSMs that function as media gateways can be configured to meet the requirements of an AAL2 trunking application.

In AAL2 Trunking applications, the voice TDM interface and the packet network interface need to be configured. The trunking application involves VXSM cards, the PXM-45 card, and the AXSM cards. These cards all function together and must be configured accordingly.

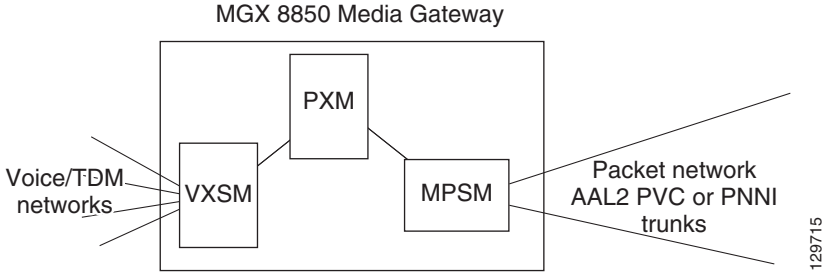
VoATM trunking configuration consists of the following tasks.

- PXM-45 card configuration
- AXSM card configuration
- VXSM card configuration
- Provisioning Trunk PVCs

Multipurpose Service Module Alternative

This chapter describes procedures in which the interface to the packet network ia and AXSM card. For AAL2 trunking applications (on an MGX 8850 platform only), VXSM can 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 configuration procedures in this chapter are applicable to MPSM configurations except that the MPSM card must be provisioned instead of the AXSM card. The MPSM card must be configured for ATM context using the MPSM **cnfclictx atm** command. After the context is set to ATM, provisioning is performed with the **upln**, **addport** and **addcon** command sequence. For more details, refer to the MPSM user documentation.



Quick Start Procedure

Table 4-1 shows a brief overview of the media gateway setup for a VoATM trunking application. A more detailed procedure appears later in this chapter.

Table 4-1 Media Gateway Setup for a VoATM Trunking Application Commands

Task	Subtask/Commands
Basic node setup	Basic PXM-45 setup commands **cnfname** **cnfdate** **cnftmzn** **cnftmznmgt** **cnftime** **addcontroller** **ipifconfig** **addsct**
Setup the AXSM cards	AXSM Setup Commands **upln** **cnfln** **addport** **addpart**
Setup VXSM card	Create VXSM resource partition **addrscptn** Config Voice Interfaces **addvif** **cnfpath -sts -payload** (OC-3 only) **cnfvif** Bring up VXSM Lines **upln** **uppath -sts-1 -ds1** (OC-3 only)
Create slave end of AAL2 bearer trunk connections on the local VXSM.	VXSM connection command **addcon**
Create slave end of AAL5 HDLC signaling trunk connections on the local VXSM (if applicable)	VXSM connection command **addcon**
Create master end of each AAL2 bearer trunk connection at remote VXSM.	Remote VXSM command **addcon**
Create master end of each AAL5 HDLC signaling trunk connection at remote VXSM (if applicable)	Remote VXSM command **addcon**

Table 4-1 Media Gateway Setup for a VoATM Trunking Application Commands

Task	Subtask/Commands
Configure AAL2 trunks to set up CIDs. If the application transports SS7 signaling across the network, use AAL2 profile CUSTOM 200 (clear channel)	VXSM addcid command
If using Nx64, configure AAL5 signaling trunks	addnx64prof addnx64aal5
Configure PNNI on PXM card	PXM commands dnpnport cnfpnportsig uppnport

Configuring the PXM-45 Card

Log on to the PXM-45 card and perform the following steps to configure the PXM-45 card for VoATM using the VXSM. The PXM-45 has a large number of commands. These steps address only the minimum commands required to set up the MGX 8850 as a media gateway.

Step 1 Use the **cnfname** to give the MGX 8850 a node name.

```
unknown.7.PXM.a > cnfname <node name>
```

Enter up to 32 characters for the new node name (node name is case-sensitive).

For example:

```
unknown.7.PXM.a > cnfname gateway1
```

After the user responds **Yes** to a confirmation request, the name is changed to gateway1.

Step 2 Use the **cnfdate** command to set the date.

```
gateway1.7.PXM.a > cnfdate <mm/dd/yyyy>
```

Step 3 Use the **cnftmzn** command to set the time zone.

```
geteway1.7.PXM.a > cnftmzn <timezone>
```

Step 4 Use the **cnftmzngmt** command to set an offset if an offset from GMT is to be used.

```
geteway1.7.PXM.a > cnftmznmgt <timeoffsetGMT>Offset can be from -12 to +12.
```

Step 5 Use the **cnftime** command to enter the time.

```
geteway1.7.PXM.a > cnftime <hh:mm:ss>
```

Step 6 Use the **addcontroller** command to add a PNNI controller to the PXM-45 card

```
geteway1.7.PXM.a > addcontroller <cntrlrId> i <cntrlrType> <slot> [cntrlrName
```

cntrlrId is the controller ID, enter 2 to specify a PNNI controller.

cntrlrType is the controller type, enter 2 to specify a PNNI controller type.

slot is the PXM slot in the MGX 8850, enter 7 or 8 as appropriate.

cntrlrName is an optional controller name, enter a text name is desired.

Step 7 Use the **ipifconfig** command to specify a LAN IP address for the node.

```
geteway1.7.PXM.a > ipifconfig lnPci0 <IP_Addr><netmask <Mask>
```

Specify the values for the IP address and its associated netmask.

AXSM Card Configuration

Log on to the AXSM card and perform the following steps to configure the AXSM card for VoATM using the VXSM. The AXSM has a large number of commands. These steps deal only with the minimum commands required to setup the MGX 8850 as media gateway.

Step 1 Setup a Service Class Template (SCT) for the AXSM card. The SCT file name has the following format: AXSM_SCT.CARD.2.V1

The SCT file must have been ftp-ed to the node's PXM-45 disk in the C:SCT/TEMP directory

Use the **dspctchksum** command to display the checksum value of the file. Note the value of checksum

Note A Service Class Template (SCT) is a collection of ATM configuration parameter settings that are stored in a single file and can be applied to multiple lines or ports. SCT files include the following types of configuration data:

General link parameters
COSB (Class of Service Buffers) parameters
Virtual circuit threshold parameters
COSB threshold parameters

Step 2 Use the **cc** command to switch to the active PXM-45 card.

Step 3 On the PXM-45 card, use the **addsct** to move the file to the F:SCT/AXSM directory on the PXM-45 disk. This has the effect of installing the SCT.

```
geteway1.10.AXSM.a > addsct <card type> <sct type> <sct ID> <Maj ver> <chksum>
```

cardtype is the card whose SCT you want to make available to the card by installing the SCT in the appropriate directory. Enter 1 for AXSM

scttype identifies either a port-level or a card-level SCT. Enter 2 for card level.

SCT ID refers to a specific service class template. The SCT is either provided by Cisco or created through CWM. Possible IDs are, Cisco-provided: 1-100 and User-created: 101-255. The default SCT ID is 0.

Maj ver is the major version number of the file. This number is assigned by Cisco.

checksum is the checksum for the file. Use the value obtained from the dspsctchksum command. The value is also published in the relevant release notes.

Step 4 While still logged into the PXM-45 card, repeat Steps 1 and 2 for the port SCT to be used by the PXM-45. In the addsct command specify 1 (port level) for the **scttype** parameter.

Step 5 Use the **cc** command to switch back to the AXSM card.

Step 6 Use the **upln** command to bring up the AXSM lines to be used by the gateway. This command establishes minimal connectivity over the line.

```
geteway1.10.AXSM.a > upln <bay.line>
```

For bay, enter 1 if the line on the back card is in the upper bay and enter 2 if it is in the lower bay. For line, enter the back card port number to which the line is connected.

Step 7 Use the **cnfln** command to configure a SONET lines.

```
geteway1.10.AXSM.a > cnfln -sonet <bay.line> -slt <LineType> -clk <clock source>
```

Enter the bay and line of the line being configured (see upln above). For LineType, enter 1 for SONET or 2 for SDH. For clockSource, enter 1 to use a clock received over the line from a remote node or 2 (the default) to use the local timing defined for the local node.

Step 8 Use the **addport** command to enable each ATM port to be used as a trunk for voice payload.

```
geteway1.10.AXSM.a > addport <ifNum> <bay.line> <guaranteedRate> <maxRate> <sctID>
<ifType>
```

For ifNum, enter a number from 1 to 60 to identify this interface. The interface number must be unique on the card to which it is assigned. For UNI and NNI ports, you can assign one logical interface per line.

For guaranteedRate and maxRate, enter an OC3 value in the range of 50 to 353207 cells per second.

For ifType, 1 specifies UNI, 2 specifies NNI. For trunking mode, each trunk port should be configured as NNI.

Step 9 Use the **addpart** command to create resource partition on the AXSM card. This command automatically creates a controller partition on the AXSM card. This command should be executed for each port that uses the controller.

```
geteway1.10.AXSM.a > addpart <ifNum> <partId> <ctrlrId> <egrminbw> <egrmaxbw> <ingminbw>
<ingmaxbw> <minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

For ifNum, enter the port number. For partId, enter 1 for PNNI. For cntrlid, enter 2 for PNNI.

The remaining parameters are used to specify maximum and minimum values for vpi/vci, bandwidth, connections, etc., see the Cisco MGX 8850 (PXM45 and PXM1E) Command Reference, Release 5 for details.

VXSM Card Configuration

Log on to the VXSM card and perform the following steps to configure the VXSM card for VoIP. The VXSM has a large number of commands. These steps deal only with the minimum commands required to setup the MGX 8850 as a media gateway

Create VXSM Resource Partition

Step 1 Use the **addrscprtn** command to create a resource partition for the VXSM card.

```
geteway1.5.VXSM.a > addrscprtn <ifNum> <partId> <ctrlrId> <egrminbw> <egrmaxbw> <ingminbw>
<ingmaxbw> <minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

For *ifNum*, enter 1 for port number. For *partId*, enter 1 for PNNI. For *cntrlid*, enter 2 for PNNI.

The remaining parameters are used to specify maximum and minimum values for vpi/vci, bandwidth, connections, etc., see the Cisco MGX 8850 (PXM45 and PXM1E) Command Reference, Release 5 for details.

Configuring the TDM Interface

Identifying Voice Circuits

The OC-3, 48 T1/E1, and 3 T3/E3 versions of the VXSM cards, support a variety of multiplexing schemes for interfacing to voice circuits. These schemes fall into four major categories:

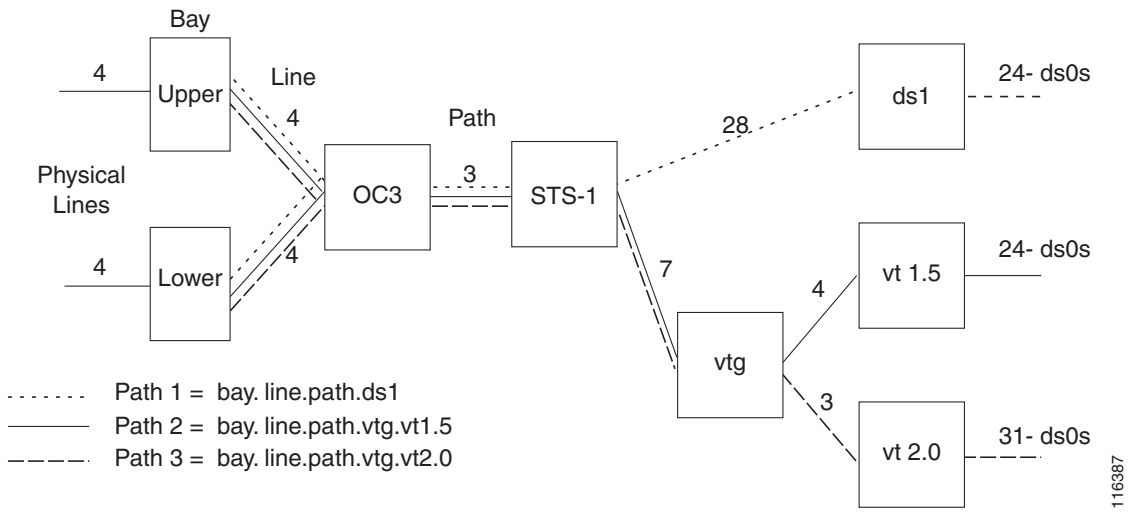
- Multiplexing under the OC-3 standards.
- Multiplexing under the SDH (Synchronous Digital Hierarchy) standards.
- Multiplexing under the T1 and E1 standards.
- Multiplexing under the T3 and E3 standards (T3 only in Release 5.2).

Many of the VXSM commands require the user to specify a line, a single voice circuit, or a group of voice circuits. The following paragraphs describe how these items are specified for the different multiplexing schemes.

OC-3 Systems

Specifying a DS0 stream from the highly multiplexed bit stream of OC3 is performed using the relationships (paths) shown in Figure 4-1.

Figure 4-1 OC-3 Hierarchical Relationship



The bit stream interfaces with VXSM via one of the four physical lines in the OC3 back card. This interface is usually in the upper bay (but, when a redundant back card is used and is active, it is in the lower bay).

For a particular line, the OC3 stream consists of three paths and, depending upon the format, a path consists of either 7 virtual tributary groups (vtg) or 28 DS1s. A vtg can be further divided into either four virtual tributaries (version 1.5) or three virtual tributaries (version 2.0). The DS1 and the virtual tributaries (vt) consist of 24 T1 DS0s for T1 or 31 DS0s for E1.

As shown in the diagram, the relationship between DS0s and physical ports can take one of three paths. The paths are common between the physical line and STS-1 level. From the STS-1 level to the DS0, one of three paths can be taken.

The path that a particular DS1/DS0 will use can be configured by the user with the **-payload** parameter in the **cnfpath -sts** command. This parameter can be set to:

- 3 = ds3 (not applicable to SDH interface)—The path is carrying a DS3 payload.
- 4 = vt15vc11—The path is carrying a SONET-VT1.5/SDH-VC11 payload.
- 5 = vt20vc12—The path is carrying a SONET-VT2/SDH-VC12 payload.

Note The vt1.5 path and the vt2.0 path also support SDH-VC11 and SDH-VC12 interfaces respectively.

Using the system described above, DS1 paths in VXSM commands are formatted as follows:

- **SONET path payload type VT1.5 or VT2.0**

  The DS1 is specified as: *bay.line.path.vtg.vt*

  bay = upper of lower bay of the VXSM backcard.
  line = the line number on the associated OC-3 card in the range 1 to 4.
  path = the path of the virtual tributary in the range 1 to 3.
  vtg = the virtual tributary groups applicable to the connection in the range 1 to 7.
  vt = virtual tributaries in the range 1 to 4 for vt1.5 or 1 to 3 for vt2.0.

Caution The combination of seven vtgs and four vts allows the specification of one of up to 28 DS1s. Be aware that VXSM supports two schemes for mapping a DS1 to a vtg/vt combination. These schemes are known as ‘standard’ and ‘Titan’ and are described in Table 5-1VTG/VT to DS1 Mapping, page 5-3.
vtg = the virtual tributary group.
vt = virtual tributary

- **SONET path payload type is ds3.**

The DS1 is specified as: *bay.line.path.ds3.DS1*

bay = upper of lower bay of the VXSM backcard.
line = the line number on the associated OC-3 card in the range 1 to 4.
ds3 = the SONET (STS-1) path payload type as ds3 in the range 1 to 3.
ds1 = the ds1 channel within the ds3 interface in the range 1 to 28.

SDH Systems

The VXSM- 155 card supports voice circuits that are multiplexed according to the Synchronous Digital Hierarchy (SDH) standard. Each OC- 3 line presents the data stream as a 155.52 Mbps Synchronous Transport Module (STM-1).

Figure 4-2 shows the multiplexing paths between STM-1 at the physical line and the T1 or E1 voice circuits.

When using the SDH interface, the user must configure the path using the **cnfpath -sts** command. The format of this command is:

cnfpath -sts <*bay.line.path*> [**-payload** <*Path Payload*>] [**-tm** <*Tributary Mapping Type*>] [**-tg** <*Tributary Grouping*>] [**-txtrace** <*Transmit Trace*>] [**-extrace** <*Expect Trace*>]

<*bay.line.path*>, specifies the bay (upper of lower back card), the physical line number on the back card, the path number between the STM and the AU (1, 2, or 3 for AU-3, 1 for AU-4)

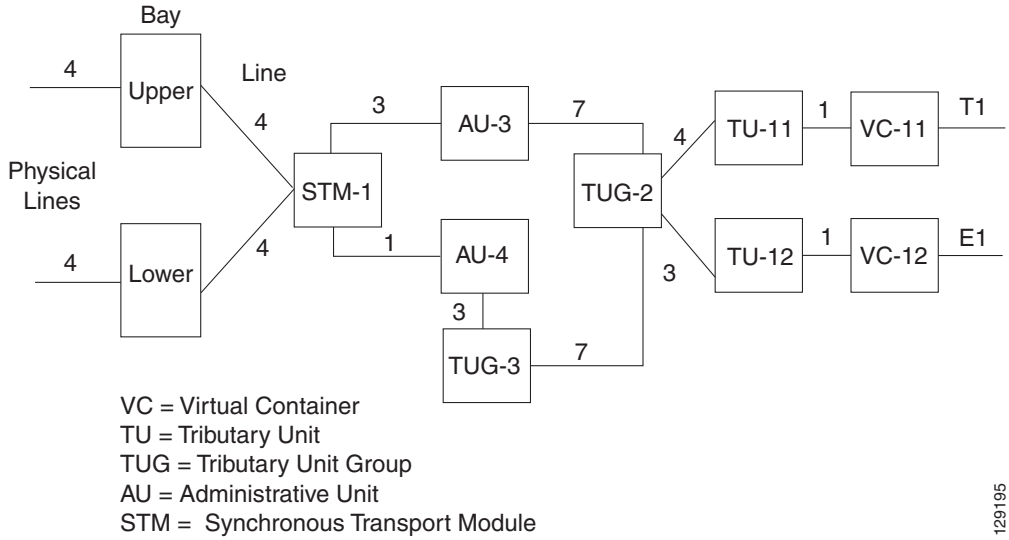
-payload <*Path Payload*>, specifies the TU/VC combination (TU-11/VC-11 for T1 or TU-12/VC-12 for E1).

-tm<*Tributary Mapping Type*>, specifies the mapping mode, 1 = asynchronous mode or 2 = byteSynchronous mode.

-tg <*Tributary Grouping*>, specifies the tributary grouping This is a choice between AU-3 (the default) or AU-4.

2 = au3Grouping—Applicable to SDH interfaces: STM1, -AU-3, -TUG-2, -TU-12, -VC12 or STM1, -AU-3, -TUG-2, -TU-11, -VC11.
3 = au4Grouping—Applicable to SDH interfaces: STM1, -AU-4, -TUG-3, -TUG-2, -TU-12, -VC12 or STM1, -AU-4, -TUG-3, -TUG-2, -TU-11, -VC11.

Figure 4-2 SDH Hierarchical Relationships



T1/E1 Systems

In T1/E1 systems, the front card supports up to 48 T1 or E1 lines. The back card supports up to 24 T1 or E1 lines. Depending upon the number of lines to be supported, one or two half high back cards are configured with a single front card; one in the upper or lower bay and the other (if configured) in the remaining open bay.

A physical line or a DS1 service is specified simply as:
bay.line

where:
bay = 1 or *2*—1 for the upper bay, 2 for the lower bay.

line = 1 – 24—The physical T1 line on the backcard in the range 1 to 24.

If the command requires the interface to be further specified down to the DS0 level, the DS0 is specified as:

bay.line ds0grp

where:

ds0grp = 0 - 24 or 31 — The DS0 group in the range of 0 to 23 for T1 or 0 to 30 for E1.

T3.E3 Systems

In T3/E3 systems, the front card supports up to 6 T3 or E3 lines. The back card supports up to 3 T3 or E3 lines. Depending upon the number of lines to be supported, one or two half high back cards are configured with a single front card; one in the upper or lower bay and other (if configured) in the remaining open bay.

A DS1 is specified simply as:

bay.line.path

where:

bay = *1* or *2*—1 for the upper bay, 2 for the lower bay.

line = 1 – 3—The physical T3 line on the backcard in the range 1 to 3

path = 1 - 28—The DS1 circuit in the T3 line in the range of 1 to 28

If the command requires the interface to be specified down to the DS0 level, the DS0 is specified as:

bay.line.path ds0grp

where:

ds0grp = 0 - 24 or 31 — The DS0 group in the range of 0 to 23 for T1 or 0 to 30 for E1.

Note The VXSM T3/E3 card set is designed to support both T3 and E3 applications. However, in Release 5.2 only T3 services are supported.

Voice Interfaces (VIF)

A voice interface (vif) is a user configurable set of parameters that is applied to a group of ds0s within a ds1. The configuration settings of the vif are used by the digital signal processors (DSPs) to determine how a voice payload is to be processed by VXSM.

A voice interface is created using the **addvif** command. With this command the user specifies a vif number and its associated ds1, in addition, the type of signaling, the type of service (H.248 switching, trunking, etc.). Other bearer channel parameters such as echo cancellation and voice activity detection, are also specified. These parameters are contained within a vif which, when the vif is added, are assigned default values.

Once a vif is created, its parameters can be discovered using the **dspvif** command. There are also display and configure commands for the user to see and configure the various parameters.

An example of the **addvif** and **dspvif** commands is as follows:

The following command sequence adds a voice interface in a DS1 path for the VXSM card in slot 3 of the media gateway and then displays the results:

```
M8850_NY.3.VXSM.a > addvif 1.1.1.1.1 0 24 9 250

M8850_NY.3.VXSM.a > dspvif 1.1.1.1.1 0
=====================================================
```

```
Configuration of DS0 Group in DS1
=================================================
DS1 Line              :                 1.1.1.1.1
DS0 Group             :                 0
Service Type          :                 h248
DS0 Bit Map           :                 24
```

To configure a vif perform the following steps.

Step 1 Use the **dspvifs** command to check that the vif exists. If it doesn't, use the **addvif** command to create the vif.

Step 2 For a particular ds1, use one of the display vif commands to display its associated vif parameter values. Determine which parameter (if any) need to be modified.

dspvif [<*bay.line.path.vtg.vt* >] | [<*bay.line.path.ds3.ds1*>] <*ds0GroupId*> *for OC-3*

dspvif <*bay.line*> <*ds0GroupId*>*for 48 T1/E1*

dspvifterms

dspvifterm [< *bay.line.path.vtg.vt* >] | [<*bay.line.path.ds3.ds1*>] <*ds0GroupId*> *for OC-3*

dspvifterm <*bay.line*> <*ds0GroupId*> *for 48 T1/E1*

dspvifparam <*bay.line*> <*ds0GroupId*>*for 48 T1/E1*

dspvifparams

Step 3 Use the following configure vif commands to modify vif parameters.

cnfvifparam <*specified ds!*> **<***ds0GroupId*> <*NoiseRegEnable*> <*NonLinearProcEnable*> <*MusicOnHoldThreshold*> <*ModemPassThru*> <*UpspeedCodec*> <*Repetition*>

cnfvifterm <*specified ds!*> <*ds0GroupId*> <*gatewayLinkId*> <*packageIds*> <*profileId*>*(Only applicable when service is H.248)*

See the chapters entitled VXSM Commands for a description of the commands listed in steps 2 and 3.

Configuring the TDM Lines

Use the following steps to configure the TDM lines on the VXSM.

Step 1 For OC3 cards, use the -**payload** parameter in the **cnfpath** -**sts** command to specify the ds1 path with the OC3. The choices are ds3, vt1.5, and vt2.0.

cnfpath -sts<*bay.line.path*>*[-payload <PathPayload>][-tm <TributaryMappingType>][-tg <TributaryGroupingType>][-txtrace <PathTraceToTransmit>][-exptrace <PathTraceToExpect]*

<bay.line.path>

bay: 1

line: 1 - 4

path: 1 - 3 or 1 (AU4 only)

[-payload <PathPayload>]

3 - ds3

4 - vt15vc11

5 - vt20vc12

[-tm <TributaryMappingType>]

1 - asynchronous

2 - byteSynchronous (NA for ds3)

[-tg <TributaryGroupingType>]

1 - notApplicable (SONET)

2 - au3Grouping (SDH)

3 - au4Grouping (SDH)

[-txtrace <PathTraceToTransmit>]

trace-string: size 16(SDH) or 64(Sonet)

[-exptrace <PathTraceToExpect]

trace-string: size 16(SDH) or 64(Sonet)

Step 2 Use the **upln** command to bring up a VXSM line.

```
geteway1.5.VXSM.a > upln <bay.line>
```

For bay, enter 1 for upper bay or 2 for upper bay.

For line, enter a value in the range 1 - 4 for OC3 or 1 - 24 for 48T1/E1.

Step 3 For OC3 cards, use the **uppath** command to specify the STS-1 path within the OC3

```
geteway1.5.VXSM.a > uppath -sts<bay.line.path>
```

For bay, enter 1 for upper bay or 2 for lower bay.

For line, enter a value between 1 and 4 to indicate the physical OC3 interface on the back card.

For path, enter a value between 1 and 3 to indicate the DS3 path within the OC3 interface.

Step 4 For OC3 cards, use the **uppath** command to specify the DS1 path within the DS3

```
geteway1.5.VXSM.a > uppath -ds1<bay.line.path.vtg/ds3.vt/ds1>
```

For bay, enter 1 for upper bay or 2 for upper bay.

For line, enter a value between 1 and 4 to indicate the physical OC3 interface on the back card.

For path, enter a value between 1 and 3 to indicate the DS3 path within the OC3 interface.

Note vtg = the virtual tributary groups applicable to the connection.
vt = virtual tributaries

Step 5 Use the **addvif** command to add a voice interface for a DS0 group within a DS1.

For OC3 cards, the syntax of this command is:

addvif <*LineNum*> <*Ds0GrpIndex*> <*Ds0BitMap*> <*ServiceType*><*BulkProvisionNumber*>

Where:

LineNum—(bay.line.path.vtg.vt or bay.line.path.ds1)

bay {1 - upper}

line (range=1..4)

path (range=1..3)

vtg (range=1..7)

vt (range=1..4)(ds1) (range=1..3)(e1)

ds1 (range=1..28)

Ds0GrpIndex—DS0 group index

T1: (range=0..23)

E1: (range=0..30)

Ds0BitMap—DS0 channel number

For trunkingService or DS0Xconn: single bit input

For H248: multiple bits input (1-24 or 1, 5, 10-20)

T1: 1,2,3..24

E1: 1,2,3..31

ServiceType—service type

8 - Trunking

9 - H248

10 - DS0Xconn

BulkProvisionNumber—bulk provisioning number

Single DS0 configuration (range=1..8064(OC-3)/1152(T1)/1488(E1))(default=1)

Multiple DS0 configuration (range=1..336(OC-3)/48(T1E1))(default=1)

For 48T1/E1 cards the syntax of this command is the same as for OC-3 except that the LineNumparameter is expressed as:

LineNum—(bay.line)

bay {1 - upper, 2 - lower}

line (range=1..24)

Creating VXSM Trunks

In trunking non-switching applications, an AAL2 PVC connection needs to be created for each bearer trunk to be supported. In addition, provision must be made for transporting signaling information across the network. HDLC signaling is transported using separate AAL5 PVCs; SS7 signaling is carried in the AAL2 PVC using the AAL2 custom profile of 200. All these connections extend between the VXSM cards at the local and remote endpoints of the trunk.

Creating a Trunk Connection

To make connections between a local VXSM and a remote VXSM card, perform the following procedure. This procedure should be performed for each trunk to be supported by the media gateway Each trunk requires a PVC for a bearer circuit and, if used, a separate PVC for signaling.

Two connections types can to be created.

- The first type is AAL2 and is used for bearer circuits over the ATM network, up eight such PVCs can be configured.
- The second type is HDLC/AAL5 and is used for CCS signaling (when used).

For each connection, select one end of the trunk as the slave and the other end as the master.

Step 1 On the VXSM card at the slave end, use the **addcon** command to configure the slave end of the connection.

```
geteway1.5.VXSM.a > addcon <ifNum> <vpi> <vci> <serviceType> <pvcType> <application>
<mastership>
[-slave <NSAP.vpi.vci>] [-lpcr <local PCR>] [-rpcr <remote PCR>] [-lscr <local SCR>]
[-rscr <remote PCR>] [-lmbs <local MBS>]...
```

For ifNum specify 1 as the interface number. For vpi and vci specify values in the ranges 0 to 255 and 0 to 65535 respectively. For service type, specify 1 (constant bit rate) or 2 (vbr-rt).

For pvc type, specify 1 (AAL5) if the connection is for CCS signaling or specify 2 (AAL2) if the connection is for bearer.

For application specify 3 for a CCS signaling connection or 2 for a bearer connection.

For mastership specify 2 for slave.

Omit the - slave parameter. The gateway will assign a value and display it as NSAP.VPI.VCI. The user should note the value and use it when adding the master end of the connection on the AXSM.

Of the remaining optional parameters, enter values or accept the defaults. These parameters are best set from the master end. See the CLI chapter for details.

Step 2 On the VXSM card at the master end, use the **addcon** command to configure the master end of the connection.

```
geteway1.5.VXSM.a > addcon <ifNum> <vpi> <vci> <serviceType> <pvcType> <application>
<mastership>
[-slave <NSAP.vpi.vci>] [-lpcr <local PCR>] [-rpcr <remote PCR>] [-lscr <local SCR>]
[-rscr <remote PCR>] [-lmbs <local MBS>]...
```

For ifNum, specify 1 as the interface number. For vpi and vci specify values in the ranges 0 to 255 and 0 to 65535 respectively. For service type, specify 1 (constant bit rate) or 2 (vbr-rt).

For mastership, specify 1 for master.

For the -slave parameter, enter the NSAP.VPI.VCI that was noted when configuring the slave end of the connection.

Of the remaining optional parameters, enter values or accept the defaults. See the CLI chapter for details.

Note The PVC connections must be configured such that Connection Admission Control (CAC) mastership/slave follows that of the Connection Mastership/Slave.

Step 3 The path between the two VXSM cards, including the ports on the gateway AXSM cards and the intervening nodes is determined by PNNI. Use the **dsppnport** command to check that the ports on the gateway AXSM cards are enabled and configured for NNI.

Step 4 For each AXSM port that may be used as a trunk, use the **cnfpnportsig** command to setup the PNNI signaling on that port.

The port must be down to use this command. When a port is first created, its administrative state is down, in which there is no need to down it. If the port is up, do the following:

1. De-activate the port by using the **dnpnport** command.
2. Modify parameters as needed by using the **cnfpnportsig** command.
3. Activate the port by using the **uppnport** command.

Use the cnfpnportsig command to configure the port as signaling NNI.

The syntax of this command is:

cnfpnportsig <*portid*> [-**univer** {uni30 | uni31 | uni40 | q2931 | none | self}] [-**nniver** {iisp30 | iisp31 | pnni10 | enni | aini}] [-**unitype** {public | private}] [-**addrplan** {both | aesa | e164}] [-**side** {user | network}] [-**vpi** <*vpi*>] [-**sigvci** *signalling-vci*] [-**rccvci** *routing-vci*] [-**cntlvc** {ip}] [-**passalongcap** {enable | disable}] [-**hopcntgen** {enable | disable}] [-**vpivcialloc** {enable | disable}] [-**svcroutingpri** <*priority*>]

Table 4-2 cnfpnportsig parameters

portid	The format of the PNNI physical port identifier is as follows: • On a PXM45: *slot:subslot.port:subport*
-univer	UNI is the default for a new PNNI port, but no default *version* exists for UNI. The UNI version can be **uni30**, **uni31**, **uni40**, **q2931**, **none,** or **self**. Note that to change a UNI version, the port must be down. After configuration, up the port by using the **uppnport** command. Default: no default
-nniver	The NNI version: **iisp30**, **iisp31**, **pnni10**, **aini**, or **enni**. Note that *univer* and *nniver* are mutually exclusive—so the interface at each end of the connection must have the same interface type. Also, the port type on the PNNI controller must be the same as on the slave (through **addport** *ifType* on the AXSM, for example). The default for this parameter is PNNI 1.0. If this version is sufficient, you can forego this parameter. However, to change an NNI version, the port must be down. Remember to up the port by using the **uppnport** command after completing the **cnfpnportsig** command.
-unitype	The type of UNI is either private or public. This parameter is relevant only if you specified a UNI interface through the -**univer** parameter. Default: no default
-addrplan	The address plan of the calling party that the interface accepts. The choices are **both**, **e164**, and **aesa**. The default is **both**. Only a public UNI can use this parameter.
-**side**	For the side of the port, type **user** or **network**. When you set up PNNI signalling for IISP, one end must be *network* and one end must be *user*. If both sides are the same, a configuration error has occurred. This parameter applies to IISP only and public UNI. The network side is the side that assigns the VPI and VCI. (An NNI automatically is the network side.) Default: **network**

Table 4-2 cnfpnportsig parameters (continued)

-**vpi**	The VPI of the signaling and routing control channel (RCC) on the port. Range: 0–4095 Default: 0
-**sigvci**	The signaling VCI for the port. If you do not use the default of 5, this VCI must be in the range 32–65535. Range: 5 or 32–65535 Default: 5
-**rccvci**	The *routing control channel-vci*: the VCI for PNNI RCC. If you do not use the default of 18, this VCI must be in the range 32–65535. Range: 18 or 32–65535 Default: 18
-**cntlvc**	Enable for an IP-based signaling channel. This option applies only to a feeder connected to the switch. An IP-based control channel is mutually exclusive of either UNI or NNI. The only choice for -**cntlvc** is "ip." Default: "ip" (for Internet Protocol)
-**passalongcap**	Pass-along capability: type "enable" or "disable." With this capability, the port has the ability to pass along unrecognized information elements (IEs) or messages. Enabling or disabling the pass-along capability applies to AINI, IISP, and public UNI. For all other types, the port behaves as if pass-along is enabled—you cannot disable pass-along on the other port types. Default: enable
-**hopcntgen**	This parameter applies to AINI only. Type the entire word, "enable" or "disable." If you enable hop counting for AINI, the controller generates the hop counter information IE for all setup messages that pass through the interface if this IE does not already exist in the setup message. You must also enable AINI hop count IE for the switch by using the **cnfainihopcount** command. Default: enable
-**vpivcialloc**	This parameter applies to AINI: type "enable" or "disable." If you enable it, the interface becomes responsible for assigning the VPI and VCI for all connections. Note that if you enable VPI/VCI allocation on one side of the AINI link, allocation must be disabled on the other side of the link, Default: enable
-**svcroutingpri**	The -**svcroutingpri** option lets you specify a default routing priority for a port. This parameter becomes relevant when a setup message for an SVC or SPVC arrives with no PSIE at a node that supports priority routing. For example, the PSIE may have been dropped at a via node that does not support priority routing. In such a situation, the value for **svcroutingpri** becomes the routing priority for the connection. See the **cnfpri-routing** description for details on priority routing. The routing priority is used during de-routing. SVCs and SPVCs are released according to the routing priority. This release prioritization promotes faster re-routing of higher priority connections. Range: 1–15 Default: 8

The configuration of the port can be checked by using the **dsppnportsig** command.

```
M8850_NY.7.PXM.a > dsppnport 1:2.1:1

Port:               1:2.1:1           Logical ID:       16848897
IF status:          up                Admin Status:     up
UCSM:               enable
Auto-config:        enable            Addrs-reg:        enable
IF-side:            network           IF-type:          nni
UniType:            private           Version:          pnni10
PassAlongCapab:     n/a
Input filter:       0                 Output filter:    0
minSvccVpi:         0                 maxSvccVpi:       200
minSvccVci:         35                maxSvccVci:       255
minSvpcVpi:         1                 maxSvpcVpi:       200

       #SpvcCfg:  #SpvcActive:  #SpvpCfg:  #SpvpActive:
p2p :  0          0             0          0
p2mp:  0          0             0          0
       #Svcc:     #Svpc:        Total:
p2p :  0          0             0
p2mp:  0          0             0
                                Total:     0
```

Configuring AAL2 Trunks

When an AAL2 bearer trunk has been established, it can be configured further using the following commands.

CIDs

Each voice channel must be assigned a channel identifier (CID) for transport across the AAL2 trunk.

Note Configure subcell multiplexing before adding a CID. See next section.

Use the **addcid** command to create a CID and associate it with a ds1/ds0 voice stream. For OC3 cards, the format of this command is:

addcid *<ifIndex> <VPI> <VCI> <CID> <bay.line> <Ds1PathIndex> <Ds0 Group Index> <Profile Type><Profile Number> <Voice Codec> <VBD Codec><Repetition>*

For T1/E1 systems the format of this command is:

addcid *<ifIndex> <VPI> <VCI> <CID> <bay.line.> <Ds0_Group_Index> <Profile_Type> <Profile_Number> <Voice_Codec> <VBD_Codec>*<Repertition>

The vpi and vci parameters must be the vpi and vci of the AAL2 PVC. The CID must be a value between 8 and 255. The vci.vpi,CID combination, uniquely defines a channel in a specified PVC and associates it with a specified ds1/ds0 voice channel.

Profile Type
This parameter specifies the ATM AAL2 profile type for the AAL2 CID.

The valid values are as follows:
1 = ITU
2 = Custom

Profile Number
This parameter specifies the ATM AAL2 profile number for the AAL2 CID.

The valid value are as follows:

For the ITU profile type—1, 2, 3, 7, and 8.
For custom profile type—100. 101, 110, and 200.

When the AAL2 connection is used to transport SS7 signaling, select profile type 200.

Voice Codec
This parameter specifies the voice codec used for an AAL2 voice trunking connection.

The valid values are:
2 = G.729a
3 = G.726-16
4 = G.726-24
5 = G.726-32
6 = G.711u
7 = G.711a
13 = G.729ab
18 = Clear channel
19 = G.726-40

When the AAL2 connection is used to transport SS7 signaling, select 2 = Clear channel.

VBD Codec
This parameter specifies the voice band data codec used in an AAL2 voice trunking connection.

The valid values are:
1 = None (default)
2 = G726r32k
3 = G726r40k
4 = G711u
5 = G711a

Repetition

Once a CID has been created, it can be reconfigured using the **cnfcid** command.

For the VXSM OC3 card:

cnfcid <*ifIndex*> <*VPI*> <*VCI*> <*CID*> <*Profile Type*> <*Profile Number*> <*Voice Codec*> <*VBD Codec*>

For the VXSM T1/E1 card:

cnfcid <*ifIndex*> <*VPI*> <*VCI*> <*CID*> <*Profile Type*> <*Profile Number*> <*Voice Codec*> <*VBD Codec*>

Subcell Multiplexing

With subcell multiplexing, a partially filled cell can be filled with data from another CID. This makes a more efficient use of the bandwidth of the PVC. The partially filled cell is delayed for this purpose but only for a specified period. When the period is up and the cell is still partially filled, it is sent unfilled.

Use the **-ctimer** parameter in the **addcon** or **cnfcon** command to specify the period that an unfilled cell will wait before being transmitted. The wait period is in the range 0 to 50. Configuring the subcell multiplexing feature must be performed before adding CIDs to the connection.

Upspeed

VXSM supports detection of FAX and Modem devices attached to the TDM (trunk) side. The following tones are supported:

- V.21 preamble fax tone
- V.25 (CED) modem/fax tone 2100 Hz (with or without phase reversal)

VXSM uses the standard user-state control packets. indicating the change to voiceband data (VBD). The user-state control packets are sent as type 3 packets with triple redundancy.

Upon detection of a modem or fax tone, the master end of the connection performs a CAC check. If successful, it upspeeds to a less complex codec (for example, G.711) to accommodate the voiceband data.

The CAC is performed by the master end of the connection (the CAC-Master). The CAC-Master is specified by the user in the **addcon** command using the -**cmaster** parameter.

The upspeed codec is specified in **addcid** command using the **VBD_codec** parameter.

Configuring HDLC Signaling AAL5 Trunks for Nx64 Format

In trunking mode, HDLC signaling is transferred across the network as AAL5 connections. If the HDLC data stream conforms to an Nx64 format, the required configuration involves the following steps.

Step 1 Establish an Nx64 profile that can be used by Nx64 AAL5 connections.

addnx64prof <*profile_index*>[<*Nx64TransportMode*>][<*Nx64FrameFillPattern*>][<*InterFrameGapFlagCount*>] [<*Nx64BitInversion*>]

<profile_index>

Specify an index number that uniquely identifies a Nx64 profile entry.

The first entry (the value of this object is one) is used for default profile, it cannot be modified or deleted.

The value for this parameter is a number in the range 2 - 65535.

[<Nx64TransportMode>]

Specify the Nx64 packet stream transport mode as HDLC.

1 = hdlc (the Nx64 data the gateway receives are HDLC frames)

2 = transparent (the Nx64 data the gateway receives are unstructured bit stream and they will be transmitted to the network transparently)

[<Nx64FrameFillPattern>]

Specify the Nx64 HDLC frame start/end fill pattern.

1 = hdlcPattern (specifies 0x7E HDLC frame start/end bit pattern)

2 = idlePattern (specifies 0xFF IDLE bit pattern)

This parameter is applicable only when the transport mode is set to hdlc.

[<InterFrameGapFlagCount>]

Specify the HDLC interframe gap flag count.

A value of 0 means that only one flag is transmitted between a pair of frames and it is shared by them. In this case, the interframe flag is the start flag for frame (m) and the end flag for frame (m+1).

This object is only applicable when the transport mode is configured as 'hdlc', otherwise, the value of this object is ignored.

The valid value for this parameter is a number in the range from 0 – 15.

[<Nx64BitInversion>]

Specify whether or not bit inversion is turned on to support inverted HDLC functionality.

When this parameter is set to 'true', all the data stream on the Nx64 link is bit inverted

1 = true
2 = false.

Step 2 Establish an Nx64 AAL5 entry. Use the **asnx64aal5** command to create an Nx64 entity. This command associates a particular AAL5 connection with a physical interface and a Nx64 profile.

addnx64aal5 *<port><vpi><vci><bay.line.path.vtg/ds3.vt/ds1><ds0_group_number><nx64_profile>*

<port><vpi><vci><bay.line.path.vtg/ds3.vt/ds1>

These parameters identify the individual AAL 5 connection to be configured.

<port.>

This parameter is used to specify the port number of the Nx64 AAL5 entry.

The valid value for this parameter is the number 1.

<vpi><vci>

Specify the AAL5 connection to be configured. The vpi is a number in the range 1 - 255. The vci is a number in the range 1 – 65535.

<bay.line.path.vtg/ds3.vt/ds1>

Specify the DS0 path identifier to be used in adding a Nx64 AAL5 entry for the VXSM OC-3 card.

The valid values of this construct and their meaning are as follows:
bay = 1 – Designates the VXSM OC-3 card in the upper bay.
line = 1 – 4—Line number. Specifies one of four possible working lines for the OC-3 interface.
path = 1 – 3—Path identification number. Specifies the path identifier for the following path payload type:

vt1.5 payload—For T1 interface.
vt2.0 payload—For E1 interface.

Note T1 and E1 interfaces cannot be used simultaneously in conjunction with a VXSM card.

vtg/ds3 = 1 – 7—Virtual tributary group or 1 for ds3 path identification number.
vt/ds1 = 1 – 4—Virtual tributary or ds1 path identification number, as follows:

vt = 1 – 4—For T1 interface.
vt = 1 – 3—For E1 interface.
ds1 = 1—28.

ds0= 1 - 24 (T1)/1 - 31(E1)Specifies the DS0 path identifier to be used in adding a Nx64 AAL5 entry for the VXSM OC-3 card.

The valid values of this construct and their meaning are as follows:
bay = 1—Designates the VXSM OC-3 card in the upper bay.
line = 1 – 4—Line number. Specifies one of four possible working lines for the OC-3 interface.
path = 1 – 3—Path identification number. Specifies the path identifier for the following path payload type:

vt1.5 payload—For T1 interface.
vt2.0 payload—For E1 interface.

Note T1 and E1 interfaces cannot be used simultaneously in conjunction with a VXSM card.

vtg = 1 – 7—Virtual tributary group path identification number.
vt = 1 – 4—Virtual tributary path identification number, as follows:

vt = 1 – 4—For T1 interface.
vt = 1 – 3—For E1 interface.

ds0= 1 - 24 (T1)/1 - 31(E1)

<ds0_group_number>

Specify a number that uniquely identifies a DS0 group containing one or more DS0 that connect to an AAL5 trunking connection.

This object is mandatory when adding an AAL5 entry. Once an AAL5 entry is added, this object can not be modified.

The valid value for this parameter is a number in the range 1 - 31

<nx64_profile>

Specify the Nx64 data profile for an AAL5 trunking connection

The value for this parameter is a number in the range 1 - 65535.

Step 3 Steps 1 and 2 above can be repeated for Nx64 profile and entry needed to support the application.

Configuring More Features

In addition to the features described so far in this chapter, there are many more VXSM features that can be configured by the user. Refer to Chapter 5 in this guide to see configuration details of these additional features. Such features include:

- Clocking
- Connection Admission Control (CAC)
- Network Bypass
- Differentiated Services
- Fax/Modem Services
- Jitter Compensation

CHAPTER 5

Configuring VXSM Features

Configuring T1/E1 and T3 Lines

VXSM permits the user to configure many parameters associated with a physical T1, E1, or T3 line. To configure a line:

Step 1 Use the **cnflnoos** command to take the line out of service.

Step 2 Use the **dspln** command to display the current configuration of the line, for example

```
dspln <bay.line>
```

Step 3 Determine which parameters need to be changed,

Step 4 Use the **cnfln** command to change the required parameters.

For T1/E1 lines, this command is:

cnfln <*bay.line*> [< **-lt** *LineType* >] [< **-sc** *SendCode* >] [< **-lpb** *Loopback* >] [< **-signal** *SignalMode*>][< **-detect** *LoopbackCodeDetection* >] [< **-lc** *LineCoding* >] [< **-len** *LineLength* >] [< **-lm** *LineMod*>} [< **-lbo** *LineBuildOut* >] [< **-rep** *Repetition* >]

For T3 lines, this command is:

cnfln <*bay.line*> [**-lt** <*LineType*>] [**-sc** <*SendCode*>] [**-lc**<*LineCoding*>] [**-len**<*LineLength*>] [**-lpb** <*Loopback*>] [**-clock** <*TxClockSource*>]

Step 5 Use the **dspln** command to display the new parameter values and verify that they are correct.

Step 6 Use the **cnflnis** command to bring the line into service.

Step 7 Use the **upln** command to bring up the line.

The BERT (bit error rate testing) and alarm parameters can also be configured for the line using the **addbert**, **cnfbert** and **cnflnalm** commands

Configuring SONET Lines and Paths

VXSM permits the user to configure many parameters associated with a physical SONET line/path.

To configure a SONET line, perform the following procedure.

Step 1 Use the **dnln** command to down the OC-3 line

Step 2 Use the **dspln** command to display the current configuration of the line, for example

```
dspln n.m (where n is bay and m is the line number)
```

Step 3 Determine which parameters need to be changed,

Step 4 Use the **cnfln** command to change the required parameters.

cnfln *bay.line* [< **-slt** *MediumType* >] [< **-lpb** *LoopbackType* >] [< **-sfs** *FrameScramble* >] [< **-rdiv** *DIVType* >][< **-rdip** *RDIPType* >] [< **-txtrace** *TraceToTransmit* >] [< **-extrace** *TraceToExpect* >]

Note The **cnfln** command configures parameters at the physical OC-3 level only. To configure parameters at the path (ds1) level, use the cnfpath command.

Step 5 Use the **dspln** command to display the new parameter values and verify that they are correct.

Step 6 Use the **upln** command to up the OC-3 line.

To configure a SONET path, perform the following procedure.

Step 1 Use the **cnfpathoos** command to take the path out of service.

Step 2 Use the **dsppath** command to display the current configuration of the path, for example

`dsppath` [< *bay.line.path.vtg.vt* >] | [< *bay.line.path.ds1*>]

Step 3 Determine which parameters need to be changed.

Step 4 Use the **cnfpath** command to change the required parameters.

This command has several versions depending upon the path type (ds1, ds3, e1, or sts). As an example, the ds1 version has the format:

cnfpath -ds1 [*bay.line.path.vtg.vt*] | [*bay.line.path.ds1*] [***-lt*** <*LineType*>] [***-sc*** <*SendCode*>] [***-lpb*** <*Loopback*>] [***-signal*** <*SignalMode*>] [***-detect*** <*LoopbackCodeDetection*>] [***-rep*** <*Repetition*>]

Note VXSM supports two numbering schemes for mapping DS1 circuits to their vtg/vt values. These two schemes are known as standard and Titan. See next section for details.

Step 5 Use the **dsppath** command to display the new parameter values and verify that they are correct.

Step 6 Use the **cnfpathis** to bring the path into service.

VTG/VT to DS1 Mapping Scheme

For applications using the SONET-VT1.5/SDH-VC11 payload path type, VXSM supports two numbering schemes for mapping VTG/VT pairs to DS1s.

The first scheme conforms to ITU-T GR 253 (also Bellcore Std. TR 253) and is referred to as the ‘standard’ scheme.

The second scheme supports certain types of DACS equipment (for example Tellabs 5500 DACS). This scheme is referred to as the Titan scheme (also referred to as the M13 count method).

With this feature, the user can specify which numbering scheme is to be used.

This feature adds two new CLI commands; one to display the currently selected mapping scheme and one to change the mapping scheme.

The SONET-VT1.5/SDH-VC11 payload path type supports 7 VTGs each containing 4 VTs for total of 28 DS1s.

Standard Scheme

In the ITU-T GR.253 spec, the VTG-VT number pairs are incremented such that the VTG number increments from 1-7 before the VT number is incremented. That is, the first VTG-VT pair is 1-1, the second pair is 2-1, the third pair is 3-1, and so on, up to 7-1. The next pair is 1-2, followed by 2-2, 3-2,4-2 ..7-2, then 1-3, 2-3..7-3 and so on until 1-4, 2-4..7-4.

Titan Scheme

In the Titan (M13 Count) numbering scheme, VTG-VT number pair are incremented such that the VT increments from 1-4, before the VTG is incremented. That is, the first VTG-VT pair is 1-1, the second pair is 1-2, and so on up to 1-4. The next pair is 2-1, followed by 2-2, 2-3, 2-4, then 3-1, 3-2, 3-3, 3-4 and so on until 7-1, 7-2, 7-3, 7-4.

The complete mapping schemes are shown in Table 5-1.

Table 5-1 VTG/VT to DS1 Mapping

DS1	Standard, ITU-T GR 253		Titan, M13 Count	
	VTG	VT	VTG	VT
1	1	1	1	1
2	2	1	1	2
3	3	1	1	3
4	4	1	1	4
5	5	1	2	1
6	6	1	2	2
7	7	1	2	3
8	1	2	2	4
9	2	2	3	1
10	3	2	3	2
11	4	2	3	3
12	5	2	3	4
13	6	2	4	1
14	7	2	4	2
15	1	3	4	3
16	2	3	4	4

Table 5-1 VTG/VT to DS1 Mapping (continued)

DS1	Standard, ITU-T GR 253		Titan, M13 Count	
	VTG	VT	VTG	VT
17	3	3	5	1
18	4	3	5	2
19	5	3	5	3
20	6	3	54	4
21	7	3	6	1
22	1	4	6	2
23	2	4	6	3
24	3	4	6	4
25	4	4	7	1
26	5	4	7	2
27	6	4	7	3
28	7	4	7	4

User Interface

The VTG/VT to DS1 mapping feature uses the following two CLI commands.

- Display VT mapping

  Syntax: **dspvtmapping**

  This command displays the current setting of VTG/VT to DS1 mapping scheme, values are standard or Titan. Standard denotes ITU-T GR 253, Titan denotes M13 count.

- Configuring VT mapping

  Syntax: **cnfvtmapping** <VtMappingMode>

  1—standard (default)

  2—titan

  This command switches the current setting of VTG/VT to DS1 mapping scheme to the alternative scheme.

Note To execute the **cnfvtmapping** command:

1. The cnfvtmapping command is valid on the VXSMOC-3 card only.
2. All SONET lines on the card must be down.
3. All SONET lines on the card must be configured with medium type as sonet.
4. All SONET paths on the card must be configured as VT1.5.

Note When VT mapping mode is set to titan, the following commands are affected on the VXSM OC-3 card.

cnfln: the option -slt (medium type) are rejected

cnfpath -sts: the options -payload and -tg are rejected

In Titan mode, the DS1 path order will be changed in the following commands (see Table 5-1 for path order).
CLI: dsppaths -ds1
dsppathalms -ds1
dsppathstates (for ds1 only)
dspvif***s (for ds1 only)
dsplapds (for ds1 only)
dspberts -ds1
dspds0xcons (for ds1 only)

Configuring Clocking

The clock for the media gateway can be one of the following sources.

- A BITS clock source received on the PXM-45 back card on ports 35 and 36 using an E1 or T1 RJ-48 connector. In a redundant configuration, a Y-cable is for the BITS clock.
- The PXM internal oscillator (stratum 3 circuit on PXM-45 back card)
- A Clock derived from VXSM line or AXSM line

The clock source is configured on the active PXM card using the **cnfclksrc** command.

The syntax of this command is:

cnfclksrc <*priority*> <*portid*>[***-bits*** { e1|t1 } *][**-revertive** { enable|disable }]*

where:

priority—This is either primary or secondary (default = primary)

portid—The specification of the port ID depends upon the selected clock source.

If the BITS clock source is selected, portid is specified as:

[shelf.]slot.port

shelf—always 1 and is purely optional.

- slot—the logical slot number 7 for a BITS circuit on the PXM UI S3 (regardless of where the active PXM resides).
- port—a logical number that indicates the upper or lower external clock connector on the UI S3 back card. The logical port number for the upper connector is 35. The lower connector is 36.

If a service module line is selected as the source, portid is specified as:

- [shelf.]slot:subslot.port:subport
- shelf—always 1 and optional.
- slot —the slot number of the service module.
- subslot—identifies the upper or lower bay of the back card, either a 1 for the upper bay or 2 for the lower bay (default is 1).
- port—is the line number on the service module back card. (The specified line must already be active (see upln).
- subport—is the logical port number. This value is the logical port (or ifNum) that you must have assigned through **addport**. Also, the logical port must be known to PNNI (see **dsppnports**).

Note When specifying a clock source on a VXSM card, the value 10 must be added to both the line and logical port numbers. For example, a primary clock source on a VXSM in slot 3, upper shelf, line 1, logical port 1 would be specified as:

cnfclksrc primary 3:1.11:11

- -**bits**—This keyword parameter is required if slot number 7 and port number of 35 or 36 are specified in portid (indicating BITS as the clock source) Type the string **-bits**, followed by a space, then either **e1** or **t1**.
- -**revertive**—An option that applies to only the BITS clock. Type the string **-revertive**, followed by the complete word **enable** or **disable**. The default is **disable**.

Step 7 Use the **cnfclksrc** command again to configure the secondary clock source.

Step 8 Use the **cnfclkparms** command to configure the signal type and cable type for BITS sources (if applicable). The configuration applies to both (upper and lower) lines.

The syntax of this command is:

cnfclkparms <*signal type*> <*cable type*>

where:

signal type, 1 = data; 2 = syn (this parameter is not supported in this release)

cable type, 1 = twisted; 2 = coax

Note E1 lines can be either twisted pair or coaxial cable. T1 lines must always be specified as twisted pair.

Below is an example of a sequence of clock configuration commands.

```
8850japan.7.PXM.a > cnfclksrc primary 7.35 -bits t1 -revertive enable
8850japan.7.PXM.a > cnfclksrc secondary 7.36 -bits t1 -revertive enable
8850japan.7.PXM.a > cnfclkparms 1 1
```

Confirm the clock source using the **dspclksrc** command.

On the PXM card, use the **dspclksrcs** command to display the clocking configuration.

For example:

```
8850japan.7.PXM.a > dspclksrcs
Primary clock type:     bits t1
Primary clock source:   7.35
Primary clock status:   bad
Primary clock reason:   no clock
Secondary clock type:   bits t1
Secondary clock source: 7.36
Secondary clock status: bad
Secondary clock reason: no clock
Active clock:           internal
source switchover mode: revertive
```

Appendix A in this document covers the subject of clocking in greater detail.

Connection Admission Control

Connection admission control (CAC) is configured when an ATM connection is added using the **addcon** command. CAC is applied depending upon the values specified for the service type, peak cell rate (PCR), and sustained cell rate (SCR) parameters.

These parameters permit you to specify the bandwidth (expressed as a cell rate) requirements for the virtual circuit being added. If the specified bandwidth is not available, the connection is denied.

The addcon command has four parameters for specifying required cell rate:

- -lpcr
- -rpcr
- -lscr
- -rscr
  - l—Means in the local to remote direction
  - r—Means remote to local direction

The four parameters allow the user to specify PCR and SCR values for the PVC in each direction.

If the service type is specified as CBR (constant bit rate), PCR values are used as maximum bandwidth requirements otherwise, SCR values are used as available bandwidth requirements.

To facilitate the CAC function, VXSM performs load balancing on all PVCs configured on the card.

Configuring Redundancy

VXSM provides the following redundancy features.

1:1 Front card/back card redundancy

1:1 APS SONET line redundancy

1+1 APS SONET line redundancy

PVC channel protection

1:1 Front Card/Back Card Redundancy

VXSM front and back cards can be configured for redundancy provided they are installed in adjacent slots (for example, 1 and 2, 9 and 10).

On the PXM card execute the **addred** command.

```
addred <redPrimarySlotNum> <redSecondarySlotNum> <redType>
```

redPrimarySlotNum and *redSecondarySlotNum* should be specified as the slot number of the active card andthe standby card respectively.

<redType> is redundancy type where redType = 1(1:1 Y-Cable) or 2(1:N). Enter 1 for Y-cable.

APS SONET Line Redundancy

To setup a working/protection line pair, use the **addapsln** command. This command allows the user to specify an OC-3 port as a working line and a corresponding OC-3 port as a protection line. 1:1, 1+1, and 1+1 Annex B protection types are supported.

To configure 1:1 or 1+1 line redundancy perform the following steps.

Step 1 Use the **addapsln** command to setup a working protection line pair.

addapsln <*working line*> <*protection line*> <*archmode*>

Working line and protection line are expressed as *slot.bay.line*.

For working line, slot = physical slot of working line, bay = 1 (upper), line in the range of 1 to 4

For protection line, slot = physical slot of protection line, bay = 1 (upper), line in the range of 5 to 8

For archmode, 1 = (1+1), 2 = (1:1), 3 = (1+1AnxB)

Note 1+1 and 1+1AnxB are supported on the same card or across 2 card slots. 1:1 is supported only on the same card,.

Step 2 Use the **cnfapsln** to configure aps fault thresholds and other parameters.

cnfapsln <working line> [-**sf** <SigFaultBER>] [-**sd** <SigDegradeBER>]
[-**wtr** <WaitToRestore >][-**dr** <Direction>] [-**rv**< Revertive>] [-**proto** <Protocol>]

working and protection lines are expressed as slot.bay.line of the working line (see addapsln above).

SigFaultBER and sigDegradeBER are bit error rates for fault detect and fault degrade detect respectively. If these rates are detected, switchover takes place.

SigFaultBER
This is an integer n in the range from 3 – 5, with a default value of 3. This parameter represents a value of 10^{-n}, where n is 10^{-3} to 10^{-5}.

sigDegradeBER
This is an integer n in the range from 5 – 9, with a default value of 5. This parameter represents a value of 10^{-n}, where n is 10^{-5} to 10^{-9}.

Waittorestore
This parameter defines the interval in minutes to wait before attempting to switch back to the working line after a switchover (not applicable if the line is configured in non-revertive mode). The range is 1 to 12 minutes.

The framer clears the signal-fault and signal-degrade states when the APS switchover occurs.

The permissible value of this parameter is an integer in the range from 1 – 12.

Direction
This parameter configures the switching direction that this APS line will support.

1 = Unidirectional—On a failure, only that direction fails over.

2 = Bidirectional—On a failure, both directions fail over.

Revertive
This parameter is used to configure the APS revertive or nonrevertive mode.

1 = Nonrevertive mode—The protection line continues to be the active line. The active line does not switch to the working line.

2 = Revertive mode—Switches the working line back to the active state after the wait-to-restore interval has expired and the working line signal-fault/signal-degrade state has been cleared.

Protocol
This parameter configures the APS channel protocol to be implemented at the near end terminal.

The K1 and K2 overhead bytes in a SONET signal are used as an APS channel to effect the APS protocol.

1 = Bellcore—The APS channel protocol is implemented as defined in the Bellcore document GR-253-CORE.

2 = ITU—The APS channel protocol is implemented as defined in the ITU document G.783, Annex A.

PVC Channel Protection

Perform the following procedure to configure a dual PVC pair in which a primary PVC is protected by a secondary PVC.

Step 1 Create the primary PVC using the **addcon** command.The -pref parameter is used to specify whether the PVC is a primary, secondary, or none. Specify 1 for primary.

Step 2 Create the secondary PVC using the **addcon** command.The -pref parameter is used to specify whether the PVC is a primary, secondary, or none. Specify 2 for secondary.

Note The primary PVC should be added first and then the secondary. When a PVC is deleted, the secondary should be deleted first. The PCR and SCR values for the primary and secondary PVCs must be the same.

Changing the preference of a PVC from secondary to primary or unknown and from primary of unknown to secondary are not allowed. Only primary to unknown and unknown to primary are allowed.

Step 3 Use the **cnfconprotect** command to configure the protection.

cnfconprotect *ifNum vpi vci protect fallbackPort fallbackVpi fallbackVci*

ifNum
This is the interface number of the PVC, specify 1

vpi, vci
These are the vpi and vci values of the already created PVC.

fallbackPort
This specified whether protection is to applied or not. 1 = protect, 2 = no protection (default).

fallbackVpi, fallbackVci
These are the vpi and vci values of the fallback PVC

Step 4 Use the **cnfoamparams** command to configure the operation, administration, and management (OAM) cells for a dual PVC protection group.

cnfoamparams *gap retry recover*

gap
This parameter defines in milliseconds the inter-cell gap for dual PVC (DPVC) operation, administration, and management (OAM) cells. The permissible range is 20 – 5000, with a default value of 5000.

retry
This parameter defines the retry threshold (in number of cells) during a PVC failure.

When the number of consecutive OAM cells being sent without receiving an acknowledgment (ACK) is equal to the value of this parameter, switchover occurs.

The permissible range is 0 – 20, with a default value of 3.

recover
This parameter defines the threshold (in number of cells) for recovery of a failed PVC.

The permissible range is 0 – 20, with a default value of 5.

When the number of consecutive OAM cells being sent while receiving an acknowledgment (ACK) is equal to the value of this parameter, the failed PVC is considered to have recovered from its failed state.

Note PVCs cannot be deleted while they are part of a dual PVC protection group and while they are active. To delete a PVC, first use cnfconprotect to set the group to unprotected (fallbackPort = 2). Then use the **dncon** to make the secondary PVC inactive, delete the secondary PVC and the primary PVC.

Configuring PRI Backhaul

In switching applications, VXSM is able to extract Q.931 signaling frames from an ISDN PRI D channel and backhaul them to the media gateway controller for processing (this feature is described in Chapter 2). Configuration of this feature consists of the following steps.

Step 1 Establishing a communication link between the VXSM and the media gateway controller. This communication link can is based upon a RUDP (Reliable UDP) session set.

Step 2 Establishing an LAPD session between VXSM and the voice TDM network.

Configuring RUDP

To configure an RUDP session between VXSM and the media gateway controller, perform the following steps.

Step 1 Establish IP connectivity with the media gateway controllers (see Chapter 2 for details).

Step 2 Use the **addsesset** command to create a session set.

```
addsesset <set number> <fault tolerant>
```

set number
Integer value of 1 (currently only session set is supported)

fault tolerant
Integer value

1 = fault tolerant

2 = nonfault tolerant

Step 3 Use the **adddnsdn** command to add the domain server domain name

```
adddnsdn <Domain Name>
```

Step 4 Use the **adddnssrvrip** command to add the IP address of the domain server

```
adddnssrvrip 1 172.29.66.35
```

Step 5 Use the **addmgcdn** command to ass the domain name of the media gateway controller

```
addmgcdn 1 mgc7
```

Step 6 Use the **addsesgrp** command to create each session group

```
addsesgrp <group number> <set number> <mgcname>
```

group number
Integer value of 1 or 2 (specify 1 for non-fault tolerant mode or 2 for fault tolerant mode).

set number
Integer value of 1(only 1 is supported)

mgcname
Domain name of the call agent (a text string of 1-64 characters.

Step 7 Use the **addses** command to create each RUDP session. Each session group can have up to four sessions.

```
addses <session number> <group number> <priority> <local port> <remote port>
```

session number
Integer value (1 to 8)

group number
Integer value (1 or 2)

priority
Integer value in the range of 1 to 4. A lower number means higher priority.

local port
Integer value in the range of 1124 to 65535

remote port
Integer value in the range of 1124 to 65535

Step 8 For each session that has been created, the session parameters can be further configured using the commands in Table 5-2 (see Chapter 6 for CLI details).

Table 5-2 RUDP Session Commands

Command	Configures the…
cnfsesport	Local port/remote port values. The <local port, remote port and Remote IP address> combination must be unique across the group.
cnfsesmaxwindow	Maximum number of segments that can be sent without receiving an acknowledgement for a specific RUDP session.
cnfsessyncatmpts	Maximum number of attempts to synchronize with MGC for a specific RUDP session.
cnfsesmaxseg	Maximum number of octets to synchronize with VSC for a specific RUDP session.
cnfsesmaxreset	Maximum number of autoresets that are performed before a connection is reset.
cnfsesretrans	Timeout value for retransmission of unacknowledged packets in millisecondes and the maximum number of times consecutive retransmission are attempted before the connection is considered broken.
cnfsesack	Timeout value to send out an acknowledgment and the maximum number of acknowledgments that are accumulated before sending an acknowledgment.
cnfsesoutofseq	Maximum number of out of sequence packets that are accumulated before sending an EACK segment is sent. A value of 0 indicates an DACK is sent immediately if an out of order segment is received.
cnfsesnullsegtmout	Number of milliseconds of idle time before sending a null segment.
cnfsesstatetmout	Number of milliseconds of idle time before sending a null segment.

Configuring LAPD

To configure a LAPD parameters for a DS0 used for ISDN D channel, perform the following steps.

Step 1 Use the **addlapd** command to create an LAPD session on a specified DS0.

```
addlapd <bay.line.path.vtg.vt:ds0>|<bay.line.path.ds1:ds0>|<bay.line>:<ds0>[-side
<LAPDside>][-type <Type>][-window <WindowSize>]{-n200<n200>}[-t200 <Timer200>][-t203
<Timer203>][-ds0 <Ds0Format>][-profile <IsdnHdlcProfile>][-as <AS Name>][-appltype
<AppType>]
```

Use one of these formats to specify the DS0 on an OC-3 card:

<bay.line.path.vtg.vt:ds0> |<bay.line.path.ds1:ds0>

bay: 1

line: 1 - 4

path: 1 - 3

vtg: 1 - 7

vt: 1 - 4(T1)/3(E1)

ds1: 1 - 28

ds0: 1-24 (T1) 1-16(E1) for RUDP
1-24 (T1) 1-31(E1) for SCTP

Use this format to specify the DS0 on a T1/E1 card

<bay.line>:<ds0>

bay: 1

line: 1 - 4

ds0: 1 - 24 (T1), 1 - 16(E1)

The following parameters are the same for both OC-3 and T1/E1 cards.

side <LAPDsid>

Specify whether the LAPD stack is at user side or network side

1 - network

2 - user

-type <Type>

Specify the switch type at the remote end of the ISDN line.

1 - CCITT

3 - AT&T 5ESS PRA

4 - AT&T 4ESS

6 - NT dms100 PRA

7 - VN 2 or VN 3

8 - INS Net

9 - tr6 MPC

10 - tr6 PBX

12 - Austel Primary

13 - National ISDN-1

14 - ETSI

15 - NT dms250

16 - Bellcore

17 - National ISDN-2

-window <WindowSize>

Specify the maximum number of sequentially numbered I-frames that may be outstanding

1..128 (default=7)

-n200 <n200>

Specify the maximum number of retransmissions of a frame

1..10 (default=3)

-t200 <Timer200>

Specify the maximum time to wait for acknowledgment of a transmit frame

100..1023000 ms (default=1000)

-t203 <Timer203>

Specify the maximum time in milliseconds allowed without frames being exchanged. This value should be greater than that for -t200

100..1023000 ms (default=1000)

-ds0 <Ds0Format>

Specify the DS0 format. 56k(1) is robbed-bit for T1.

1 - ds056k

2 - ds064k}

-profile <IsdnHdlcProfile>

Specify the HDLC profile which contains a list of HDLC attributes for the PRI backhaul connection

1..128 (default = 1)

-as <AS Name>

Specify the LAPD application server (AS) name (12 chars). An AS is a logical entity serving LAPD D-channel.Zero length string (size 0) means there is no AS association with this LAPD D-channel

This parameter is used for PRI backhaul using SCTP only and is not configurable for RUDP.

-appltype <AppType>

Specify the PRI backhaul application protocols as 1 or 2.

1 = sctp (default)

2 = rudp

Step 2 When an LAPD session has been created, the session parameters can be further configured using the commands in Table 5-3 (see Chapter 6 for CLI details).

Table 5-3 LAPD Session Commands

Command	Function
cnflapd	Modify an existing Lapd entry. The applType cannot be modified in this command. The line must be deleted and then added back again to change the applType.
dsplapdcnt	Display LAPD statistics counters
dsplapdhdlccnt	Display LAPD HDLC statistics counters

Configuring Announcements

In switching applications VXSM supports the feature in which pre-recorded announcements can be delivered in either direction (to the calling or called party) under the control of the MGC. These announcements can be played during call setup and after the call has been established. The announcement files must be available in the VXSM memory to be played out or, if the file is not resident in VXSM memory, VXSM uses TFTP to obtain the file from an external announcement server, caches it and plays it out.

To configure the Announcements feature, perform the following steps.

Step 1 It is the responsibility of the user to record all announcements and have them stored in PCM format as computer files in the announcement file server. The announcement file server must IP reachable from the VXSM.

Step 2 Use the **cnfanndn** command to specify the name of the announcement file server.

```
cnfanndn <ServerDomainName>
```

Step 3 Use the **cnfanncontrols** command to configure announcement parameters.

cnfanncontrols [**-path** <*SubDirPath* >] [**-dn** <*DomainNameResolution*>] [**-ip** <*ipAddress*>] [**-age** <*ageTime*>] [**-tout** <*ReqTimeOut* >] [**-per** <*maxPermanent*>]

SubDirPath is a string up to 64 characters that specifies the subdirectory path to the default TFTP directory in the announcement file server in which the announcement files are stored.

DomainNameResolution specifies how the domain name of the announcement file server is to be resolved.

- 1 = Internal only (default value)—Indicates internal resolution of domain name for announcement file server.
- 2 = External only—Indicates external resolution of domain name for announcement file server.

If this parameter is set to the value 1, the IP address associated with the file server is determined according to the value of the **-ip** *ipAddress* parameter.

- *ipAddress*—IP address for the announcement file server. If the *DomainNameResolution* is configured as external only, this item is ignored.
- *ageTime*—Time in minutes that an announcement remains valid after it is fetched into the VXSM announcement cache. The range is 1 to 1440. After arriving in the cache, an announcement is not refreshed until it is aged. Subsequent play announcement requests do not affect the agetime or cause the file to be refreshed from the server.
- *ReqTimeOut*—Time, in seconds, within which an announcement must start playing after the VXSM receives the announcement signal from the MGC. The default value is 5 seconds.
- *maxPermanant*—Maximum number, in the range 0 to 136, that permanent announcement files can be added to Media Gateway. The default value is 41. A value of 0 indicates that the age time function is disabled.

Step 4 Use the **addannfile** to map an announcement name number to the announcement filename. This command also lets you specify the number of times the announcement is to be played, whether the file is to be permanent or not, and the signal duration of the announcement file.

addannfile *cannoAudioFileNumber FileName* [**-noc** *numberOfCycles*] [**-type** *fileType*] [**-dur** *signalDuration*]

- *cannoAudioFileNumber*—An index value that identifies the announcement file to be used by the media gateway. The permissible value of this parameter is an integer in the range from 1 - 1024.
- *Filename*—Specifies the name of a valid announcement file that has been stored in the media gateway announcement table. This announcement file name, which can be composed of up to 64 characters, can incorporate path or subdirectory information
- *noc*—Specifies the number of times the announcement file is to be played.

  The permissible value of this parameter is an unsigned integer in the range from 0 - 65535, with a default value of 1.

  The value zero specifies that an announcement file is to be played or looped continuously.

  type—Specifies the type of the announcement file.

The integer value for this parameter must be one of the following:

- *1* = Dynamic file type (default)—A dynamic file can be removed from cache when the age of the file reaches a specified limit or in accordance with a least recently used (LRU) algorithm when the cache is full.
- *2* = Permanent file type—A permanent file can be stored in cache until it is deliberately deleted.

This parameter indicates the duration (in milliseconds) that the announcement file is to be played during an announcement cycle. This parameter is applicable only for purposes of playing a fixed announcement.

For fixed announcement play, the -noc *numberOfCycles* parameter and the -dur *signalDuration* parameter are used together to determine how long the announcement is to be played.

The permissible value for these parameters is an integer in the range from 0 - 65535.

A value zero for -dur indicates that the duration of the announcement is variable and that the **-noc** *numberOfCycles* parameter (see above) will be used to determine play time.

This parameter is used only when the Play Announcement signal from the MGC does not incorporate a parameter specifying the number of cycles that the announcement is to be played.

Step 5 Use the **cnfannfile** to configure a specific announcement file.

cnfannfile *cannoAudioFileNumber FileName* [**-noc** *numberOfCycles*] [**-dur** *signalDuration*]

- *cannoAudioFileNumber*—Index value that identifies the announcement file to be used by the media gateway. The permissible value of this parameter is an integer in the range from 1 - 1024.
- *Filename*—Specifies the name of a valid announcement file that has been stored in the media gateway announcement table. This announcement file name, which can be composed of up to 64 characters, can incorporate path or subdirectory information
- *noc*—Specifies the number of times the announcement file is to be played.

The permissible value of this parameter is an unsigned integer in the range from 0 - 2147483647, with a default value of 1.

The value zero specifies that an announcement file is to be played or looped continuously.

For fixed announcement play, the -noc *numberOfCycles* parameter and the -dur *signalDuration* parameter are used together to determine how long the announcement is to be played.

The permissible value for these parameters is an integer in the range from 0 - 65535.

A value zero for -dur indicates that the duration of the announcement is variable and that the -noc *numberOfCycles* parameter (see above) will be used to determine play time.

This parameter is used only when the Play Announcement signal from the MGC does not incorporate a parameter specifying the number of cycles that the announcement is to be played.

Configuring Network Bypass

Configuration for the Network Bypass feature consists of making a mesh of PVCs between VXSM and other cards in the gateway. When the mesh of PVCs is complete the feature is enabled through the **cnfnwbypass** command.

For each PVC in the following procedure the attributes of the PVC are:

- AAL5

- PVC type is bearer
- Traffic type: UBR
- Peak Cell Rate to support 24 OC-3s
- No CAC (all internal PVCs run over the shelf's backplane)
- Internal PVCs are not assigned IP addresses

In order to configure the media gateway for the Network Bypass feature, perform the following procedure.

Step 1 Create a PVC between each VXSM card and its associated RPM or AXS M card. Specify the attributes listed above. The procedure is to configure the slave end at the RPM or AXSM first and the master end on the VXSM second. Details are provided in Chapter 3, the section titled Creating Connections to the RPM-XF Card.

Step 2 For each VXSM card create one PVC to each of the other VXSM cards in the shelf. Use the **addcon** command and specify the attributes listed above. It does not matter which is the master and which is the slave.

Step 3 For each VXSM card create a single pvc for which the VXSM card is specified for both ends. Use the **addcon** command and specify the attributes listed above.

Step 4 By default, the network bypass feature is disabled. To enable the feature, enter the **cnfnwbypass** command on each VXSM card. The format of this command is:

cnfnwbypass <*nwbypass*>

nwbypass—Has the value 1, 2, or 3

1—disable (default)

2—unconditional enable

3—conditional enable

Conditional enable allows the MGC to control the use of this feature. It can explicitly, in a given call flow, ask for this attribute to be returned.

The current status of the network bypass feature can be shown by entering the **dspnwbypass** command.

Configuring Differentiated Services

For VoIP applications, VXSM provides support for the quality of service (QoS) feature known as Differentiated Services (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).

VXSM's support of this feature is to permits users to specify the values of the point code to be inserted into the IP header ToS field. The specified values are entered through the **cnfiptos** command and are applied card-wide. VXSM does not check the entered value nor does it understanding the meaning of the point code values. It is the responsibility of the network administrator to ensure that the routers understand how to process the point codes.

The **cnfiptos** commands allows you to specify ToS values for both control and bearer packets (although DiffServ is really confined to bearer packets). The command has the format:

cnfiptos <*ControlToS*> <*BearerToS*>

- *ControlToS*—An integer in the range of 0 to 255 with a default of 104
- *BearerToS*—An integer in the range of 0 to 255 with a default of 184

For the control path, the default of 104 maps to DiffServ Codepoint 011010 which is Assured Forwarding (AF31 PHB) for signalling/control (see RFC 2597 for more information)

For the bearer path, the default of 184 maps to Diffserv Codepoint 101110 which is Expedited Forwarding (EF) PHB or premium service. (see RFC 2598 for more information)

The current values of the ControlToS and the BearerToS parameters can be displayed using the **dspiptos** command.

Configuring Fax and Modem Services

VXSM supports the management of nonvoice services within a voice connection. VXSM supports the following two methods.

- Fax, modem, and TTY passthrough over a VoIP or VoATM network
- T.38 Fax relay over VoIP. Both Call Agent controlled and Gateway controlled methods are supported.

VXSM provides event-handling for the VBD events that are detected in the voice or IP interface of the media gateway. The event handling is mapped to different event handling functions that are defined in VBD profiles or fax relay profiles.

Configuring for nonvoice services consists of the following major steps.

1. Set up event mapping with pointers to fax/modem/TTY passthrough and fax relay profiles
2. Set up fax/modem/TTY passthrough profiles
3. Set up T.38 fax relay profiles
4. Associate voice interfaces with particular voiceband event mappings

Configuring Voiceband Event Mapping

The voiceband event mapping feature permits VXSM to determine how voiceband (VBD) events are to be handled. When this feature is configured, VBD events are mapped to different event handling functions defined in fax relay profiles and VBD profiles.

Perform the following procedure to configure a voiceband event mapping.

Step 1 VXSM automatically creates an event mapping table (index 1 for VoIP Switching, index 11 for AAL2 Trunking) that contains records for event mapping types and pointers to profiles. Use the **dspeventmapping** command to display the default values.

For fax/modem passthrough use **dspeventmapping -ced**

For TTY passthrough use **dspeventmapping -v18aTone**

For T.38 fax relay use **dspeventmapping -v21Tone, dspeventmapping -cngTone**

For low speed modem tones use: **dspeventmapping -v21Modem, dspeventmapping -v23Modem, dspeventmapping -bellModem,** or **dspeventmapping -v8bis** (the **-prof** and **-mode** parameters are not supported for low speed modems**.**

Step 2 If the default values must be changed, use the appropriate **cnfeventmapping** command.

For fax/modem passthrough use

cnfeventmapping -ced<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*HandleMode*>]

For TTY passthrough use

cnfeventmapping -v18aTone<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*HandleMode*>]

For T.38 fax relay use

cnfeventmapping -v21Tone<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

cnfeventmapping -cngTone<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

For low speed modem tones use:

cnfeventmapping -v21Modem<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

cnfeventmapping -v23Modem<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

cnfeventmapping -bellModem<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

cnfeventmapping -v8bis<*EventMappingIndex*>[**-htype** <*HandleType*>]
[**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

cnfeventmapping -bell202 <*EventMappingIndex*>[**-htype** <*HandleType*>]

The parameters for all these commands are the same.

EventMappingIndex—Identifies a set of voice data events supported by VXSM and how they are managed in the media gateway. The entries with value 1 of this object is the default handling for the voice data events in the media gateway.

-**htype**<*HandleType*>—This object specifies the type of the handle function in response to this event detection. The value none specifies that the handling of this event is disabled.

1 = none

2 = vbd

3 = fax

4 = tty

See note below.

-**prof**<*EventMappingProfileIndex*>—Specifies the index of the profile which defines the handling attributes in response to the event detection. If the EventHandleType is equal to 'none', this object is not applicable (not supported for H.248 and xGCP).

If the *EventMappingType* is equal to vbd, the VBD profile with the given index is attached to event. If the *EventMappingType* is equal to fax, the fax profile with the given index is attached to the event. If *EventMappingType* is equal to tty, the TTY profile with the given index is attached to the event.

The profile index value can be in the range of 1 to 25.

-**mode**<*HandleMode*—Specifies the mode of event handling. Network manager cannot add or delete, but can modify the default entries (not supported for H.248 and xGCP. The value of the *EventHandlingMode* can be:

1 – None—MG detects tones from both TDM and IP side and does not send NSE event to peer on detecting VBD tones from TDM side. This mode can be used when remote end is a third-party gateway and does not support Cisco proprietary NSE protocol but it does detect tone from IP side.

2 - nse—MG detects tone from both TDM and IP side and sends a NSE event to peer on detecting the VBD tone from TDM side.

For TGCP/MGCP, user can configure only EventMappingType for low speed modem event types (v21Modem, v23Modem, bellModem, v8bis). Configuring *EventMappingProfileIndex* and *EventHandlingMode* for low speed event types is not supported for TGCP/MGCP. These are supported only for H.248 (Megaco). For TGCP/MGCP, the low speed events are mapped to ced or v18aTone event types depending upon the htype value. If htype for low speed modem events is set to VBD, the ced event parameters such as profile and mode will apply to the event and if htype is set to TTY, v18aTone event parameters will apply to the event.

Step 3 Any event mapping index that has been created and is no longer required can be removed with the **deleventmapping** command.

deleventmapping <*EventMappingIndex*>

Where <EventMappingIndex> specifies the event mapping index number to be deleted.

Step 4 If additional event mapping records need to be created, use the **addeventmapping** command and repeat the steps above with additional profiles. The format of this command is:

addevent mapping <*EventMappingIndex*>

EventMappingIndex— Identifies a set of voice data events supported by VXSM and how they will be handled in the media gateway. An integer in the range 2 to 10 for VoIP Switching, 12 to 20 for AAL2 Trunking. A value of 1signifies the default handling for the voice data events in the media gateway

Note When a v21 event mapping is associated with a handle type = fax (**-htype** 3), the T.38 feature is enabled at the card level. Once the T.38 feature has been enabled for a specific eventmap, that configuration will be in effect until the eventmap has its v21 tone event association reconfigured for handle type = vbd (-**htype** 2). While the association is in effect, attempts to associate with any other eventmap have no effect.

Configuring a Voiceband Data Profiles

The VBD profile is used to determine the handling of fax/modem passthrough when it is detected in a voice interface. The profile includes such information as codec to be used for upspeed, size of jitter buffer, and the value for the inactivity time-out.

Perform the following procedure to configure a voiceband data profile.

Step 1 VXSM automatically creates a vbd profile (index 1 for VoIP Switching, index 11 for AAL2 Trunking), with default values. Use the **dspvbdprof** command to display the current values.

dspvbdprof <*VbdProfileIndex*>

```
knodar.10.VXSM.a > dspvbdprof 1
================================================================
```

```
                Voice Band Data Configuration Profile
================================================================
VBD Profile Index               :     1
VBD Upspeed CODEC Type          :     G.711u
VBD Jitter Buffer Delay Mode    :     fixed
VBD Jitter Buffer Maximum Delay :     135
VBD Jitter Buffer Nominal Delay :     70
VBD Jitter Buffer Minimum Delay :     0
VBD Inactivity Timeout          :     4
VBD Locally Disable VAD         :     enable
VBD Packet Period Control       :     enable
VBD Packet Period               :     10
VBD Echo Cancellor Override     :     disable
VBD NonLinear Processor Override:     disable
```

Check the values in the profile and use the following steps only if additional profiles are to be created or if existing profiles are to be modified.

Step 2 Use the **addvbdprof** command to create a vdb profile. The format of this command is:

addvbdprof<*Index*>[-**upscodec** <*Codec*>][-**jmax** <*JitterMaxDelay*>][-**jnom** <*JitterNomDelay*>] [-**inact** <*InactivityTimeout*>][-**vad** <*LocalVadDisable*>][-**ppcontrol** <*PacketPeriodControl*>][-**pp** <*PacketPeriod*>][-**ecan** <*EcanOverride*>][-**nlp** <*NLPOverride*>]

VbdProfileIndex—Identifies the VBD profile. The entry with the value of this object set to 1 is the default VBD profile for the media gateway. The default VBD profile is automatically created by the system and cannot be added or deleted, but can be modified by network manager. An integer in the range of 2 to 25

-upscodec<*UpspeedCodec*>—Specifies the CODEC type to use for upspeed. Upspeed is used to change the transmission rate of the voice interface to a higher rate of CODEC type. If CODEC type is set to "none" that means VXSM will not change codec and packetization period during upspeed. In this case it is expected that MGC will change codec and packetization period on receiving VBD event notification

1 = none
14 = G.726-32 (h248 only)
15 = G.711u
16 = G.711a
27 = Clear channel

-jmax<*MaxjitterDelay*>—Specifies the maximum jitter buffer size in the VBD connection. The value of *MaxjitterDelay* should be greater than the value of *NomjitterDelay.* An integer in the range of 20 o 135 milliseconds

-jnom<*NomJitterDelay*>—Specifies the nominal jitter buffer size in the VBD connection. The value of *NomjitterDelay* should be smaller than the value of *MaxjitterDelay.* An integer in the range of 5 to 135 milliseconds.

-inact<*InactivityTimeout*>—Specifies a timeout value before teardown the call if there is no activity in the VBD connection. The value of 0 is to disable the inactivity detection. An integer in the range of 0 to 60 seconds.

-vad <*LocalVadDisable*>—Specifies whether VAD will be disabled or not by MG during upspeed. The value can be 1 (enable) and 2 (disable). Enable means VXSM will disable VAD during upspeed and disable means VAD will not be changed by MG during upspeed.

-ppcontrol <*PacketPeriodControl*>—Specifies whether packetization period will be changed by MG during upspeed or not. The value can be 1 (enable) and 2 (disable). Enable means VXSM changes packetization period during upspeed and disable means packetization period does not change by MG during upspeed. If the codec type set to none, the packetization period is not controlled by VXSM irrespective of the value of *PacketPeriodControl.*

-pp<*PacketPeriod*>—Specifies the packetization period for the VBD connection. The packetization period represents the time for the media gateway to collect the data from TDM side before it sends out the packet. The value can be:

4 = 10 ms
5 = 15 ms
6 = 20 ms
7 = 25 ms
8 = 30 ms

-**ecan** <*EcanOverride*>—Specifies VBD Echo Canceller Override

1 - enable
2 - disable(default)

-**nlp** <*NLPOverride*>—Specifies VBD NLP(NonLinear Processor) Override

1 - enable
2 - disable(default)

Step 3 When a VBD profile has been created, the parameter values can be changed using the **cnfvbdprof** command. The format of this command is:

cnfvbdprof <*Index*>[-**upscodec** <*Codec*>][-**jmax** <*JitterMaxDelay*>][-**jnom** <*JitterNomDelay*>] [-**inact** <*InactivityTimeout*>][-**vad** <*LocalVadDisable*>][-**ppcontrol** <*PacketPeriodControl*>][-**pp** <*PacketPeriod*>][-**ecan** <*EcanOverride*>][-**nlp** <*NLPOverride*>]

For details of the parameters, refer to the **addvbdprof** command above.

Configuring a TTY Data Profile

The TTY profile is used to determine the handling of TTY passthrough when it is detected in a voice interface. The profile includes such information as codec to be used for upspeed, size of jitter buffer, the value for the inactivity time-out, the value for packetization period and VAD control.

Perform the following procedure to configure a TTY data profile.

Step 1 VXSM automatically creates a TTY profile (index = 1), with default values. Use the **dspttyprof** command to display the current values.

dspttyprof <*TtyProfileIndex*>

```
ns1_knodar.3.VXSM.a > dspttyprof 1
================================================================
              TTY Configuration Profile
================================================================
Profile Index               :         1
CODEC Type                  :         G.711a
Jitter Buffer Delay Mode    :         fixed
Jitter Buffer Maximum Delay :         135
Jitter Buffer Nominal Delay :         70
Jitter Buffer Minimum Delay :         0
Locally Disable VAD         :         enable
```

```
Packet Period Control       :         enable
Packet Period               :         10
Echo Canceller Override     :         disable
NonLinear Processor Override:         disable
```

Check the values in the profile and use the following steps only if additional profiles are to be created or if existing profiles are to be modified.

Step 2 Use the **addttyprof** command to create a TTY profile. The format of this command is:

addttyprof <*TtyProfileIndex*> [**-ttycodec** <*Codec*>][**-jmax** <*JitterMaxDelay*>][**-jnom** <*JitterNomDelay*>][**-vad** <LocalVadDisable>][**-ppcontrol** <*PacketPeriodControl*>] [**-pp** <*PacketPeriod*>][-**ecan** <*EcanOverride*>][-**nlp** <*NLPOverride*>]

TtyProfileIndex—Identifies the TTY profile. The entry with the value of this object set to 1 is the default TTY profile for the media gateway. The default TTY profile is automatically created by the system and cannot be added or deleted, but can be modified by network manager. An integer in the range of 2 to 25

-ttycodec<*Codec*>—Specifies the CODEC type to use for TTY upspeed. Upspeed is used to change the transmission rate of the voice interface to a higher rate of CODEC type. If CODEC type is set to "none" that means VXSM will not change codec, VAD and packetization period during upspeed. In this case it is expected that MGC will change codec, VAD and packetization period on receiving VBD event notification.

1 = none
14 = G.726-32
15 = G.711u
16 = G.711a
27 = Clear channel

-**jmax**<*JitterMaxDelay*>—Specifies the maximum jitter buffer size in the TTY data connection. The value of *JitterMaxDelay* should be greater than the value of *JitterNomDelay.* An integer in the range of 20 o 135 milliseconds

-jnom<*JitterNomDelay*>—Specifies the nominal jitter buffer size in the TTY data connection. The value of *JitterNomDelay* should be smaller than the value of. *JitterMaxDelay.* An integer in the range of 5 to 135 milliseconds

-vad <*LocalVadDisable*>—Specifies whether VAD will be disabled or not by MG during TTY upspeed. The value can be 1 (enable) and 2 (disable). Enable means VXSM disables VAD during upspeed and disable means VAD will not be changed by MG during upspeed. If the upspeed codec type set to none, the VAD will not be controlled by VXSM irrespective of the value of LocalVadDisable.

-ppcontrol <*PacketPeriodControl*>—Specifies whether packetization is changed by MG during upspeed or not. The value can be 1 (enable) and 2 (disable). Enable means VXSM changes packetization during upspeed and disable means packetization is not changed by MG during upspeed. If the upspeed codec type set to none, the packetization is not controlled by VXSM irrespective of the value of PacketPeriodControl.

-pp <*PacketPeriod*>—Specifies the value of the packetization period in TTY data connection. The value can be:

4 = 10 ms
5 = 15 ms
6 = 20 ms
7 = 25 ms
8 = 30 ms

-**ecan** <*EcanOverride*>—Specifies VBD Echo Canceller Override

1 - enable
2 - disable(default)

-**nlp** <*NLPOverride*>—Specifies VBD NLP(NonLinear Processor) Override

1 - enable
2 - disable(default)

Step 3 When a TTY profile has been created, the parameter values can be changed with the **cnfttyprof** command. The format of this command is:

cnfttyprof <*TtyProfileIndex*> [**-ttycodec** <*Codec*>][**-jmax** <*JitterMaxDelay*>][**-jnom** <*JitterNomDelay*>][**-vad** <*LocalVadDisable*>][**-ppcontrol** <*PacketPeriodControl*>] [**-pp** <*PacketPeriod*>][**-ecan** <*EcanOverride*>][-**nlp** <*NLPOverride*>]

For details on parameters, refer to the **addttyprof** command above.

Configuring a T.38 Fax Relay Profile

The fax profile is used to determine the handling of T.38 fax relay when a V21 tone is detected in a voice interface. The profile includes such information as T.38 variant, error correction mode, inactivity time-out, fax rate.

Perform the following procedure to configure a voiceband data profile.

Step 1 VXSM automatically creates a fax profile (index = 1), with default values. Use the **dspfaxprof** command to display the current values.

dspfaxprof <*FaxProfileIndex*>

```
M8850_NY.3.VXSM.a > dspfaxprof 1
=====================================================
             Fax Relay Configuration Profile
=====================================================
Fax Profile Index               :     1
Control Mode                    :     t38FallbackPt
Varient of T.38 Standered       :     0
Transport Protocol              :     udp
Method Used for TCF             :     network
Maximum Transmission Rate       :     14400
High-Speed Data Packet Rate     :     30
Low-Speed Data Redundancy       :     5
High-Speed Data Redundancy      :     0
Named-Signal-Event Timeout      :     1000
Inactivity Timeout              :     10
Nominal Delay                   :     200
Error-Correcting-Mode Status    :     enable
NSF Code Override Status        :     enable
NSF Manufacturing Country Code  :     173
NSF Vendor Code                 :     0051
```

Check the values in the profile and use the following steps only if additional profiles are to be created or if existing profiles are to be modified.

Step 2 Use the **addfaxprof** command to create a fax profile. The format of this command is:

addfaxprof <Index> [**-mode** <*Mode*>][-**t38var** <*T38Variant*>][-**bearer** <*BearerTxProtocol*>][-**maxtx** <*MaxFaxTxRate*>][-**hspktp** <*HsPacketSize*>][-**lsred** <*LsDataRedundancy*>] [-**hsred** <*HsDataRedundancy*>][-**nsf** <*NsfOverrideEnable*>][-**nsfcc** <*NsfCountryCode*>][-**nsfvc** <*NsfVendorCode*>][-**nse** <*NseAckTimeout*>][-**inact** <*InactivityTimeout*>][-**nom** <*FaxNominalDelay*>][-**ecm** <*T30EcmEnable*>]

FaxProfileIndex—Identifies the fax profile. The entry with the value of this object set to 1 is the default fax profile for the media gateway. The default fax profile is automatically created by the system and cannot be added or deleted, but can be modified by network manager. An integer in the range of 2 to 25

-**mode**<*T38Mode*>—This object specifies the control mode of a fax call that the gateway will follow upon detecting a V.21 preamble.

Enter a 1 or a 2 as defined below. The default is 1.

1 = t38FallbackPassthru - When a V.21 preamble is detected, T.38 is used to manage the fax call.

If T.38 attempt fails, then a passthrough is attempted.

2 = t38Only - When a V.21 preamble is detected, T.38 will be used to handle the fax call. If T.38 attempt fails, no other modes are attempted.

-t38var<*T38Variant*>—This object specifies the ITU-T T.38 version for different packet data coding.

ITU-T T.38 has 3 different versions, enter a 0, 1, or 2 as defined below. The default is 0.

0 = T.38 06-1998 standard.
1 = Same as 0
2 = T.38 03-2002 standard

Note This parameter is not configurable.

-bearer <*BearerTxProtocol*>—This object specifies the transport protocol in bearer path.

Enter 1 = udp - UDP (User Datagram Protocol). The default is 1.

-maxtx <*MaxFaxTxRate*>This object specifies the maximum fax transmission rate.

Enter the number for the appropriate rate. The default is 14400 bps.

3 = 2400 bps
4 = 4800 bps
5 = 7200 bps
6 = 9600 bps
7 = 14400 bps
8 = 1200 bps

-hspktp <*HsPacketSize*>This object specifies the packet rate of primary high-speed (HS) data packet.

Enter a number as follows:

.4 = 10
6 = 20
8 = 30 (default)
10 = 40
12 = 50
14 = 60
16 = 70
18 = 80

-lsred <*LsDataRedundancy*>This object specifies the number of preceding packets of IFP (Internet Fax Protocol) packet transmission redundancy for the low-speed control information exchanged during the first phase of a T.38 fax relay connection.

Enter a number in the range 0 to 8. The default is 5.

-hsred <*HsDataRedundancy*>This object specifies the number of preceding packets of the IFP packet transmission redundancy for the high-speed control and image information exchanged following the initial low-speed phase of a T.38 fax relay connection.

Enter a number in the range 0 to 2. The default is 0

-nsf <*NsfOverrideEnable*>This object enables or disables the gateway to override the NSF (Non-Standard Facilities) code in the following T.30 signals: NSF, NSC (Non-Standard Facilities Command) and NSS (Non-Standard Facilities Set-up).

Enter 1 or 2.

- 1 = enable
- 2 = disable

-nsfcc <*NsfCountryCode*>This object specifies the country code for identifying the country where the media gateway with non-standard capabilities was manufactured.This object is applicable only if **-nsf** is set to true.

Enter a number in the range 0 to 255. The default is 173.

-nsfvc <*NsfVendorCode*> Vendor Code (also called the Terminal Provider Code) in the NSF is a two-byte field identifying the manufacturer of the media gateway with non-standard capabilities.This object is applicable only if**-nsf** is set to true.

-nse <*NseAckTimeout*> This object specifies a timeout value for NSE timer. This timer is started after sending an NSE 200 while waiting for the NSE 201 acknowledgment or NSE 202 negative acknowledgment.Expiration of the timer indicates that the request to switch to T.38 has been rejected or discarded by the far end.

Enter a number in the range 250 to 10000 ms in the increments of 250 ms. The default is 1000 ms.

-inact <*InactivityTimeout*> This object specifies a timeout value before revert to voice mode if application supports it when there is no activity in the fax relay. The value of 0 is to disable the inactivity detection.

Enter a number in the range 0 to 65535 seconds. The default is 10.

-nom <*FaxNominalDelay*> This object specifies the nominal delay in the fax relay.

Enter a number in the range 5 to 65535 ms. The default is 200.

-ecm <*T30EcmEnable*> This object enables or disables T.30 ECM (Error Correcting Mode). ECM is a feature implemented by many new fax devices which improves image quality and page compression capabilities through a reliable image data transmission protocol ECM. When the value of this object is 'true', the ECM feature is enabled. Otherwise, the ECM feature is disabled. If fax calls are failing due to high packet loss, then set this object to false may improve the fax success rate.

Enter a 1 for enable, or 2 for disable.

Step 3 When a fax profile has been created, the parameter values can be changed with the **cnffaxprof** command. The format of this command is:

Use the **cnffaxprof** command to create a fax profile. The format of this command is:

cnffaxprof <Index> [**-mode** <*Mode*>][-**t38var** <*T38Variant*>][-**bearer** <*BearerTxProtocol*>][-**maxtx** <*MaxFaxTxRate*>][-**hspktp** <*HsPacketSize*>][-**lsred** <*LsDataRedundancy*>] [-**hsred** <*HsDataRedundancy*>][-**nsf** <*NsfOverrideEnable*>][-**nsfcc** <*NsfCountryCode*>][-**nsfvc** <*NsfVendorCode*>][-**nse** <*NseAckTimeout*>][-**inact** <*InactivityTimeout*>][-**nom** <*FaxNominalDelay*>][-**ecm** <*T30EcmEnable*>]

For details on the parameters, refer to the **addfaxprof** command above.

Configuring H.248 for Call Agent Controlled T.38 Fax Relay

When configuring VXSM for CA controlled T.38 Fax Relay with H.248, the H.248 protocol must be setup correctly. This involves configuring the RTP termination with the IPFAX package and the VIF termination with the CTYP package.

Step 1 Use the **dsptermtypes** command to display all currently configured VIF termination types.

For example:

```
archer.2.VXSM.a > dsptermtypes
=====================================================
          All Termination Types
=====================================================

Term Type ID    Term Type   Profile ID Package IDs
============   ============ ========== ============
       1         pdnRtp         0       0-G 4-DG 6-CG 10-RTP 34-IPFAX
```

Step 2 Check that there is a term type with package 34 (IPFAX) configured. If not, use the **cnftermtype** command to add IPFAX. The format of this command is:

cnftermtype -rtp <*Index*> <*PackageIds*> <*ProfileId*>

where *PackageIds* is a list of package numbers separated by commas. The list of supported packages is:

0 = G—Generic.
4 = DG—Basic DTMF (Dual Tone Multifrequency) tones generator.
6 = CG—Call progress tones generator.
9 = NT—Network.
10 = RTP—RTP (Real-time Transport Protocol).
12 = AN—Generic announcement.
13 - BCG—
15 = SrvTn—Basic services tone generation.
26 - GRI—
27 - RtcpXr—
28 - XrBm—
30 - DS—
32 - Xnq—
34 - IPFAX—IP fax

For example:

```
archer.2.VXSM.a > cnftermtype 2 0,4,6,10,34
```

Step 3 Use the **dspvifterms** command to display all configured VIF terminations.

For example:

```
Martler.2.VXSM.a > dspvifterms
=========================================================
             Term in all Voice Interfaces
=========================================================

  DS1/E1   DS0 Group  GW Link Profile    Packages

========== =========  ======= ======= ==============
 1.1.1.1.1     1           1      0   0-G 4-DG 5-DD 6-CG 8-CT 11-TDMC 12-AN 15-n 33-CTYP
 1.1.1.2.1     1           1      0   0-G 4-DG 5-DD 6-CG 8-CT 11-TDMC 12-AN 15-n
```

Step 4 For any VIF being configured check that the package number 33 (CTYP) is configured. If not, use the **cnfvifterm** command to add CTYP. The format of this command is:

cnfvifterm *<LineNum> <Ds0GrpIndex> <GatewayLinkId> <H248PkgIds><ProfileIndex> <Repetition>*

Where:

LineNum for OC-3—(bay.line.path.vtg.vt or bay.line.path.ds1)

bay {1 - upper}

line (range=1..4)

path (range=1..3)

vtg (range=1..7)

vt (range=1..4)(ds1) (range=1..3)(e1)

ds1 (range=1..28)

LineNum for T1/E1—(bay.line)

bay {1 - upper}

line (range=1..24)

LineNum for T3—(bay.line.ds1)

bay {1 - upper}

line (range=1..3)

ds1 (range=1..28)

Ds0GrpIndex—DS0 group index

T1: (range=0..23)

E1: (range=0..30)

GatewayLinkId—Gateway link ID an integer in the range 0 to 12 (0 = delete termination). The GatewayLinkId is used to associate the physical termination with a particular virtual gateway.

H248PkgIds—H248 package IDs {(multiple IDs) | #=current value}

0 - G
4 - DG
5 - DD
6 - CG
8 - CT
11 - TDMC
12 - AN
13 - BCG
15 - SrvTn
19 - Lltr
20 - BCAS
21 - RBS
22 - OSES
23 - AMET
24 - BCASAddr
25 - CASB
26 - GRI
31 - EriTermInfo
33 - CTYP

#—Current packagesProfileIndex—Profile index (range=0..25)(default=0)

Enter all the packages to be supported separated by commas. For example, 0,4,6,9,10,12,15,27,28.

Note To add a package, it is necessary to include all the current packages that are required and the package to be added. If only the added package is specified, all the current packages will be discarded.

Repetition—Bulk provisioning number

Single DS0 configuration (range=1..8064(OC-3)/1152(T1)/1488(E1)(default=1)

Multiple DS0 configuration (range=1..336(OC-3)/48(T1E1))(default=1)

Step 5 Use the **dspeventmapping -v21Tone** and the **dspeventmapping -cngTone** commands to check that they have been configured. For example

```
dspeventmapping -v21Tone 1
============================================================
          V21 Tone Event Mapping Configuration
============================================================
VBD Event Mapping Index:                  1
VBD Event Index              :            v21Tone
VBD Event Handle Type     :               fax
VBD Event Profile Index   :               1
VBD Event Handle Mode       :             none

dspeventmapping -cngTone 1
============================================================
          CNG Tone Event Mapping Configuration
============================================================
VBD Event Mapping Index:                  1
VBD Event Index                           cngTone
VBD Event Handle Type     :               fax
VBD Event Profile Index   :               1
VBD Event Handle Mode       :             none
```

Step 6 If eventmapping for either v.21 or CNG tones is not configured, use the **cnfeventmapping -v21Tone** and the **cnfeventmapping -cngTone** commands as appropriate. The format for these commands is:

cnfeventmapping -v21Tone<*EventMappingIndex*>[**-htype** <*HandleType*>] [**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

cnfeventmapping -cngTone<*EventMappingIndex*>[**-htype** <*HandleType*>] [**-prof** <*EventMappingProfileIndex*>] [**-mode**<*EventHandleMode*>]

See the "Configuring Voiceband Event Mapping" section on page 5-18 for more details.

Note By default CNG tone is set with HandleType=none & HandleMode=none. It is preferred to keep CNG tone settings at these settings unless some Call Agent requires something different.

Associating Voice Interfaces with Event Mapping

When the event mappings and fax profiles have been setup, the user should associate these with the VIFs to which they apply. To associate an event mapping and fax profiles with particular VIF, use the following procedure.

Step 1 To associate a VIF with a particular event mapping, use the cnfvifeventmapping command. The format of this command is:

cnfvifeventmapping <*Ds1Line*> <*Ds0GroupIndex*> <*EventMappingIndex*> <*Repetition*>

Use the *Ds1Line* and *Ds0GroupIndex* parameters to specify the voice circuit. Use the *EventMappingIndex* parameter to specify the event mapping to be associated with the voice circuit.

Consecutive DS0s can be associated with the same event mapping with the *Repetition* parameter.

Step 2 Repeat the use of the **cnfvifeventmapping** command to associate any non-consecutive DS0s or DS0s to be associated with a different event mapping index.

Configuring the Voice Quality Monitoring Feature

Before the Voice Quality Monitoring Feature can be configured, the VXSM card must be configured for VoIP applications using the H.248 call control protocol (see earlier in this chapter).

Step 1 Use the **dspdspparam** command to view the current DSP settings.

```
archer.2.VXSM.a > dspdspparam
=====================================================
              List DSP Parameters
=====================================================
SID Payload Type             :          decimal
RTCP Control                 :          true
RTCP Interval(milliseconds)  :          5000
RTCP Interval Multiplier     :          5
VAD Adaptive                 :          true
DTMF Power Level (0.1 dBm)   :          -120
DTMF Power Twist (0.1 dB)    :          0
RTCP Timer Control           :          startRtcpPktRcvd
VQM Control                  :          disable
RTCPXR Control               :          enable
RTCPXR Report Frequency      :          1
VQM Default Minimum Gap      :          16
RTCPXR external R factor     :          127
SES Threshold (ms)           :          50
```

The values that apply to VQM are:

- VQM Control
- RTCPXR Control
- RTCPCR Report Frequency
- VQM Default Minimum Gap
- RTCPXR external R factor
- Severely errored seconds (SES) threshold

Determine which of these settings (if any) need to be modified.

Step 2 Use the **cnfdspparam** command to enable VQM and modify any other VQM settings. The format of this command is:

cnfdspparam [-**ptype** <PayloadType>][-**control** <RTCPControl>][-**interval** <**RTCPTxInterval**>][-**multi** <RTCPRxMultiplier>][-**vadapt** <VADAdaptive>] [-**dtmfpl** <DTMFPowerLevel>][-**dtmfpt** <DTMF Power Twist>][-**rtcptm** <RTCP Timer Control>][-**vqm** <VQM Control>][-**xrcontrol** <RTCPXR Control>][-**xrmulti** <RTCPXR Report Freq.>] [-**gmin** <VQM default minimum gap>][-**rext** <RTCPXR ext. R factor>][**-sest** <SES Threshold>

The last six items apply to VQM.

To use the VQM feature, the -vqm parameter must be set to RFC3611 or XNQ VQM.

-vqm <VQM Control> is used to enable or disable the VQM feature where VQM Control is:

1 = disable
2 = RFC3611 VQM
3 = XNQ VQM

If XNQ VQM is enabled and H.248 package 32 is configured or if RFC 3611 VQM is enabled and packages 27 or 28 are configured, this parameter cannot be used to change VQM type to RFC 3611 VQM. To make this change, use cnftermtype to remove package 32 or 27 and 28 first

-**xrcontrol** <RTCPXR Control> is used to enable or disable the RTCP XR protocol where RTCPXR Control is:

1 = enable
2 = disable)
This parameter is not configurable and is always set to 1 and is not enabled for XNQ VQM.

-xrmulti <RTCPXR Report Freq> is used to configures the RTCP XR report frequency where RTCPXR Report Freq is an integer in the range of 1 to 5.

A value of 1 to 5 sends RTCP XR report every Nth RTCP packet.
This parameter is not configurable and is always set to 1 if VQM control is XNQ VQM.

-**gmin** <VQM default minimum gap> is used to configure the minimum gap (gmin) in the report block where VQM default minimum gap is an integer in the range of 1 to 255. The default gap minimum value is used if a value is not supplied by the MGC. The default value is 16.

For XNQ VQM, this parameter is not applicable and does not take effect.

Note One measure of voice quality is the frequency and distribution of lost and/or discarded packets. This measure divides a stream of voice packets into bursts and gaps where a burst is a period of relatively high rate of lost or discarded packets and a gap is period of low or no lost or discarded packets.

The **-gmin** parameter is a method of distinguishing between a burst and a gap by specifying the number of consecutively received (and not discarded) packets required to be considered a gap. Thus a value of 16 would require at least 16 consecutive received packets to be a gap. A values of 200 (say) would be a much more stringent requirement for a gap and thus a more stringent measure of voice quality.

-rext <RTCPXR ext. R factor> is used to configure the external R factor. The external R factor is a voice quality metric describing the segment of the call that is carried over a network segment external to the RTP segment (for example, an cellular network). RTCPXR ext. R factor is an integer in the range of 1 to 100 or the value 127. A value of 94 corresponds to toll quality, whereas values of 50 or less indicate a quality that is unusable. The value of 127 indicates that an external R factor is not available.
.For XNQ VQM, this parameter is not applicable and does not take effect.

-sest <SES Treshold> is used to specify the treshold for determining severely errored seconds (SES).A second is characterized as a severely errored second if there is degraded performance for more than the SES threshold period within that second. This parameter is a value in the range of 10 to 1000ms in increments of 5ms. The default is 50ms.
For RFC 3611 VQM, this parameter is not applicable and has no effect.

Step 3 If an H.248 Termination Type has already been created, use the **cnftermtype** command to configure the RTCPXR packages. Otherwise, use the **addtermtype -rtp** command to create a new H.248 term type. The formats of these commands are:

addtermtype -rtp <*Index*> <*PackageIds*> <*ProfileId*>

cnftermtype <*Index*> <*PackageIds*> <*ProfileId*>

The PackageIds that are supported are:

0 - G
4 - DG
6 - CG
9 - NT
10 - RTP
12 - AN
13 - BCG
15 - SrvTn
26 - GRI
27 - RtcpXr (requires RFC 3611 VQM to be enabled)
28 - XrBm (requires RFC 3611 VQM to be enabled)
30 - DS
32 - Xnq (requires XNQ VQM to be enabled)
34 - IPFAX
- use current packages

Enter all the packages to be supported separated by commas. For example, 0,4,6,9,10,12,15,27,28.

Note To add a package, it is necessary to include all the current packages that are required and the package to be added. If only the added package is specified, all the current packages will be discarded.

The profileId field represents the property profile identifier with which the terminations within this termination type are to be associated.

The valid value for this parameter is a number in the range from 0 – 25, with a default value of 0.

Note The following steps 4, 5, 6, 7, 8, and 9 are needed only if RFC 3611 VQM is enabled.

Step 4 The VXSM RFC3611 VQM feature uses a VQM profile to determine the conditions under which an alert or SNMP trap is triggered. A VQM profile contains a number of voice quality metrics where each metric specifies a reference value and a threshold percentage value. If an actual measured VQM metric (for example, round trip delay or voice packet loss rate) deviates from its reference value in the profile by more than the threshold percentage, an alert is triggered. All references and threshold percentages have built in default values.

Note An alert is triggered only if the deviation is in a direction that causes a worsening of voice quality. For example, if the Packet Loss Rate has a reference value of 10 and a threshold percentage of 20 percent, an alert is triggered if the rate exceeds 12 (10 + 20% of 10) indicating that voice quality has worsened. However, an alert is not triggered if the rate falls below 8 (10 - 20% of 10) indicating that voice quality has improved.

By default, the VXSM card automatically creates a voice quality monitoring profile with a profile number of 1. This profile cannot be added or deleted but it can be modified using the **cnfvqmthreshprof** command (see step 6 below for details). The user can either accept or modify profile #1 or create a new one. To create a new VQM threshold profile, use the **addvqmthreshprof** command. The format of this command is:

addvqmthreshprof <*VQM Profile Index*>

Where VQM Profile Index is an integer in the range 2 to 16. A profile with and index of 1 is automatically added. This profile can be modified but it cannot be deleted.

The reference and percentage values in the profile can be displayed with the **dspvqmthreshprof** command which has a voice format and a voiceband data format as follows:

dspvqmthreshprof -vbd <VQM Profile Index>

dspvqmthreshprof -voice <VQM Profile Index>

For example:

```
archer.2.VXSM.a > dspvqmthreshprof -voice 1
================================================================================
               VQM Threshold Profile (voice)
================================================================================
Index                                                        :      1
Packet Loss Rate Ref. Value                                  :      100
Packet Loss Rate Alert Threshold Percentage(%)               :      10
Jitter Buffer Discard Rate Ref. Value                        :      100
Jitter Buffer Discard Rate Alert Threshold Percentage(%)     :      10
Nominal Jitter Level Ref. Value(ms)                          :      75
Nominal Jitter Level Alert Threshold Percentage(%)           :      20
Inter-arrival Jitter Ref. Value(ms)                          :      50
Inter-arrival Jitter Alert Threshold Percentage(%)           :      20
Packet Round Trip Delay Ref. Value(ms)                       :      2000
Packet Round Trip Delay Alert Threshold Percentage(%)        :      10
End System Delay Ref. Value(ms)                              :      500
End System Delay Alert Threshold Percentage(%)               :      25
Local Residual Echo Return Loss Ref. Value(dB)               :      40
Local Residual Echo Return Loss Alert Threshold Percentage(%)  :      50
G.711a conversational R factor Ref. Value                    :      85
G.711a conversational R factor Alert Threshold Percentage(%)   :      10
G.711a conversational MOS Ref. Value                         :      42
G.711a conversational MOS Alert Threshold Percentage(%)      :      10
G.711a listening MOS Ref. Value                              :      45
G.711a listening MOS Alert Threshold Percentage(%)           :      10
G.711u conversational R factor Ref. Value                    :      85
G.711u conversational R factor Alert Threshold Percentage(%)   :      10
G.711u conversational MOS Ref. Value                         :      42
G.711u conversational MOS Alert Threshold Percentage(%)      :      10
G.711u listening MOS Ref. Value                              :      45
G.711u listening MOS Alert Threshold Percentage(%)           :      10
G.723Lo conversational R factor Ref. Value                   :      60
G.723Lo conversational R factor Alert Threshold Percentage(%)  :      6
G.723Lo conversational MOS Ref. Value                        :      31
G.723Lo conversational MOS Alert Threshold Percentage(%)     :      6
```

```
G.723Lo listening MOS Ref. Value                              :      33
G.723Lo listening MOS Alert Threshold Percentage(%)           :      6
G.723Hi conversational R factor Ref. Value                    :      60
G.723Hi conversational R factor Alert Threshold Percentage(%) :      6
G.723Hi conversational MOS Ref. Value                         :      32
G.723Hi conversational MOS Alert Threshold Percentage(%)      :      6
G.723Hi listening MOS Ref. Value                              :      34
G.723Hi listening MOS Alert Threshold Percentage(%)           :      6
G.723aLo conversational R factor Ref. Value                   :      60
G.723aLo conversational R factor Alert Threshold Percentage(%) :      6
G.723aLo conversational MOS Ref. Value                        :      31
G.723aLo conversational MOS Alert Threshold Percentage(%)     :      6
G.723aLo listening MOS Ref. Value                             :      33
G.723aLo listening MOS Alert Threshold Percentage(%)          :      6
G.723aHi conversational R factor Ref. Value                   :      60
G.723aHi conversational R factor Alert Threshold Percentage(%) :      6
G.723aHi conversational MOS Ref. Value                        :      32
G.723aHi conversational MOS Alert Threshold Percentage(%)     :      6
G.723aHi listening MOS Ref. Value                             :      34
G.723aHi listening MOS Alert Threshold Percentage(%)          :      6
G.726-32 conversational R factor Ref. Value                   :      70
G.726-32 conversational R factor Alert Threshold Percentage(%) :      15
G.726-32 conversational MOS Ref. Value                        :      38
G.726-32 conversational MOS Alert Threshold Percentage(%)     :      10
G.726-32 listening MOS Ref. Value                             :      40
G.726-32 listening MOS Alert Threshold Percentage(%)          :      10
G.729a conversational R factor Ref. Value                     :      65
G.729a conversational R factor Alert Threshold Percentage(%)  :      8
G.729a conversational MOS Ref. Value                          :      32
G.729a conversational MOS Alert Threshold Percentage(%)       :      8
G.729a listening MOS Ref. Value                               :      35
G.729a listening MOS Alert Threshold Percentage(%)            :      8
G.729ab conversational R factor Ref. Value                    :      65
G.729ab conversational R factor Alert Threshold Percentage(%) :      8
G.729ab conversational MOS Ref. Value                         :      32
G.729ab conversational MOS Alert Threshold Percentage(%)      :      8
G.729ab listening MOS Ref. Value                              :      35
G.729ab listening MOS Alert Threshold Percentage(%)           :      8
```

Step 5 If any of the current values in the VQM threshold profile needs changing, use the **cnfvqmthreshprof** to make the changes. This command permits a large set of reference and percentage values to be configured in the profile as follows:

cnfvqmthreshprof -vplr <*VQM Profile Index*> <*Voice Packet Loss Rate Ref*> <*Voice Packet Loss Rate Alert Thresh. Percentage*>

cnfvqmthreshprof -vjbdr <*VQM Profile Index*> <*Voice Jitter Buffer Discard Rate Ref*> <*Voice Jitter Buffer Discard Rate Alert Thresh. Percentage*>

cnfvqmthreshprof -njit <*VQM Profile Index*> <*Nominal Jitter Level Ref*> <*Nominal Jitter Level Alert Thresh. Percentage*>

cnfvqmthreshprof -intj <*VQM Profile Index*> <*Voice Inter-arrival Jitter Ref*> <*Voice Inter-arrival Jitter Alert Thresh. Percentage*>

cnfvqmthreshprof -rtd <*VQM Profile Index*><*Voice Packet Round Trip Delay Ref*> <*Voice Packet Round Trip Delay Alert Thresh. Percentage*>

cnfvqmthreshprof -esd <*VQM Profile Index*> <*Voice End System Delay Ref*> <*Voice End System Delay Alert Thresh. Percentage*>

cnfvqmthreshprof -lrerl <*VQM Profile Index*> <*Voice Local Residual Echo Return Loss Ref*> <*Voice Local Residual Echo Return Loss Alert Thresh. Percent.*>

cnfvqmthreshprof -moslq711a *<VQM Profile Index> <G.711a listening MOS Ref> <G.711a listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq711a *<VQM Profile Index> <G.711a conversational MOS Ref>*

<G.711a conversational MOS Alert Thresh. Percentage>

cnfvqmthreshprof -rcq711a *<VQM Profile Index> <G.711a conversational R factor Ref> <G.711a conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq711u *<VQM Profile Index> <G.711u listening MOS Ref> <G.711u listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq711u *<VQM Profile Index> <G.711u conversational MOS Ref> <G.711u conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq711u *<VQM Profile Index> <G.711u conversational R factor Ref> <G.711u conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq723Hi *<VQM Profile Index> <G.723-H conversational MOS Ref> <G.723-H conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq723Hi *<VQM Profile Index> <G.723-H conversational R factor Ref> <G.723-H conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq723Hi *<VQM Profile Index> <G.723-H listening MOS Ref> <G.723-H listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq723Lo *<VQM Profile Index> <G.723-L conversational MOS Ref> <G.723-L conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq723Lo *<VQM Profile Index> <G.723-L conversational R factor Ref> <G.723-L conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq723Lo *<VQM Profile Index> <G.723-L listening MOS Ref> <G.723-L listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq723aHi *<VQM Profile Index> <G.723a-H conversational MOS Ref> <G.723a-H conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq723aHi *<VQM Profile Index> <G.723a-H conversational R factor Ref> <G.723a-H conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq723aHi *<VQM Profile Index> <G.723a-H listening MOS Ref> <G.723a-H listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq723aLo *<VQM Profile Index> <G.723a-L conversational MOS Ref> <G.723a-L conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq723aLo *<VQM Profile Index> <G.723a-L conversational R factor Ref> <G.723a-L conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq723aLo *<VQM Profile Index> <G.723a-L listening MOS Ref> <G.723a-L listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq726 *<VQM Profile Index> <G.726-32 listening MOS Ref> <G.726-32 listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq726 *<VQM Profile Index> <G.726-32 conversational MOS Ref> <G.726-32 conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq726 *<VQM Profile Index> <G.726-32 conversational R factor Ref> <G.726-32 conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq729ab *<VQM Profile Index> <G.729ab listening MOS Ref> <G.729ab listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq729ab *<VQM Profile Index> <G.729ab conversational MOS Ref> <G.729ab conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq729ab *<VQM Profile Index> <G.729ab conversational R factor Ref> <G.729ab conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -moslq729a *<VQM Profile Index> <G.729a listening MOS Ref> <G.729a listening MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -moscq729a *<VQM Profile Index> <G.729a conversational MOS Ref> <G.729a conversational MOS Alert Thresh. Percentage>*

cnfvqmthreshprof -rcq729a *<VQM Profile Index> <G.729a conversational R factor Ref> <G.729a conversational R factor Alert Thresh. Percentage>*

cnfvqmthreshprof -vbdinterjit *<VQM Profile Index> <VBD Inter-arrival Jitter Ref> <VBD Inter-arrival Jitter Alert Thresh. Percentage>*

cnfvqmthreshprof -vbdjbdr *<VQM Profile Index> <VBD Jitter Buffer Discard Rate Ref> <VBD Jitter Buffer Discard Rate Alert Thresh. Percentage>*

cnfvqmthreshprof -vbdplr *<VQM Profile Index> <VBD Packet Loss Rate Ref> <VBD Packet Loss Rate Alert Thresh. Percentage>*

The description, range, and default value for each parameter are shown in Table 5-4. For each parameter, there is a reference value and a threshold percentage. If the measured value of the parameter deviates from the reference value by more than the threshold percentage, an alert is generated.

Table 5-4 VQM Reference Ranges and Defaults

Parameter	Description	Reference Range and Default Values
-vplr *<PktLossRate>*	Voice Packet Loss Rate	Voice Packet Loss Rate: Rate is (1 to 100 default is 5) Voice Packet Loss Rate Alert Thresh. Percentage (0 to 99, default is 10)
-vjbdr *<JBDiscardRate>*	Voice Jitter Buffer Discard Rate	Voice Jitter Buffer Discard Rate: Range is (1 to 100, default is 11) Voice Jitter Buffer Discard Rate Alert Thresh. Percentage (0 to 99, default is 1)
-njit *<NomJitterLevel>*	Nominal Jitter Level	Nominal Jitter Level: Range is (1 to 65535, default is 50) Nominal Jitter Level Alert Thresh. Percentage (0 to 99, default is 20)
-intj *<IntArrJitter>*	Voice Inter-arrival Jitter	Voice Inter-arrival Jitter: Range is (1 to 65535, default is 50) Voice Inter-arrival Jitter Alert Thresh. Percentage (0 to 99, default is 20)
-rtd *<RoundTripDelay>*	Voice Packet Round Trip Delay	Voice Packet Round Trip Delay: Range is (1 to 65535, default is 1000) Voice Packet Round Trip Delay Alert Thresh. Percentage (0 to 99, default is 10)

-esd *<EndSystemDelay>*	Voice End System Delay	Voice End System Delay: Range is (1 to 65535, default is 200) Voice End System Delay Alert Thresh. Percentage (0.99, default is 10)
-lrerl *<LocalRERL>*	Vooice Local Residual Echo Return Loss	Voice Local Residual Echo Return Loss: Range is (1 to 100, default is 40) Voice Local Residual Echo Return Loss Alert Thresh. Percentage (0 to 99, default is 10)
-rcq711a *<codec G.711a RCQ>*	G.711a conversational R factor	G.711a conversational R factor: Range is (1 to 100, default is 93) G.711a conversational R factor Alert Thresh. Percentage (0 to 99, default is 20)
-moscq711a *<codec G.711a MOSCQ>*	G.711a conversational MOS	G.711a conversational MOS: Range is (10 to 50, default is 42) G.711a conversational MOS Alert Thresh. Percentage (0 to 99, default is 14)
-moslq711a *<codec G.711a MOSLQ>*	G.711a listening MOS	G.711a listening MOS: Range is (10 to 50, default is 42) G.711a listening MOS Alert Thresh. Percentage (0 to 99, default is 5)
-rcq711u *<codec G.711u RCQ>*	G.711u conversational R factor	G.711u conversational R factor: Range is (1 to 120, default is 93) G.711u conversational R factor Alert Thresh. Percentage (0 to 99, default is 20)
-moscq711u *<codec G.711u MOSCQ>*	G.711u conversational MOS	G.711u conversational MOS: Range is (10 to 50, default is 42) G.711u conversational MOS Alert Thresh. Percentage (0 to 99, default is 14)
-moslq711u *<codec G.711u MOSLQ>*	G.711u listening MOS	G.711u listening MOS: Range is (10 to 50, default is 42) G.711u listening MOS Alert Thresh. Percentage (0 to 99, default is 5)
-req723Hi *<codec G.723-H RCQ>*	G.723Hi conversational R factor	[G.723Hi conversational R factor Ref (0..100 def=78)] [G.723Hi conversational R factor Alert Thresh. Percentage (0..99 def=23)]
-moscq723Hi *<codec G.723-H MOSCQ>*	G.723Hi conversational MOS	[G.723Hi conversational MOS Ref (10..50 def=38)] [G.723Hi conversational MOS Alert Thresh. Percentage (0..99 def=21)]
-moslq723Hi *<codec G.723-H MOSLQ>*	G.723Hi listening MOS	[G.723Hi listening MOS Ref (10..50 def=38)] [G.723Hi listening MOS Alert Thresh. Percentage (0..99 def=9)]

-req723Lo *<codec G.723-L RCQ>*	G.723Lo conversational R factor	[G.723Lo conversational R factor Ref (0..100 def=74)] [G.723Lo conversational R factor Alert Thresh. Percentage (0..99 def=23)]
-moscq723Lo *<codec G.723-L MOSCQ>*	G.723Lo conversational MOS	[G.723Lo conversational MOS Ref (10..50 def=36)] [G.723Lo conversational MOS Alert Thresh. Percentage (0..99 def=22)]
-moslq723Lo *<codec G.723-L MOSLQ>*	G.723Lo listening MOS	[G.723Lo listening MOS Ref (10..50 def=36)] [G.723Lo listening MOS Alert Thresh. Percentage (0..99 def=9)]
-req723aHi *<codec G.723a-H RCQ>*	G.723aHi conversational R factor	[G.723aHi conversational R factor Ref (0..100 def=78)] [G.723aHi conversational R factor Alert Thresh. Percentage (0..99 def=23)]
-moscq723aHi *<codec G.723a-H MOSCQ>*	G.723aHi conversational MOS	[G.723aHi conversational MOS Ref (10..50 def=38)] [G.723aHi conversational MOS Alert Thresh. Percentage (0..99 def=21)]
-moslq723aHi *<codec G.723a-H MOSLQ>*	G.723aHi listening MOS	[G.723aHi listening MOS Ref (10..50 def=38)] [G.723aHi listening MOS Alert Thresh. Percentage (0..99 def=9)]
-req723aLo *<codec G.723a-L RCQ>*	G.723aLo conversational R factor	[G.723aLo conversational R factor Ref (0..100 def=74)] [G.723aLo conversational R factor Alert Thresh. Percentage (0..99 def=23)]
-moscq723aLo *<codec G.723a-L MOSCQ>*	G.723aLo conversational MOS	[G.723aLo conversational MOS Ref (10..50 def=36)] [G.723aLo conversational MOS Alert Thresh. Percentage (0..99 def=22)]
-moslq723aLo *<codec G.723a-L MOSLQ>*	G.723aLo listening MOS	[G.723aLo listening MOS Ref (10..50 def=36)] [G.723aLo listening MOS Alert Thresh. Percentage (0..99 def=9)]
-rcq726 *<codec G.726 RCQ>*	G.726-32 conversational R factor	G.726-32 conversational R factor : Range is (1 to 100, default is 81) G.726-32 conversational R factor Alert Thresh. Percentage (0 to 99, default is 22)
-moscq726 *<codec G.726 MOSCQ>*	G.726-32 conversational MOS	G.726-32 conversational MOS : Range is (10 to 50, default is 39) G.726-32 conversational MOS Alert Thresh. Percentage (0 to 99, default is 20)

-moslq726 *<codec G.726 MOSLQ>*	G.726-32 listening MOS	G.726-32 listening MOS : Range is (10 to 50, default is 39) G.726-32 listening MOS Alert Thresh. Percentage (0 to 99, default is 8)
-rcq729a *<codec G.729a RCQ>*	G.729a conversational R factor	G.729a conversational R factor : Range is (1 to 100, default is 82) G.729a conversational R factor Alert Thresh. Percentage (0 to 99, default is 22)
-moscq729a *<codec G.729a MOSCQ>*	G.729a conversational MOS	G.729a conversational MOS : Range is (10 to 50, default is 39) G.729a conversational MOS Alert Thresh. Percentage (0 to 99, default is 19)
-moslq729a *<codec G.729a MOSLQ>*	G.729a listening MOS	G.729a listening MOS : Range is (10 to 50, default is 39) G.729a listening MOS Alert Thresh. Percentage (0 to 99, default is 8)
-rcq729ab *<codec G.729ab RCQ>*	G.729ab conversational R factor	G.729ab conversational R factor : Range is (1 to 100, default is 82) G.729ab conversational R factor Alert Thresh. Percentage (0 to 99, default is 22)
-moscq729ab *<codec G.729ab MOSCQ>*	G.729ab conversational MOS	G.729ab conversational MOS : Range is (10 to 50, default is 39) G.729ab conversational MOS Alert Thresh. Percentage (0 to 99, default is 19)
-moslq729ab *<codec G.729ab MOSLQ>*	G.729ab listening MOS	G.729ab listening MOS : Range is (10 to 50, default is 39) G.729ab listening MOS Alert Thresh. Percentage (0 to 99, default is 8)
-vbdplr *<vbd PktLossRate>*	VBD Packet Loss Rate	VBD Packet Loss Rate : Range is (1 to 100, default is 2) VBD Packet Loss Rate Alert Thresh. Percentage (0 to 99, default is 10)
-vbdjbdr *<vbd JBDiscardRate>*	VBD Jitter Buffer Discard Rate	VBD Jitter Buffer Discard Rate : Range is (1 to 100, default is 2) VBD Jitter Buffer Discard Rate Alert Thresh. Percentage (0 to 99, default is 10)
-vbdinterjit *<vbd IntArrJitter>*	VBD Inter-arrival Jitter	VBD Inter-arrival Jitter : Range is (1 to 65535, default is 50) VBD Inter-arrival Jitter Alert Thresh. Percentage (0 to 99, default is 20)

Step 6 VXSM supports one trigger per call at any one time and there is no support for multiple simultaneous triggers in a single call. With the reference and threshold values for each of the VQM parameters set in the VQM threshold profile, each T1/E1 interface can be configured with its own single trigger parameter. In addition, a default trigger parameter can be configured for the whole gateway or a virtual gateway. If both the default gateway trigger parameter and T1/E1 interface level trigger parameters are configured, the quality alert will be based on the T1/E1 interface trigger metric.

Use the **cnfvqmtrigger** command to specify which alert parameter(s) should trigger an alert.

The formats of this command are as follows:

- **cnfvqmtrigger -gw** <*VoiceType*><*VbdType*>[**-profileId** <*VQM Profile Index*>]

  This form of the command specifies default voice and voiceband trigger types for the gateway.

  cnfvqmtrigger -vgw <*Alert Trigger Index***> <***VoiceType***><***VbdType***>[-profileId <***VQM Profile Index***>]**

  This form of the command specifies default voice and voiceband trigger types for a virtual gateway.

- **cnfvqmtrigger -e1** <*Alert Trigger Index*><*VoiceType*><*VbdType*>[**-profileId** <*VQM Profile Index*>]

  This form of the command specifies voice and voiceband trigger types for a specific E1 interface. The interface is specified in the *Alert Trigger Index* in the form <bay.line.path.vtg.vt>.

- **cnfvqmtrigger -ds1** <*Alert Trigger Index*><*VoiceType*><*VbdType*>[**-profileId** <*VQM Profile Index*>]

  This form of the command specifies voice and voiceband trigger types for a specific DS1 interface. The interface is specified in the *Alert Trigger Index* in the form <bay.line.path.vtg.vt> or <bay.line.path.ds1>

Voice and Voiceband Data trigger types are specified as follows:

For voice

1 - Not Config.
2 - Packet Loss Rate
3 - Jitter Buffer Discard Rate
4 - Inter Arrival Jitter
5 - Nominal Jitter Level
6 - Packet Round Trip Delay
7 - End System Delay
8 - Local Residual Echo Return Loss
9 - conversational R factor
10 - conversational MOS
11 - listening MOS
255 - none(default)
The default is 255

For voiceband data

1 = not configured
2 = Packet loss rate
3 - Jitter Buffer Discard Rate
4 - Inter Arrival Jitter
255 = disabled

The default is 255

Note Trigger types are shown in Table 5-5.

For the profileId parameter, select the alert threshold profile for threshold values in the range from 1 to 16, the default value is 1.

Table 5-5 VQM Trigger Types

Quality Alert Trigger	DSP Parameter	Alert Qualification	Voice Phase Trigger	VBD Phase Trigger
Local End System Delay	End System Delay	Instantaneous values above or below threshold must be integrated over a time interval of at least 1 second.	Yes	No
Pkt Rnd Trip Delay	Round Trip Delay	Instantaneous values above threshold must be integrated over 3 consecutive crossings which correspond roughly to a time interval of approximately 15 seconds. (typically 3 RTCP report intervals).	Yes	No
Cumulative Packet Loss Ratio	Loss Rate	No further verification necessary. This threshold crossing already represents averages over a suitable interval for transience or persistence verification	Yes	Yes
Cumulative Packet Discard Ratio	Discard Rate	No further verification necessary. This threshold crossing already represents averages over a suitable interval for transience or persistence verification.	Yes	Yes
RFC3550 Inter-arrival Jitter	RFC 3550 Jitter	Averaged inter-arrival jitter J is a smoothed estimation of jitter. Thus average jitter J needs no further verification except at the beginning of a call where the total elapsed time interval must be at least 10 seconds for this metric to be valid. During the first 10 seconds, no alert will be generated due to invalid value for the inter-arrival jitter.	Yes	Yes
MOS_LQ	MOS_LQ	MOS_LQR similar to R-factor (see below) is a smoothed average over a time interval (10seconds) and hence need no further verification.	Yes	No

Table 5-5 VQM Trigger Types (continued)

MOS_CQ	MOS_CQ	MOS_CQR similar to R-factor (see below) is a smoothed average over a time interval (10seconds) and hence need no further verification.	Yes	No
R-Factor	R Factor	R-factor similar is a smoothed average over a time interval (10seconds) and hence need no further verification.	Yes	No
Nominal Jitter Buffer Size	JB Nom Delay	Nominal jitter buffer size is already integrated over several samples (e.g. time) hence no further verification is necessary except at connection start. Averages should be over a total elapsed time of not less than 10 seconds to be meaningful.	Yes	No
RERL	RERL dB	RERL = ERL+ERLE is a measure of the total echo loss imposed by the system. Instantaneous values above threshold must be integrated over 3 consecutive crossings which correspond roughly to a time interval of approximately 15 seconds. (typically 3 RTCP report intervals).	Yes	No

Step 7 If alert traps are to be sent to an SNMP network manager, use the **cnfvqmtrap** command to enable traps. The format of this command is:

cnfvqmtrap <*Trap Enable*>

For Trap Enable

1 = true (enable)
2 = false (disable)

Step 8 If traps and/or events are generated at a very high rate, VXSM performance can be adversely affected. The **cnfvqmthrottle** command can be used to control the rate at which traps and events are generated.

There are two formats for the command, one for traps and one for events.

For traps, the format of the command is:

cnfvqmthrottle -trap [*Trap Rate*] [*Trap Rate Interval*]

Trap Rate is expressed as maximum traps per second in the range 1 to 1000 with a default of 100.

Trap Rate Interval is expressed as an integer with the value of 0 or a value in the range of 100 to 60,000 ms with a default of 1000 ms

For events, the format of the command is:

cnfvqmthrottle -event [*Event Rate*] [*Event Rate Interval*]

Event Rate is expressed as maximum traps per second in the range 1 to 1000 with a default of 100.

Event Rate Interval is expressed as an integer with the value of 0 or a value in the range of 100 to 60,000 ms with a default of 1000 ms.

Note Trap and Event rates and intervals can be configured only if the value for rate divided by the value for interval produce a result between 10 and 100 traps or events per second.

A rate interval value of 0, disables the throttle.

Step 9 The **cnfvqmhistory** command can be used to configure how the history file is reported to a network management system. This command has a variety of formats as shown below.

cnfvqmhistory -vgw <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -gw [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -bpvc <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -au4 <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -au3 <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -sts <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -stm1 <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -oc3 <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -e1 <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

cnfvqmhistory -ds1 <*VQM History Index*> [**-name** <*Group Name*>][**-reset** <*Reset VQM History Data*>]

The history table has multiple entries in which each entry tracks the history of a set of calls in a region. A history entries are grouped according to the following characteristics:

- 1 entry per T1/E1 interface (maximum of 336 entries)
- 1 entry per STS/AU3 path (a total of 12 entries)
- 1 entry per OC-3/STM1 line (a total of 4 entries)
- 1 entry per bearer IP interface (a total of 8 entries)
- 1 entry per virtual gateway
- 1 entry for gateway

The VQM History Index parameter defines the history entry as follows:

Command	VQM History Index Parameter and Ranges
cnfvqmhistory -gw	
cnfvqmhistory -vgw	<vgwIndex> vgwIndex range is 1 to 12

Command	VQM History Index Parameter and Ranges
cnfvqmhistory -bpvc	<vpi.vci> vpi range is 0 to 255 vci range is 0 to 65535
cnfvqmhistory -oc3	<bay.line> bay range is 1 line range is 1 to 4
cnfvqmhistory -stm1	<bay.line> bay range is 1 line range is 1 to 4
cnfvqmhistory -sts	<bay.line.path> bay range is 1 line range is 1 to 4 path range is 1 to 3
cnfvqmhistory -au3	<bay.line.path> bay range is 1 line range is 1 to 4 path range is 1 to 3
cnfvqmhistory -au4	<bay.line.path> bay range is 1 line range is 1 to 4 path range is 1
cnfvqmhistory -ds1	<bay.line.path.vtg.vt> bay range is 1 line range is 1 to 4 path range is 1 to 3 vtg range is 1 to 7 vt range is 1 to 4 or <bay.line.path.ds1> bay range is 1 line range is 1 to 4 path range is 1 to 3 ds1 range is 1 to 28
cnfvqmhistory -e1	<bay.line.path.vtg.vt> bay range is 1 line range is 1 to 4 path range is 1 to 3 vtg range is 1 to 7 vt range is 1 to 3
cnfvqmhistory -ln (T1/E1 card only)	<bay.line> bay range is 1 to 2 line range is 1 to 24

Command	VQM History Index Parameter and Ranges
cnfvqmhistory -t3 (T3 card only)	<bay.line> bay range is 1 to 2 line range is 1 to 3
cnfvqmhistory -ds1 (T3 card only)	<bay.line.ds1> bay range is 1 to 2 line range is 1 to 3 ds1 range is 1 to 28

The **-name** <*Group Name*> and **-reset** <*Reset VQM History Data*> parameters are common to all command formats.

The **-name** <*Group Name*> parameter is a user defined name to identify the group. This parameter is a text field with 1 to 128 characters.

The **-reset** <*Reset VQM History Data*> *parameter is defined as:*

1 = run
2 = stop
3 = reset

Note For each cnfvqmhistory command, VXSM has an equivalent dspvqmhistory command.

Configuring the Online Diagnostic Feature

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 nonintrusive 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
G723 family               0              3022
```

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.

Configuring for Jitter Compensation

Configuring for jitter compensation is a matter of setting values for minimum, maximum, and nominal delays in the appropriate commands. The procedure is different between voice codec jitter and the various form of voiceband data.

Jitter Delay for Voice Codecs

For voice codec transmissions (or Clear Channel for trunking signaling data), configuration of jitter delay is performed using the **cnfcodecparam** command.

This command has the format:

cnfcodecparam <*AdaptationType*> <*CodecIndex*> [**-pref** <*Preference*>]
[**-vpktp** <*VoicePktPeriod*>] [**-vbdpktp** <*VBDPktPeriod*>] [**-mod**e <*JitterMode*>]
[**-max** <*MaxDelay*>] [**-nom** <*NomDelay*>] [**-min** <*MinDelay*>] [**-dtmf** <*DtmfRelay*>]
[**-payload** <*PayloadType*>]

The relevant jitter delay parameters are

-mode <*JitterMode*> **, -max** <*MaxDelay*>**, -nom** <*NomDelay*>, and **-min** <*MinDelay*>]

Step 1 Set the jitter mode parameter to either 1 for adaptive mode or 2 for fixed mode. Adaptive mode is normally used for voice codecs, fixed mode is normally used clear channel.

Step 2 Enter a value, in milliseconds, for the nominal delay. The value should be the expected average jitter experienced on the arriving packets.

For voice codecs, the permissable range of values that can be entered is 5 – 135 ms.
In the absence of any other knowledge, the default value specified in the **cnfcodecparam** command generally operates satisfactorily.

For clear channel enter a value of 70 ms

Step 3 Enter a maximum delay value, in milliseconds, that is greater than the value for the nominal delay.

For voice codecs, the permissable range of values that can be entered is 20 – 135 ms

For VAD off, the recommended value for max. jitter delay is 2J+P where:
J = nominal delay value and P = the packetization period.

For VAD on, the recommended value for max. jitter delay is 2J+P+(P-S) where:
J = nominal delay value, P = the packetization period, and S= 5ms for G.711/G.726-32 or 10ms for G.729a/ab.

For clear channel enter a value of 135 ms

Step 4 Enter a minimum delay value, in milliseconds, that is less than the value for the nominal delay.

For voice codecs, the permissable range of values that can be entered is 0 – 135 ms

For VAD off or on, the recommended value for max. jitter delay is 0.5J where:
J = nominal delay value.

For clear channel enter a value of 0 ms.

Jitter Delay for AAL2 Applications

1. For sub-cell multiplexing AAL2 situations in which the buffer is in **adaptive** mode, the jitter can adapt to a very low value and would be unable to adjust to a sudden jitter introduced by the CU_TIMER To avoid this condition from occurring, the value of the minimum jitter delay should be set at least as high as the value of the CU_TIMER on the PVC at the remote end.

   For similar situations but where the buffer is in **fixed** mode, the value of the nominal jitter delay should be set as high as the value of the CU_TIMER on the PVC at the remote end plus the expected average network jitter.

2. When using Custom 110 AAL2 profile, the CU_TIMER on the PVC at the remote end should be set to be less than or equal 10 msec (if subcell multiplexing ia enable at the remote end). The reason for this is the limitation of the Custom 110 profile.

Jitter Delay for Fax, TTY, and Modem Traffic

The nominal and/or maximum jitter delay values specified for voiceband data, such as fax, modem, and tty are configured using the configure voiceband data jitter, **cnfvbdjitter**, command and the appropriate add or configure profile command. These commands contain parameters for setting the nominal and maximum jitter delays. For example, to configure a tty profile, use the **cnfttyprof** command.

cnfttyprof <*TtyProfileIndex*> [**-ttycodec** <*Codec*>][**-jmax** <*JitterMaxDelay*>][**-jnom** <*JitterNomDelay*>][**-vad** <LocalVadDisable>][**-ppcontrol** <*PacketPeriodControl*>] [**-pp** <*PacketPeriod*>]

Permissible values are shown in Table 5-6.

Table 5-6 Voiceband Data Jitter Delay Parameters

Command	Parameter	Range (ms)	Default (ms)
Configure jitter buffer	nominal delay	5..135	70
Configure jitter buffer	maximum delay	Not available	Not available
Add/Configure Fax Profile	nominal delay	20..200	200
Add/Configure Fax Profile	maximum delay	Not available	Not available
Add/Configure TTY Profile	nominal delay	5..135	70
Add/Configure TTY Profile	maximum delay	20..135	135
Add/Configure vbd Profile	nominal delay	5..135	70
Add/Configure vbd Profile	maximum delay	20..135	135

See *Cisco Voice Switch Services Configuration Guide for MGX Switches and Media Gateways, Release 5.3* for details of these commands.

Note The default vbd -jnom 70 valuemay or may not work on a V.21 modem
Some low speed modems establish active sessions very quickly. They are also very sensitive to silence gaps. An unavoidable silence gap occurs when the modem tone is first detected. An up speed occurs. During the up speed a jitter buffer adaptation and codec change takes place. This gap can cause a low

speed modem to prematurely disconnect or fail to fully train up. The default -jnom setting of 70ms is based on Fax and High speed modem up speeds. If a network will be using low speed modems such as V.21, assign a vbd profile with a value around 40ms.

DSP Resources under Mixed Codec Conditions

When the same codec is used to set up calls on the gateway, the available DSP resources are fully used. However, when different codecs are used to set up calls, the amount of usable DSP resources may be limited due to fragmentation.

Fragmentation occurs 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 are 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.

VXSM as a Signaling Gateway

Signaling Gateway Description

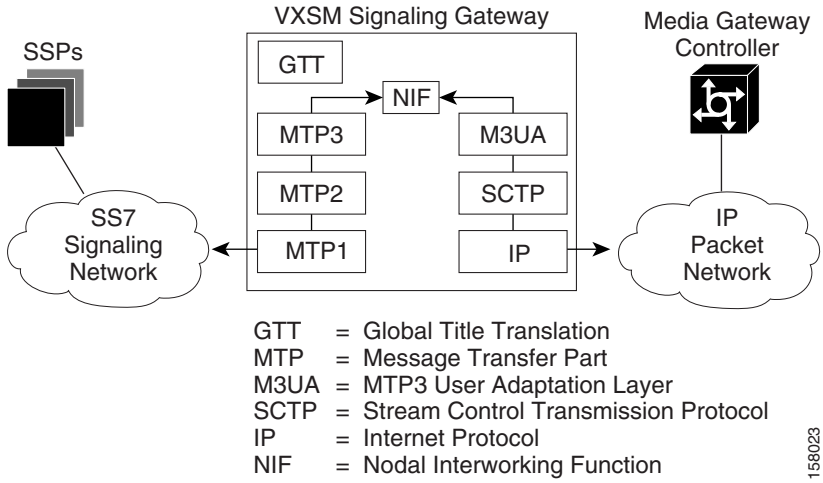
A VXSM card in an MGX 8880 and functioning as a media gateway can also be configured to provide the functions of a signaling gateway between SS7 and IP networks. By this means, communication can be established between entities, such as Signaling End Points, on a SS7 network and Application Servers, such as a Media Gateway Controller, on an IP network.

VXSM supports one instance of a Signaling Gateway that can operate concurrently with one or several instances of Media Gateways.

The VXSM signaling gateway feature permits up to 16 DS0 lines on a VXSM card to be configured as SS7 signaling lines. As shown in Figure 6-1, signaling messages to and from the SS7 network use the MTP1, MTP2, and MTP3 layers of the SS7 protocol stack. Received messages have the MTP3 component extracted and relayed onto the IP network using the M3UA, SCTP, and IP protocol stack. The interworking at the MTP3 level is performed by a Nodal Interworking Function (NIF).

At the MTP2 level messages destined to the local point code are queued for local processing. An example of this are messages that require their dialed digits to be translated to an address format that can be used by MTP to route the message. Such translation is performed by the Global Title Translation (GTT) module. Messages not requiring local processing are passed to NIF for further routing.

Figure 6-1 VXSM Signaling Gateway Protocol Stacks



A summary list of the VXSM Signaling Gateway Features is as follows:

- Up to 16 SS7 Low Speed Signalling Links (64Kpbs)
- 1:1 hot card redundancy for both configuration and dynamic data
- Command Line Interface (CLI) for VXSM SG/MG configuration
- SNMP Management interface through MIBs to configure SG/MG and to display and retrieve status and statistics
- Concurrent SG operation of M3UA, IUA, and DUA
- Support both ITU and ANSI SS7 variants
- SCTP for M3UA Transport layer; SCTP compliant with RFC 2992
- M3UA implementation compliant with RFC 3332. Refer [9] for compliance details
- SCCP support for Global Title Translation
- Multiple Point Code Assignment
- AS point code assignment and management
- Flexible AS routing key assignment
- AS traffic mode: load-sharing, over-ride and broadcast
- ASP to ASP routing through the SG by using routing keys
- QOS mapping to IP TOS for M3UA traffic.

Signaling Gateway Statistics

The VXSM Signaling Gateway supports the collection of statistics on both the SS7 and IP networks. The values of the statistics counters can be uploaded to a Network Management System upon demand.

On the SS7 side, up to 64 entries of link statistics counters can be collected periodically and upload to NMS on demand. On the IP side, a maximum of 16 entries of ASP statistics can be collected and uploaded.

SS7 Statistics Supported

The number of MTP3 packets received by this link Q752/3.5

The number of MTP3 packets sent by this link Q752/3.3

The number of MTP3 bytes received by this link Q752/3.4

The number of MTP3 bytes send by this link Q752/3.1

The number of MTP3 packets retransmitted on this link Q752/3.2

The number of MTP3 bytes retransmitted on this link Q752/3.2

Duration of link in the In-Service state Q752/1.1

Count of Signaling Link failure—All reasons Q752/1.2.

Count of Signaling Link failure—Abnormal FIBR/BSNR Q752/1.4

Count of Signaling Link failure—Excessive delay of acknowledgement Q752/1.4

Count of Signaling Link failure—Excessive error rate Q752/1.5

Count of Signaling Link failure—Excessive duration of congestion Q752/1.6

Count of alignment or proving errors Q752/1.7

Count of signal units received in error Q752/1.8

Count of negative acknowledgement received Q752/1.9

Count of local automatic changeover events Q752/1.10

Count of local automatic changeback events Q752/1.11

Duration of Signaling Link unavailable (for any reason) Q752/2.1

Duration of Signaling Link unavailable due to local management actions Q752/2.5

Duration of Signaling Link unavailable due to remote management actions Q752/2.6

Duration of Signaling link unavailable due to link failure Q752/2.7

Duration of Signaling Link unavailable due to remote processor outage Q752/2.9

Count of remote processor outage events Q752/2.10 and Q752/2.11

Duration of local busy Q752/2.15

Count of local inhibition Q752/2.16 and Q752/2.17

Count of remote inhibition Q752/2.18 and Q752/2.19

The number times this signaling link was marked congested. This measurement is specified in Q752/3.6

Cumulative duration of signaling link congestion Q752/3.7

The number of packets (MSUs) discarded due to signaling link level 1 congestion Q752/3.10

The number of packets (MSUs) discard due to signaling link level 2 congestion Q752/3.10

The number of packets (MSUs) discard due to signaling link level 3 congestion Q752/3.10

The number times this signaling link entered congestion level 1 and packets were discarded. Q752/3.11

The number times this signaling link entered congestion level 2 and packets were discarded. Q752/3.11

The number times this signaling link entered congestion level 3 and packets were discarded. Q752/3.11

IP Statistics Supported

The number of data packets received from this ASP

The number of data packets sent to this ASP

The number of data packets received from MTP3

The number of data packets sent to MTP3

The number of ASP Up messages received

The number of ASP Up ACK messages sent

The number of ASP Up ACK messages sent

The number of ASP Down ACK messages sent

The number of ASP Active messages received

The number of ASP Active ACK messages sent

The number of ASP Inactive messages received

The number of ASP Inactive ACK messages sent

The number of ASP Error messages received

The number of ASP Error messages sent

The number of ASP Notify messages sent

The number of Destination Unavailable messages received

The number of Destination Unavailable messages sent

The number of Destination Available messages received

The number of Destination Available messages sent

The number of Destination User Part Unavailable messages received

The number of Destination User Part Unavailable messages sent

The number of Destination State Audit messages received

The number of Destination State Audit messages sent

The number of Signaling Congestion messages with congestion level 0 (or no congestion) received

The number of Signaling Congestion messages with Congestion level 1 received

The number of Signaling Congestion messages with Congestion level 2 received

The number of Signaling Congestion messages with Congestion level 3 received

The number of Signaling Congestion messages with Congestion level 0 sent

The number of Signaling Congestion messages with Congestion level 1 sent

The number of Signaling Congestion messages with Congestion level 2 sent

The number of Signaling Congestion messages with Congestion level 3 sent

Configuring a Signaling Gateway

Setting up a Signaling Gateway on a VXSM card consists of configuring the following items.

- The SS7 network side of the signaling gateway.
- The IP network side of the signaling gateway
- The Application Severs and Application Server Processes
- The SCCP/GTT functions.

Configure the SS7 Network Side

To configure the SS7 side of the Signaling Gateway, perform the following steps.

Step 1 Use the **addss7** command to create an instance of the SS7 side of the signaling gateway. The format of this command is:

addss7 <*Ss7Variant*> [**-name** <*Name*>][**-nwind** <*NetworkIndicator*>]
[**-nwname** <*NetworkName*>] [**-tfr** <*TxRestrictedMsg*>][**-frestart** <*FastRestart*>]
[**-distsccp** <*DistributedSccp*>][**-multicong** <*MultiCongestion*>]
[**-sumroute** <*SummaryRouting*>][**-linktest** <*AutoLinkTest*>][**-prevtxp** <*PreventiveTxp*>]

For *Ss7Variant*, set the variant as either 1 = ansi or 1 = itu.

For -**name**<*Name*>, if used, enter a Signaling Point identifier as a character string up to 30 characters.If this parameter is not specified, it defaults to the local point code

For **-nwind** <*NetworkIndicator*> enter a network indicator:

0 = international
1 = internationalSpare
2 = national
3 = natSpare

For **-nwname** <*NetworkName*> enter a network name, a character string up to 19 characters.

For **-tfr** <*TxRestrictedMsg*> enter whether Transfer Restricted messages are allowed or not.

1 = enable (allowed)

2 = disable (not allowed)(default)

For **-frestart** <*FastRestart*> enter the Fast Restart state

1 = enable

2 = disable (default)

For **-distsccp** <*DistributedSccp*> enter the Evenly Distributed Class 0 SCCP state

1= enable (allowed)

2 = disable (not allowed) (default)

For **-multicong** <*MultiCongestion*> enter Allow Multiple Congestion Levels

1= enable (allowed)

2 = disable (not allowed) (default)

For **-sumroute** <*SummaryRouting*> enter summary route state.

This parameter is used to control the usage of the summary route when both a summary route (or ANSI cluster route) and a full point-code route (within that summary) are configured. It is used to indicate whether the summary route is to be used when the full point-code destination is inaccessible as follows.

1= enable (allowed) (default)

2 = disable (not allowed)

For **-linktest** <*AutoLinkTest*> enter whether Auto Link Test is to be performed when link is up

1= enable (allowed)

2 = disable (not allowed) (default)

For **-prevtxp** <*PreventiveTxp*> enter whether a link test is automatically run when the link comes into service. Link test is performed by sending an SLTM message and verifying the acknowledgment (SLTA) from the adjacent node. A link test is automatically run when the link comes into service.

1= enable (allowed)

2 = disable (not allowed) (default = 2)

Step 2 To create an SS7 point code for the signaling gateway, use the **addss7pc** command. This command has the following format.

addss7pc <*PointCodeIndex*> <*PointCode*><*PointCodeType*>

For <*PointCodeIndex*> enter a point code index, an integer in the range of 1 to 3.

For <*PointCode*> enter a point code in the format of <p1>.<p2>.<p3>,

where p1, p2, p3 = 0..255, for example 255.255.255

For <*PointCodeType*> enter the point code type.

1 - primary

2 - secondary

3 - capability

Step 3 To create an SS7 link set, use the addss7linkset command. The signaling gateway can have up to 64 linksets and a linkset can consist of up to 16 SS7 links.

addss7linkset <*LinksetId*> <*SourcePointCodeId*> <*AdjPointCode*>
[-**name** <*LinksetName*>][-**slsrot** <*SlsRotate*>][-**slsshift** <*SlsShift*>]
[-**llinh** <*LastLinkInhibit*>][-**prof** <*ProfileId*>][-**shut** <*LocalInhibit*>]

For <*LinksetId*> enter a Link Set ID, an index number in the range of 1 to 32.

For <*SourcePointCodeId*> enter the Source point code ID, an integer in the range of 1 to 3.

For <*AdjPointCode*> enter the adjacent point code in the format of <p1>.<p2>.<p3>,

where p1, p2, p3 = 0..255, for example 255.255.255

For -**name** <*LinksetName*> enter the name of the linkset, a character string of up 19 characters.

For -**slsrot** <*SlsRotate*> enter the signaling link selector rotation state. This defines whether or not signaling link selector(SLS) is rotated. This option only applies to ANSI variant and returns false for all other variants. By default, SLS rotation is enable by default for ANSI linksets. ANSI specifications state that SLS rotation should not be performed on C type linksets.

1 = enable (default)

2 = disable

For -**slsshift** <*SlsShift*> enter a value used to shift the signaling link selector (SLS) when rotation is enabled. This option only applies to ANSI variant and will return 0 all other variants. An integer in the range of 0 to 3.

For -**llinh** <*LastLinkInhibit*> enter whether taking out-of-service of the last link of a linkset is prohibited.

1 = Signaling gateway will first verify whether a link is the last link in the linkset when user tries to delete a link. If so, such action will be denied. (Default is 1).

2 = No checking is done, user could delete the last link from the linkset. In this case, one could loose the connectivity.

For -**prof** <*ProfileId*> Enter a profile ID, and integer in the range of 0 to 10. When specified this value indicates which profile will be used to establish defaults for common configuration values like MTP2 and MTP3 timers. The zero value is used to indicate that the linkset does not have a profile.

For -**shut** <*LocalInhibit*> enter the Linkset shutdown state

1 = shutdown

2 = not- shutdown

Repeat this command as necessary for each linkset to be configured.

Step 4 To create an SS7 link, use the **addss7link** command. A linkset can have up to 16 links. The format of this command is.

addss7link <*LinksetId*> <*SignalLinkCode*> <*Ds0IfIndex*>

[-**name** <*LinkName*>][-**shut** <*LinkShut*>][-**test** <*SignalLinkTest*>]

For <*LinksetId*> enter a linkset ID, an integer in the range of 1 to 32.

For <*SignalLinkCode*> enter a Signal Link Code, an integer in the range of 0 to 15.

For <*Ds0IfIndex*>, enter the line number of the link endpoint in one of the following formats.

Interface Type	Line Number Format	Values

OC3/SDH	bay.line.path.vtg.vt:ds0 or bay.line.path.ds1:ds0	bay {1 - upper} line (range=1..4) path (range=1..3) vtg (range=1..7) vt (range=1..4)(ds1) (range=1..3)(e1) ds1 (range=1..28) ds0 (range= 1..24 for T1 1..31 for E1)
T1/E1	bay.line:ds0	bay {1 - upper} line (range=1..24) ds0 (range= 1..24 for T1 1..31 for E1
T3	bay.line.ds1:ds0	bay {1 - upper} line (range=1..3) ds1 (range=1..28) ds0 (range= 1..24 for T1 1..31 for E1

For -**name** <*LinkName*> enter the name of the link, a character string of up 20 characters.

For -**shut** <*LinkShut*> enter the Linkset shutdown state

1 = shutdown

2 = not- shutdown

For -**test** <*SignalLinkTest*>enter the Signaling Link Test state

1 = enable (default)

2 = disable

Repeat this command as necessary for each link to be configured.

Step 5 To create an SS7 Route, use the **addss7route** command. The signaling gateway can maintain characteristics of each SS7 route (for example, state of congestion) to determine how to handle messages to the SS7 network. The format of this command is.

addss7route <*Dpc*> <*DpcMask*> <*LinksetCost*> <*LinksetId*>

For <*Dpc*> enter the destination point code of the route in the format of <p1>.<p2>.<p3>,

where p1, p2, p3 = 0..255, for example 255.255.255

Valid values are based on the SS7 variant (dspss7)

itu—7.255.7 or 7.255.0 or 7.0.0
ansi—255.255.255 or 255.255.0 or 255.0.0

For <*DpcMask*> enter the mask used to define which part of Destination Point Code is significant when comparing the Destination Point Code to the destination code point in the packet to be routed.Destination Point Code Mask

For <*LinksetCost*> enter the cost assigned to this linkset matching this route. Higher numbers represent higher cost. An integer in the range of 1 to 9.

For <*LinksetId*> enter the linkset ID. An index number in the range of 1 to 32.

Repeat this command as necessary for each route to be configured.

To add an SS7 Profile Timer, use the **addss7proftimer** command. The format of this command is:

addss7proftimer <*ProfileIndex*> <*TimerNum*> <*TimerValue*>

For <*ProfileIndex*> Enter an index number in the range of 1 to 32.

For <*TimerNum*> enter an Index into table containing timer information as follows;

1 = T01	16 = T116	31 = T31
2 = T02	17 = T117	32 = T32
3 = T03	18 = T118	33 = T33
4 = T04	19 = T119	34 = T34
5 = T05	20= T120	35 = T35
6 = T06	21 = T121	38 = alignReady
7 = T07	22 = T122	39 = notAlign
8 = T08	23 = T123	40 = align
9 = T09	24 = T124	41 = provNormal
10 = T010	25 = T125	42 = ProvEmerg
11 = T011	26 = T126	43 = sendSIB
12 = T012	27 = T127	44 = rmtCongest
13 = T013	28 = T128	45 = xDelayACK
14 = T014	29 = T129	
15 = T015	30 = T130	

For <*TimerValue*> enter a timer value in milliseconds.

Configure the IP Network Side

To configure the IP side of the Signaling Gateway, perform the following steps.

Step 1 Create an instance of the IP side of the signaling gateway, use the **addl3ua** command. The format of this command is.

addl3ua <SctpPort> [-**shut** <*GwShut*>][-**rwin** <*RcvWindow*>][-**prio** <*UnorderPriority*>]
[-**instrm** <*MaxInStream*>][-**queue** <*TxQDepth*>][-**assorx** <*MaxAssocRx*>]
[-**prx** <*MaxPathRx*>][-**csto** <*CumSackTo*>][-**bdl** <*BundleEnable*>]
[-**bdlto** <*BundleTo*>][-**initrx** <*MaxInitRx*>][-**maxir** <*MaxInitRto*>]
[-**minrto** <*MinRto*>][-**maxrto** <*MaxRto*>][-**kpalive** <*KeepAliveTo*>]

For <SctpPort>This parameter specifies the local XUA SCTP port.

An integer in the range of 1 to 65535). The value zero is not allowed.

For -**shut** <*GwShut*> enter whether the signaling gateway (SG) XUA instance is shutdown or not.

1 = true (default). Indicates that the XUA Instance has been shutdown.

2 = false. Indicates that the XUA Instance is not shutdown

To configure this parameter to 'false' (to bring the XUA SG instance in service), at least one local IP has to be configured. Otherwise, the configuration attempt is rejected.

For -**rwin** <*RcvWindow*> enter the size of the advertised receiving window, in bytes, for the SCTP association. An integer in the range of 1500 to 65535 bytes)(default=64000)

For -**prio** <*UnorderPriority*> enter the delivery priority of the unordered data. 'high': delivered first before sequenced data 'equal': same priority as sequenced data.

1 = high

2 = equal (default)

For -**instrm** <*MaxInStream*> enter the maximum number of inbound SCTP streams allowed at this signaling gateway. An integer in the range of 1 to 336)(default=17)}

For -**queue** <*TxQDepth*> enter the allowed maximum number of ULP (Upper Layer Protocol) datagrams waiting to be sent in transmission queue. An integer in the range of 0 to 65535 datagrams)(default=1000)}

For -**assorx** <*MaxAssocRx*> enter the maximum number of data retransmissions in the association context. This value must be smaller than the maximum number of data retransmissions in the association context. An integer in the range of 2 to 10)(default=10)}

For -**prx** <*MaxPathRx*> enter the maximum number of data retransmission in a SCTP path for a remote IP. The remote IP is considered Inactive after retransmitting for the value specified in this parameter. An integer in the range of 2 to 10)(default=4)}

For -**csto** <*CumSackTo*> enter the amount of time to wait for the cumulative selective ACK. An integer in the range of 100. to 500 ms)(default=200)}

For -**bdl** <*BundleEnable*> enter whether to enable or disable SCTP user message bundling. Multiple user messages can be bundled into a single SCTP packet to transmit. During a period of congestion, the implementation bundles messages whenever possible even if bundling is disabled.

1 - true (default)

2 - false

For -**bdlto** <*BundleTo*> enter the maximum amount of time that SCTP will wait for messages for bundling. Multiple user messages can be bundled into a single SCTP packet. This parameter allows a user to configure the packet bundling interval to be used for a new SCTP association. An integer in the range of 100 to 1000 ms)(default=100)

For -**initrx** <*MaxInitRx*> Enter the maximum number of times SCTP initialization and cookie chunks to be retransmitted before reporting failure for association request. Modification of this parameter does not affect existing association as this parameter is used during association initialization. If this parameter is changed after association initialization, the new value will be used when restarting association. An integer in the range of range of 1 to 10)(default=8)

For -**maxir** <*MaxInitRto*> enter the retransmission interval for initialization and cookie chunks. Modification of this parameter does not affect existing association as this parameter is used during association initialization. If this parameter is changed after association initialization, the new value will be used when restarting association. An integer in the range of range of 2000 to 20000 ms)(default=1)

For -**minrto** <*MinRto*> enter the lower bound for retransmission time out doubling operation, up on RTO timer expire. RFC 2960 specifies up on RTO timer expire, retransmission time out values should be doubled for the next retry. An integer in the range of range of 300 to 60000 ms)(default=1000)

For -**maxrto** <*MaxRto*> enter the upper bound for retransmission time out doubling operation, up on RTO timer expire RFC 2960 specifies up on RTO timer expire, retransmission time out values should be doubled for the next retry. User can specify upper bound for this retransmission time out. Once this value is reached, time out value is not going to be doubled. An integer in the range of range of range=300 to 60000 ms)(default=1000)

For -**kpalive** <*KeepAliveTo*> enter the heartbeat timeout interval for the SCTP path. An integer in the range of range of 500 to 60000 ms)(default=3000)

Step 2 To add an XUA local IP address for the signaling gateway IP side, use the **addl3ualocip** command. The format of this command is.

addl3ualocip <*LocIpIndex*> <*LocIpAddress*>

For <*LocIpIndex*> enter a local IP index. An integer in the range of 1 to 4

For <*LocIpAddress*> enter the local IP address of the XUA signaling gateway in dotted decimal notation.

Step 3 Bring the gateway IP side to the up state, use the **cnfl3ua** command. To do this, the user need only specify the -shut parameter as follows.

cnfl3ua -shut 2

Configure the Application Server Processes and Application Servers

To configure the Application Server Processes and Application Servers, perform the following steps.

Step 1 To create an IP side (M3UA) Application Server Process, use the **addl3uaasp** command. The format of this command is.

addl3uaasp <*AspIndex*> <*AspName*> <*RemotePort*> [-**aspshut** <*AspShut*>]
[-**aspblock** <*Block*>][-**aspqos** <*QosClass*>] [-**aspqueue** <*TxQDepth*>]
[-**aspassorx** <*MaxAssocRx*>][-**aspprx** <*MaxPathRx*>] [-**aspcsto** <*CumSackTo*>]
[-**aspbdl** <*BundleEnable*>][-**aspbdlto** <*BundleTo*>] [-**aspminrto** <*MinRto*>]
[-**aspmaxrto** <*MaxRto*>][-**aspka** <*KeepAliveTo*>] [-**mtype** <*MatchType*>]
[-**mqos** <*MatchQos*>][-**msi** <*MatchSi*>]

For <*AspIndex*> enter an L3UA Application Server Process index. An integer in the range of 1 to 16.

For <*AspName*>enter the name of the Application Server Process. A character string of up to 12 characters.

For <*RemotePort*> enter the configured remote SCTP port number used to create the association. The value zero means any nonzero remote port is acceptable. An integer in the range of 0 to 65536.

For -**aspshut** <*AspShut*> enter the ASP state.

1 = true (default). Indicates that the ASP has been shutdown

2 = false. Indicates that the ASP is not shutdown.

To configure this parameter to false, at least one ASP remote IP must have been added. Otherwise, the attempt is rejected.

For -**aspblock** <*Block*> enter whether ASP is blocked or not.

When an ASP is blocked, it cannot receive normal data traffic, but it can send or receive control messages.

1 = true. Indicates that the ASP has been blocked by an administrative action.

2 = false (default). Indicates that the ASP is not blocked.

When this parameter is set to false, all of the configured remote IP take effect, and this ASP is ready for service. The SCTP association are created and all the configuration for this ASP are in sync with the SCTP layer. After true is configured when the previous value is false, service is interrupted.

For -**aspqos** <*QosClass*> enter the QOS class for the ASP. An integer in the range of 0 to 7 (default = 0). A value of zero (0) indicates that QOS class is not defined.

When QOS class is defined, it overrides the QOSclass specified in the **addqosclass** and **cnfqosclass** commands.

For -**aspqueue** <*TxQDepth*> enter the allowed maximum number of ULP (Upper Layer Protocol) datagrams waiting to be sent in transmission queue. An integer in the range of 0 to 65535 datagrams) (default=1000).

For -**aspassorx** <*MaxAssocRx*> enter the cumulative selective acknowledgment time-out value used when a new SCTP association starts.An integer in the range of 100 to 500 (default=200).

For-**aspprx** <*MaxPathRx*> enter the maximum number of data retransmission in a SCTP path for a remote IP. The remote IP is considered Inactive after retransmitting for the value specified in this parameter. An integer in the range of 2 to 10) (default=4).

For -**aspcsto** <*CumSackTo*> enter the cumulative selective acknowledgment time-out value used when a new SCTP association starts.An integer in the range of 100 to 500 (default=200).

For -**aspbdl** <*BundleEnable*> enter whether to enable or disable SCTP usermessage bundling.

1 = true

2 = false (default=1)

Multiple user messages can be bundled into a single SCTP packet to transmit. During period of congestion, the implementation bundles messages whenever possible even if bundling is disabled.

For -**aspbdlto** <*BundleTo*> enter the maximum amount of time that SCTP will wait for messages bundling. An integer in the range of 100 to 1000 ms) (default=100)

For -**aspminrto** <*MinRto*> enter the lower bound for retransmission time out doubling operation, up on RTO timer expire RFC 2960 specifies up on RTO timer expire, retransmission time out values should be doubled for the next retry. An integer in the range of 300 to 60000 ms) (default=100).

For -**aspmaxrto** <*MaxRto*> enter the upper bound for retransmission time out doubling operation, up on RTO timer expire RFC 2960 specifies up on RTO timer expire, retransmission time out values should be doubled for the next retry. User can specify upper bound for this retransmission time out. Once this value is reached, time out value is not going to be doubled. An integer in the range of 300 to 60000 ms) (default=100).

For -**aspka** <*KeepAliveTo*> enter the heart beat timeout interval for the path. An integer in the range of 500 to 60000 ms) (default=3000).

For -**mtype** <*MatchType*> enter the match criterion to classifying packets for QoS functionality.

1 = matchNone (default)

2 = matchAny

3 = matchSi

For -**mqos** <*MatchQos*> enter the QoS class identifier used to assign a QoS class number to all inboundpackets.This parameter is only applicable if parameter -mtype is set to matchAny. An integer in the range of 0 to 7.

For -**msi** <*MatchSi*> enter the match service indicator used to assign a QoS class number to any inbound packet that has a specific service indicator. This parameter is only applicable when -mtype is set to matchSi. An integer in the range of 0 to 15.

Repeat this command as necessary to create other Application Server Processes.

Step 2 To add an XUA ASP remote IP, use the **addl3uaremip** command. The format of this command is.

addl3uaremip <*RemIpIndex*> <*AspName*> <*RemIpAddress*>

For <*RemIpIndex*> enter an index for the ASP's remote IP table. An integer in the range of 1 to 64.

For <*AspName*> enter the name of the Application Server Process. A character string of up to 12 characters.

For <*RemIpAddress*> enter the remote IP address used to create the association supporting this ASP. An IP address in dotted decimal notation.

Repeat this command as necessary for each Application Server Process

Step 3 To add a XUA Application Server entry, use the **addl3uaas** command. The format of this command is.

addl3uaas <*AsIndex*> <*AsName*> <*AsRc*> <*RkParm*> [-**dpc** <*RkDpc*>][-**opc** <*RkOpc*>] [-**omask** <*OpcMask*>][-**si** <*RkSi*>][-**gtt** <*RkGtt*>][-**cicmin** <*RkMinCic*>] [-**cicmax** <*RkMaxCic*>][-**asshut** <*AsShut*>] [-**asqos** <*QosClass*>][-**traf** <*TrafMode*>] [-**na** <*AsNa*>][-**minasp** <*MinActAsps*>] [-**asrto** <*RecoveryTo*>][-**asbrto** <*BurstTo*>]

For <*AsIndex*> enter an index of the Application Server table. An integer in the range of 1 to 16.

For <*AsName*> enter the Application Server name. This name has only local significance. A character string of up to 12 characters.

For <*AsRc*> enter the AS Routing Context a 32 bit number in the range of 0 to 4294967295.

An ASP may be configured to serve more than one AS. In this case, the Routing Context parameter is exchanged between the SG and the ASP, identifying the relevant AS. The Routing Context uniquely identifies the range of traffic associated with a particular AS, which the ASP is configured to receive. There is a 1:1 relationship between a Routing Context value and a Routing Key within an AS.

For <*RkParm*> enter the AS Routing Key Parameters. This parameter supports multiple parameter inputs, e.g. 0, 3, 6 or 0-2.

0 = dpc—The AsRkDpc is the relevant column
1 = opc—AsRkOpc and AsRkOpcMask are the relevant columns
2 = opcmask—Indicates that a mask is to be applied when the opc is specified in the routing key. If the mask is not specified then the mask is assumed to be all zeros.
3 = si—The AsRkSi is the relevant column
5 = gtt—The AsRkGtt is the relevant column. It indicates that routing key for this AS can be the result of Global Title Translation.
6 = cic—The AsRkCicMin and AsRkCicMax are the relevant columns.

Valid parameter combinations depend upon the setting of the routing key service indicator (-si) parameter as follows:

1. Routing key service indicator (-si) is configured to 3 (SCCP), the following is allowed:

dpc + si
dpc + si + opc
dpc + si + ssn
dpc + si + ssn + opc

2. Routing key service indicator (-si) is configured to 4 (TUP) or 5 (ISUP), the following is allowed:

dpc + si
dpc + si + opc
dpc + si + cic
dpc + si + cic + opc

3. The following combinations are allowed for all sis:

gtt
dpc
dpc + opc
dpc + opc + opcMask

For -**dpc** <*RkDpc*> enter the AS Routing Key Destination Point Code (DPC).

The DPC has the input format of <p1>.<p2>.<p3>

where p1, p2, p3 are decimal values of 0-255 (255.255.255)

The opc bit in the RkParam parameter is used to indicate whether this object's value has any current relevance.

For -**opc** <*RkOpc*> enter the AS Routing Key Originating Point Code (OPC).

The OPC has the input format of <p1>.<p2>.<p3>

where p1, p2, p3 are decimal values of 0-255 e.g. 255.255.255.

The opc bit in the RkParam parameter is used to indicate whether this object's value has any current relevance.

For -**omask** <*OpcMask*> enter the AS Routing Key OPC Mask

Valid values are based on the SS7 variant (dspss7)

- itu—7.255.7 or 7.255.0 or 7.0.0
- ansi—255.255.255 or 255.255.0 or 255.0.0

The opcMask bit in the AsRkParameters is used to indicate whether this object's value has any current relevance.

For -**si** <*RkSi*> enter the AS Routing Key Service Indicator.

3 - sccp
4 - tup
5 - isup

The si bit in the AsRkParameter is used to indicate whether this object's value has any current relevance

For -**gtt** <*RkGtt*> enter whether to enable or disable AS Routing Key Global Title Translation (GTT)

1 - true
2 - false (default)

For -**cicmin** <*RkMinCic*> enter the AS Routing Key Minimum CIC. An integer in the range of 0 to 65535.

The cic bit in the AsRk Parameter is used to indicate whether this object's value has any current relevance.

For -**cicmax** <*RkMaxCic*> enter the AS Routing Key Maximum CIC. An integer in the range of 0 to 65535.

The cic bit in the AsRkParameters is used to indicate whether this object's value has any current relevance

For -**asshut** <*AsShut*> enter the AS Shut state.

1 - true
2 - false (default)

true—Indicates that the AS has been shutdown by an administrative action. 'false' Indicates that the AS is not shutdown.

For -**asqos** <*QosClass*> enter the AS QoS Class. The AS specifies the QOS class for all its ASPs. An integer in the range of 0 to 7. (default=0)

For -**traf** <*TrafMode*> enter the AS Traffic Mode. Specifies the data packet traffic mode received for this AS.

1 - overRide (default)
2 - loadBind
3 - loadRndRobin
4 - broadCast
5 - undefined

For -**na** <*AsNa*> enter the AS Network Appearance. An integer in the range of 0 to 4294967295.

The Network Appearance is a local reference shared by SG and AS that together with a point code uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. It can be used to distinguish between signaling traffic associated with different networks being sent between the SG and the ASP over a common SCTP association. An example scenario is where an SG appears as an element in multiple separate national SS7 networks and the same point code value may be reused in different networks.

For -**minasp** <*MinActAsps*> enter the Minimum Active ASPs. An integer in the range of 0 to 16. (default=0). The minimum number of active ASPs serving this AS.

For -**asrto** <*RecoveryTo*> enter the Recovery Timeout. An integer in the range of 0 to 2000 ms. (default=2000)

This parameter specifies the amount of time to wait for the AS recovery process.

For -**asbrto** <*BurstTo*> enter the Burst Recovery Timeout. An integer in the range of 1000 to 10000 ms. (default=4000)

This object specifies the amount of time allowed for an association to recover from burst of traffic due to fail-over.

Step 4 To add a XUA Application Server Process Application Server entry, use the **addl3uaaspas** command. The format of this command is.

addl3uaaspas <*Index*> <*AspName*> <*AsName*> <*AspWeight*>

For <*Index*> enter an ASP AS Index. An integer in the range of 1 to 256.

For <*AspName*> enter the Application Server Process name. A character string of up to 12 characters.

For <*AsName*> enter the Application Server name. A character string of up to 12 characters

For <*AspWeight*> enter the ASP Weight. An integer in the range of 0 to 10.

When Traffic Mode is specified as loadRndRobind (see addl3uaas),this parameter specifies the weight which is used in Weighted Round Robin algorithm.

When the weight is 0, this particular ASP is selected only when there are no other active ASPs with a non-zero weight.

Step 5 To add a XUA Application Server Route entry, use the **addl3uaasroute** command. The format of this command is:

addl3uaasroute <*Index*> <*RouteName*> <*AsrRc*> <*AsrDpc*> [-**asrshut** <*AsrShut*>]

For <*Index*> enter the ASP Route Index. An integer in the range of 1 to 16.

For <*RouteName*> enter the Application server route name. A character string of up to 12 characters.

For <*AsrRc*> enter the AS Route Routing Context. An integer in the range of 0 to 4294967295.

For <*AsrDpc*> enter the AS Route Destination Point Code (DPC)

The DPC has the format: <p1>.<p2>.<p3>

where p1, p2, p3 are decimal values of 0 - 255 (255.255.255).

For -**asrshut** <*AsrShut*> enter whether the AS Route Shut is up or down (false).

1—true
2—false (default)

Step 6 To add an XUA IP QoS Class, use the **addqosclass** command.

addqosclass <*QosClass*> <*QosType*> [-**prcd** <*QosPrcdValue*>][-**dscp** <*DiffSrvCodePoint*>]

For <*QosClass*>, this parameter creates a L3UA quality of service (QoS) index.

An integer in the range of 1 to 7

For <*QosType*> enter the QoS type.

1 = ipPrecedence
2 = ipDscp

ipPrecedence specifies that IP Type of Service (TOS) is based on the PrecedenceValue.

ipDscp specifies that IP Type of Service (TOS) is based on the DiffServ Code Point.

For -**prcd** <*QosPrcdValue*> enter the ipPrecedence value. An integer in the range of -1 to 7.

This parameter value is used if QoSType is ipPrecedence.

For -**dscp** <*DiffSrvCodePoint*> enter the DiffServ Code Point. An integer in the range of -1 to 63.

This parameter value is used if QoSType is ipDscp.

Step 7 To bring the Application Server Process into the up state, use the **cnfl3uaasp** command. The format of this command is:

cnfl3uaasp <*AspIndex*> [-**aspshut** <*AspShut*>]
[-**aspblock** <*Block*>][-**aspqos** <*QosClass*>] [-**aspqueue** <*TxQDepth*>]
[-**aspassorx** <*MaxAssocRx*>][-**aspprx** <*MaxPathRx*>] [-**aspcsto** <*CumSackTo*>]
[-**aspbdl** <*BundleEnable*>][-**aspbdlto** <*BundleTo*>] [-**aspminrto** <*MinRto*>]
[-**aspmaxrto** <*MaxRto*>][-**aspka** <*KeepAliveTo*>] [-**mtype** <*MatchType*>]
[-**mqos** <*MatchQos*>][-**msi** <*MatchSi*>]

To bring the ASP to the up (not shutdown) state, merely, use the **-aspshut** parameter as follows.

cnfl3uaasp -aspshut 2

Configure SCCP-GTT Table

To configure processing rules in the SCCP-GTT module, perform the following steps.

Step 1 Make sure that any Application Servers that will be accessed by the GTT processes are already configured (see the addl3uaas command).

Step 2 To specify GTT Prefix mappings, use the **addss7gttpref** command. The format of this command is:

addss7gttpref <*PrefIndex***> <***PrefName***> <***InAddr***> [-outaddr <***OutAddr***>][-tnai <***TblNAI***>]**
[-tnp <*TblNP***>][-inai <***ItemNAI***>][-inp <***ItemNP***>][-encschem <***PrefEncodingScheme***>]**

GTT prefix conversion specifies mappings such as E.212-to-E.214 address conversion and E.212-to-E.164 address conversion. The prefix conversion involves matching of GTA digits in the input address and then replacing those digits with the digits in output address.

For **<***PrefIndex***>** enter a prefix conversion index number, an integer in the range of 1 to 20.

For *PrefName***>** enter a prefix conversion table name. A character string of up to 12 characters.

For **<***InAddr***>** enter a prefix conversion in address in the format of a hexadecimal character string of 1 to 15 characters {0, 1, 2..9, A, B..F}

This object specifies the prefix input address. If the GTA of the Called Party Address (CDPA) matches the digits in this object, then the prefix conversion is performed. The address is configured in hexadecimal string, and null string indicates that address has not been specified.

For **-outaddr <***OutAddr***>** enter a prefix conversion out address in the format of a hexadecimal character string of 1 to 15 characters {0, 1, 2..9, A, B..F}

This object specifies the prefix output address. If the GTA of the Called Party Address (CDPA) matches the digits in the input address then this object is used in the prefix conversion.The address is configured in hexadecimal string, and null string indicates that address has not been specified.

For **-tnai <***TblNAI***>** enter a network address indicator in the range of 0 to 127|253. (default=253)

The following values are generally used:

Unknown Nature of Address (0)
Subscriber Number (1)
Reserved for national use (2)
National Significant Number (3)
International Number (4)
Maximum NAI (127)
Invalid (253)

For **-tnp <***TblNP***>** enter a umbering plan, an integer in the range of 0 to 15, or the value of 253

The following values are generally used:

Unknown NP (0)
ISDN/Telephony NP (1)
Spare (2)
Data NP (3)
Telex NP (4)
Maritime Mobile NP (5)
Land Mobile NP (6)
ISDN/Mobile NP (7)
Private NP (8)
Max NP (15)
Invalid (253)

For **-inai <*ItemNAI*>** enter an item network address indicator, an integer in the range or 0 to 127 or the value of 253.

The following values are generally used:

Unknown Nature of Address (0)
Subscriber Number (1)
Reserved for national use (2)
National Significant Number (3)
International Number (4)
Maximum NAI (127)
Invalid (253).

For **-inp <***ItemNP***>** enter an item numbering plan (range=0..15|253) (default=253)

The following values are generally used:

Unknown NP (0)
ISDN/Telephony NP (1)
Spare (2)
Data NP (3)
Telex NP (4)
Maritime Mobile NP (5)
Land Mobile NP (6)
]ISDN/Mobile NP (7)
]Private NP (8)
] Max NP (15)
]Invalid (253)

For **-encschem <***PrefEncodingScheme***>** enter the encoding scheme

0 - unknown (default)
1 = BCD odd
2 = BCD even
3 = national specific

Reference—E.164 and E.214 address formats and Q.713.

Step 3 Specify Global Title Translation (GTT) Mated Applications (MAP) for a specified point code and subsystem number using the **addss7gttmap** command. The format of this command is:

addss7gttmap <*MapIndex***> <***Pc***> <***Ssn***> [-mult <***MultInd***>][-bcpc <***BackupPc***>] [-bcssn <***BackupSsn***>][-rrc <***ReRouteOnCong***>] [-adj <***PcAdjacent***>]**

A mated application (MAP) entry has two main purposes:

- MAP entries are used internally by the SCCP application to track point code states and SSN states, such as congestion and availability.
- MAP entries are used to define backups or alternates for point code-SSN combination.

For **<***MapIndex***>** enter a map index. An integer in the range of 1 to 20.

For **<***Pc***>** enter a point code in the format of <p1>.<p2>.<p3>,

where p1, p2, p3 = 0..255, for example 255.255.255

For **<***Ssn***>** enter a subsystem number.An integer in the range of 2 to 255.

This parameter specifies the primary subsystem number of the Mated Application.

For **-mult <***MultInd***>** enter a multiplicity indicator

1 = solitary (default)
2 = shared
3 = dominant

For **-bcpc <***BackupPc***>** enter a backup point code in the format of <p1>.<p2>.<p3>,

where p1, p2, p3 = 0..255, for example 255.255.255.

This object specifies the backup point code for the Mated Application. The Point Code and backup Point Code cannot be identical. The backup Point Code must be specified only if Multiplicity indicator is set to share or dominant. Otherwise, this value does not apply.

For **-bcssn <***BackupSsn***>** enter a backup subsystem number. An integer in the range of 2 to 255. (default=2)

For **-rrc <***ReRouteOnCong***>** enter whether re-route on congestion is enabled or disabled.

1 = enable
2 = disable (default)

This object specifies the Mated Application re-route on congestion truth value. This object is invalid when Multiplicity indicator is solitary.

For **-adj <***PcAdjacent***>** enter whether point code adjacent is enabled or disabled.

1 = enable (true)
2 = disable (false) (default)

This object specifies the Mated Application Point Code adjacent truth value.

true—Indicates that MAP PC is adjacent.
false—Indicates that MAP PC is not adjacent.

Step 4 To add a GTT selector entry, use the **addss7gttsel** command.

A GTT selector defines the parameters that select the translation table used to translate an SCCP message to its next or final destination. The format of this command is:

addss7gttsel <*SelIdx*> <*SelName*> <*TT*> <*GTI*> <*NP*> <*NAI*> [**-qos** <*QOS*>]
[-**pre** <*PrePrefName*>][-**post** <*PostPrefName*>]

For <*SelIdx*>Selector index. An integer in the range of 1 to 20.

For <*SelName*> Selector name. A character string of up to 12 characters.

For <*TT*> enter the Translation type. An integer in the range of 0 to 255.

For <*GTI*> Global title indicator

2 = GT includes only TT
4 = GT includes TT, NP, NAI

For <*NP*> enter the Numbering plan. An integer in the range of 0 to 15.

The following values are generally used:

Unknown NP (0)
ISDN/Telephony NP (1)
Spare (2)
Data NP (3)
Telex NP (4)
Maritime Mobile NP (5)
Land Mobile NP (6)
ISDN/Mobile NP (7)
Private NP (8)
Max NP (15)

For <*NAI*> enter the Network address indicator. An integer in the range of 0 to 127.

The following values are generally used:
Unknown Nature of Address (0)
Subscriber Number (1)
Reserved for national use (2)
National Significant Number (3)
International Number (4)
Maximum NAI (127)

For **-qos** <*QOS*> enter the Quality of service. An integer in the range of 0 to 7, or the value of 255. (default=0)

For -**pre** <*PrePrefName*> enter the Pre-prefix name. A character string of up to 12 characters.(default=null)

The Prefix Conversion Table is used to convert GTA digits. This object specifies that the conversion occurs 'before' global title translation. The null string indicates that a prefix conversion table has not been specified.

For -**post** <*PostPrefName*> enter the Post-prefix name. A character string of up to 12 characters. (default=null)

The Post Prefix Conversion Table is used to convert GTA digits. This object specifies that the conversion occurs after global title translation. The null string indicates that a post conversion table has not been specified.

Step 5 Specify GTT Application Groups, use the **addss7gttappgrp** command. This command has several different format depending upon whether the object of the application groups is an application server, a point code, or a point code and subsystem number.

For a specified application server, the format of the command is:

addss7gttappgrp -**as** <*AppGrpIndex*> <*GrpName*> <*AsName*> [-**ri** <*RouteInd*>][-**ssn** <*Ssn*>][-**mult** <*MultInd*>][-**cost** <*Cost*>][-**weight** <*GrpWeight*>][-**nwname** <*GrpNetwork*>]

For a point code, the format of the command is:

addss7gttappgrp -**pc** <*AppGrpIndex*> <*GrpName*> <*Pc*> [-**ri** <*RouteInd*>][-**mult** <*MultInd*>][-**cost** <*Cost*>][-**weight** <*GrpWeight*>][-**nwname** <*GrpNetwork*>]

For a spedified point code and subsystem number, the format of the command is:

addss7gttappgrp -**pcssn** <*AppGrpIndex*> <*GrpName*> <*Pc*> [-**ri** <*RouteInd*>][-**ssn** <*Ssn*>][-**mult** <*MultInd*>][-**cost** <*Cost*>][-**weight** <*GrpWeight*>][-**nwname** <*GrpNetwork*>]

For <*AppGrpIndex*> enter a global title address index. An integer in the range of 1 to 20.

For <*GrpName*> enter an application group name. A character string of up to 12 characters.

For <*AsName*> enter an application server name. A character string of up to 12 characters.

For <*Pc*> enter the point code in the format of <p1>.<p2>.<p3>,

where p1, p2, p3 = 0..255, for example 255.255.255

For -**ri** <*RouteInd*> Routing indicator

1 = gt (default)
2 = pcssn

For -**ssn** <*Ssn*> enter the subsystem number. An integer of the value 0 or in the range of 2 to 255. (default=0)

For -**mult** <*MultInd*> enter a multiplicity indicator

2 - shared (default)
4 - cost
5 - cgpa

For -**cost** <*Cost*> enter the cost. An integer in the range of 1 to 7. (default=1)

This object specifies the cost for the item in the GTT Application Group. This object is only applicable when the multiplicity indicator parameter has 'cost' or 'shared' value. Otherwise, this value does not apply

For -**weight** <*GrpWeight*> enter the weighting factor (range=1..999) (default=1)

Only applicable when multiplicity indicator is cgpa.

This object specifies the weighting factor used for the item in the GTT Application Group. This object is only applicable when the multiplicity indicator parameter has cgpa value. Otherwise, this value does not apply.

For -**nwname** <*GrpNetwork*> enter a target network name. A character string of up to 12 characters. (default=null)

Step 6 Specify a GTT GT Address entry, use the **addss7gttgta** command. This command has several different format depending upon whether the object of the GT Address is an application server, an application group, a point code, or a point code and subsystem number.

For a specified application server, the format of the command is:

addss7gttgta -**as** <*GtaIdx*> <*GTAddr*> <*SelName*> <*AsName*> [-**tag** <*TtSsnTag*>][-**ttssn** <*TtSsn*>][-**qos** <*QOS*>][-**ri** <*RI*>][-**nwname** <*Network*>]

For a specified application group, the format of the command is:

addss7gttgta -**app** <*GtaIdx*> <*GTAddr*> <*SelName*> <*AppGrpName*> [-**qos** <*QOS*>]

For a specified point code, the format of the command is:

addss7gttgta -pc <*GtaIdx*> <*GTAddr*> <*SelName*> <*Pc*> [-**ri** <*RI*>][-**tag** <*TtSsnTag*>][-**ttssn** <*TtSsn*>][-**qos** <*QOS*>][-**nwname** <*Network*>]

For a specified point code and subsystem number, the format of the command is:

addss7gttgta -pcssn <*GtaIdx*> <*GTAddr*> <*SelName*> <*Pc*> [-**ri** <*RI*>][-**tag** <*TtSsnTag*>][-**ttssn** <*TtSsn*>][-**qos** <*QOS*>][-**nwname** <*Network*>]

For <*GtaIdx*> enter the Global title address index. An integer in the range of 1 to 20.

For <*GTAddr*> enter the Global title address. A string of up to 15 hexadecimal digits {0, 1, 2 - 9, A, B..F}) This parameter specifies the address digits in hexadecimal of the Called Party Address (CDPA). This object is mandatory when creating an entry

For <*SelName*> enter the Selector name. A character string of up to 12 characters.

For <*AsName*> enter the Application server name. A character string of up to 12 characters.

For <*AppGrpName*> enter the Application Group name. A character string of up to 12 characters.

For <*Pc*>enter the Point code. The PC has the format: <p1>.<p2>.<p3>

where p1, p2, p3 are decimal values of 0-255 (255.255.255).

For -**ri** <*RI*> Routing indicator

1 = gt (default)
2 = pcssn

For -**tag** <*TtSsnTag*> enter the Translation type

1 = tt (title translation)
2 = ssn (subsystem number)
3 = not defined (default)

For -**ttssn** <*TtSsn*> enter the Translation type value:

For Title Translation. An integer in the range of 0 to 255 (default = 0).

For Subsystem Number. An integer of either 0 or in the range of 2 to 255 (default=0)

For -**qos** <*QOS*> enter the Quality of service. An integer in the range of 0 to 7, or the value of 255. (default=0)

For -**nwname** <*Network*> enter the Target network name. A character string of up to 12 characters. (default=null)

Loading and Upgrading VXSM Code Images

The chapter describes the procedure for setting up the image on a Cisco VXSM for the first time and for upgrading VXSM cards from an earlier software image.

Initial Considerations

To upgrade the image on a VXSM card while preserving the call processing service:

1. The VXSM card must be one of a redundant pair of VXSM cards (in adjacent slots).
2. Only one pair of VXSM cards can be upgraded at a time.
3. After the upgrade procedure starts, no configuration changes can occur until after the upgrade is complete.
4. VXSM downgrades are not supported.
5. Only those upgrade paths (marked with X) shown in Table 7-1 are allowed. Only like-to-like images are allowed. This table applies to single card upgrades and redundant card pairs upgrades.

Table 7-1 Allowable VXSM Image Upgrades

		To Version				
		Non-CALEA H.248	Non-CALEA TGCP	Non-CALEA MGCP	CALEA TGCP	CALEA MGCP
From Version	Non-CALEA H.248	X				
	Non-CALEA TGCP		X			
	Non-CALEA MGCP			X		
	CALEA, TGCP				X	
	CALEA, MGCP					X

6. Before the upgrade procedure can start, the new VXSM image must reside on the hard disk of the PXM cards. Browse the VXSM disk to ascertain whether or not the image exists. At the PXM prompt, the PXM card responds to UNIX-like commands (for example, cd for change directory; ls

for list short format) to allow the user to inspect the contents of the disk.

If the image does not exist, it must be downloaded from a workstation using the FTP protocol (refer to the *PXM-45 Configuration Guide* for more detailed information).

Check the release notes to see if the VXSM upgrade also requires an upgrade of the boot code image in addition to the runtime image. If it does, the boot code image must also reside on the PXM's hard disk.

Warning **BEFORE YOU PERFORM THE PROCEDURES DESCRIBED IN THIS CHAPTER, READ ALL OF THIS WARNING!**

Some commands for loading or upgrading boot and runtime images take several minutes to execute completely. If you resets or disturb 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 is complete.

After the execution of the burnboot, clrsmcnf, loadrev, or setrev commands, you 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 after the card enters Active, Standby, or Failed is it safe to go to the next step.

Loading a VXSM Image for the First Time

The procedure for loading images onto a VXSM card the first time the card is as follows.

Note All the commands in the following procedure are performed on the gateway's active PXM card. Check the command prompt to verify that you are logged into the PXM card.

Step 1 Telnet to the media gateway. Check that you have the PXM card prompt. If necessary, check the location of the VXSM cards by using the **dspcds** command.

Step 2 Check the release notes to see if the VXSM boot code image needs upgrading. If it does, use the **burnboot** command to burn the boot code onto the desired VXSM card (otherwise, skip to step 4).

```
burnboot <slot> <revision>
```

For *revision*, use the revision number of the boot code image to be loaded (see later in this chapter for information on revision numbers).

Step 3 Periodically check that the **burnboot** process has ended. To do this, use the **dspcds** or **dsprev** command on the PXM. When the state of the VXSM card is displayed as either Active, Standby, or Failed, proceed to the next step.

Step 4 Use the **clrsmcnf** command to the clear the VXSM card's configuration. The format of this command is:

```
clrsmcnf <slot-id> [all]
```

Step 5 Periodically check that the **clrsmcnf** process has ended. To do this, use the **dspcds** or **dsprev** command on the PXM. When the state of the VXSM card is displayed as either Active, Standby, or Failed, proceed to the next step.

Note If the -all parameter is used in the clrsmcnf command, the VXSM card will come up in the failed state. This is normal and is expected.

Step 6 Use the **setrev** command. This command loads a VXSM image with the specified call control protocol and a DSP image with the specified Codec Template. The format of this command is:

```
setrev <slot> <primary revision> [-ccp <CallControlProtocol>] [-co <CodecTemplateNumber>]
```

Specify the gateway control protocol as either H.248, TGCP, or MGCP as appropriate.

Specify the codec template number as either TGW/Wireline (default) or Cable as appropriate.

Step 7 Periodically check that the **setrev** process has ended. To do this use the **dspcds** or **dsprev** command on the PXM. When the state of the VXSM card is displayed as either Active, Standby, or Failed, proceed to the next step.

Step 8 Repeat steps 2 and 7 for any other VXSM cards that need to be brought up for the first time.

Step 9 Use the **addred** command to set up VXSM redundant pairs. The format of this command is:

```
addred <redprimaryslotnum><redstandbyslotnum><redtype>
```

Step 10 Switch to the VXSM cards. Use their commands to configure the cards as necessary and bring them into service.

Upgrade Procedure

To upgrade the VXSM cards, use the following steps. This procedure is for VXSM cards that are in service and provides a graceful upgrade in which call processing continues during the upgrade. This procedure can also be performed on one VXSM card, but the service is not preserved during the upgrade.

Warning **While upgrading a VXSM software image, it is extremely important to allow the following upgrade process to proceed without external user intervention other than the upgrade procedure. This applies to both the primary and secondary VXSM cards being upgraded and the gateway's PXM cards, External intervention may cause the VXSM cards to come up in the Failed state.**

In particular:
Do not reset VXSM or PXM cards manually or through commands such as resetcd or resetsys.
Do not save all MGX configuration with commands such as the saveallcnf command.
Do not toggle primary/secondary cards through commands such as switchredcd or delred.
Do not change the name of software image before or during the upgrade.
Do not change any configuration of active primary card during the upgrade.

This warning applies to the upgrade procedure through the completion of the commitrev command in Step 6 (see below).

If the upgrade procedure is interrupted for reasons outside the control of the user (for example, a power outage), see "Interrupted Procedure Recovery" below for instructions.

Telnet to the media gateway.

Note All the commands in the following upgrade procedure are performed on the gateway's active PXM card. Check the command prompt to verify that you are logged in to the PXM card.

Step 1 Determine which set of redundant VXSM cards is to be upgraded. Use the **dspcds** command if necessary to locate the slot numbers of the VXSM cards. Determine which VXSM card slot in the set is primary (active) and which is secondary (standby).

Step 2 Check the release notes to see if the VXSM boot code image needs upgrading. If it does, perform the following substeps a, b, c, and d; otherwise skip these steps and go to step 3.

a. use the **burnboot** command to burn the boot code onto the **standby** card.

```
burnboot <slot> <revision>
```

Note Make sure that the slot number in the burnboot command is that of the standby VXSM card.

For *revision*, use the revision number of the boot code image to be loaded (see later in this chapter for information on revision numbers).

b. Periodically check that the **burnboot** process has ended. To do this, use the **dspcds** or **dsprev** command on the PXM. When the state of the VXSM card is either Active, Standby, or Failed, proceed to the next step.

c. Use the **switchredcd** command to switch the states of the active and standby VXSM cards. The format of this command is:

```
switchredcd <fromslot><toslot>
```

The *fromslot* parameter is the slot number of the active card in the VXSM redundant pair. The *toslot* parameter is the slot number of the standby card in the VXSM redundant pair.

When this command is executed, the active card becomes the standby card and vice versa.

d. Use the **burnboot** command again to burn the boot code onto the new **standby** card.

Note Make sure that the slot number in the burnboot command is that of the new standby VXSM card.

e. Periodically check that the **burnboot** process has ended. To do this use the **dspcds** or **dsprev** command on the PXM. When the state of the VXSM card is displayed as either Active, Standby, or Failed, proceed to the next step.

f. Use the **switchredcd** command again to return the VXSM cards to their original states (active and standby).

After this command is executed, the originally active VXSM card is again active and the original standby card is again in standby. Both VXSM cards in the redundant pair have upgraded boot code with their original runtime code.

Step 3 Load the new runtime image onto the standby VXSM card using the **loadrev** command as follows:

```
loadrev <slot> <revision>
```

For *slot*, the user can enter either the slot number of the active or standby VXSM. PXM automatically selects the standby to load the new image. For *revision*, use the revision number of the image to be loaded (see later in this chapter for information on revision numbers).

Step 4 Periodically check that the **loadrev** process has ended. To do this, use the **dspcds** or **dsprev** command on the PXM. When the state of the VXSM card is displayed as either Active, Standby, or Failed, proceed to the next step.

Step 5 Use the **runrev** command to cause the active and standby cards to switch roles. This results is the new runtime image becoming the active image. The new image is also loaded onto the (now) standby card so that both cards are upgraded. The format of the **runrev** command is:

```
runrev <slot> <revision>
```

Step 6 Both VXSM cards in the redundant set have upgraded boot code images (if required) and runtime images. Use the **commitrev** command to finalize the upgrade procedure. This command removes the old images from the cards:

```
commitrev <slot> <revision>
```

Note If you suspect that an error occurred during the upgrade process, use to **abortrev** command to restore the images to their state before the upgrade was started.

Interrupted Procedure Recovery

If a VXSM software upgrade procedure is interrupted (for example, power outage), and both primary and secondary remain in Failed-U state, perform the following procedure:

Step 1 Execute the **abortrev** command:

abortrev <PrimarySlot> <NewImageRevision>

Step 2 If the primary VXSM becomes Failed/Active (out of Failed-U/Active), then execute the **resetcd** command:

resetcd <PrimarySlot>

Step 3 If the secondary VXSM becomes Failed/Active (out of Failed-U/Active), execute the **resetcd** command:

resetcd <SecondarySlot>

Both primary and secondary VXSM cards should have their original software image and original DB.

Image Filenames and Revision Numbers

Images have both a filename and a revision number.

Filenames

Filenames are used to download the image to the PXM hard disk and when browsing the disc to examine its contents. Filenames have the following formats.

cardtype_version-element{_platform}.fw

where version-element is composed of:

major-release.minor-release.maintenance.patch-phase

An example of a filename for VXSM 5.0.02 boot code is:

vxsm_005.000.002.200_bt.fw

An example of a filename for VXSM 5.0.02 runtime code is:

vxsm_005.000.002.202.fw

Revision Numbers

Revision numbers are used to identify images in the **burnboot**, **loadrev**, **runrev**, **commitrev**, and **abortrev** commands. Revision numbers are derived from the filenames by:

- Using only the version-element portion of the filename (card type, platform, and the.fw extension are not used).
- Removing the leading zeroes from the major/minor/maintenance/patch numbers.
- Enclosing the maintenance.patch number in parentheses.
- Adding a phase identifier to the end.

Thus, revision numbers appear in the general format:

major-release.minor-release(maintenance.patch)phase

Using this process, the filename *vxsm_005.000.002.202.fw* converts to the version number of

5.0(2.202)

Note In this example, the phase identifier is omitted because the image is released. Phase identifiers are used only for images that are still under development.

Note For details on upgrading images, filenames, and revision numbers, refer to the *Cisco MGX (PXM45/PXME1), MGX 9850, MGX 8830, and MGX 8880 Command Reference* under the **loadrev** description.

CALEA and Non-CALEA Image Numbering

A numbering relationship between a VXSM CALEA image and its corresponding non-CALEA image applies to filenames and version numbers.

The relationship is as follows:

The value of the *minor-release* field for a non-CALEA release has 50 added to it to signify the corresponding CALEA release.

For example, if the filename and revision number for a non-CALEA VXSM release are:

filename = vxsm_005.000.002.202.fw

revision number = 5.0(2.202)

The filename and revision number for the corresponding CALEA release is:

filename = vxsm_005.050.002.202.fw

revision number = 5.50(2.202)

CHAPTER 8

VXSM Troubleshooting

This chapter describes how to trouble shoot and resolve known types of problems on the Cisco MGX 8850 VXSM card. The following topics are covered in this chapter:

- Collecting Troubleshooting Data
- Troubleshooting Procedures
- Obtaining Information on Current Voice Calls—H.248
- Obtaining Information on Current Voice Calls—xGCP
- Bearer Tracing Feature
- Troubleshooting Commands

Collecting Troubleshooting Data

This section provides procedures for collecting troubleshooting data for when a VXSM card fails. These procedures use PXM45, VXSM, RPM-XF and AXSM commands. See Chapter 5, "VXSM CLI Commands" in this document for detailed descriptions of the VXSM CLI commands. Refer to the following documents for descriptions of the PXM45, RPM-XF and AXSM CLI commands:

- *Cisco MGX 8850 (PXM1E/PXM45), MGX 8950, and MGX 8830 Command Reference, Release 5.2.*
- *Cisco ATM Services (AXSM) Software Configuration Guide and Command Reference for MGX Switches, Release 5.2*
- *Cisco MGX Route Processor Module (RPM-XF) Installation and Configuration Guide, Release 4*

Table 8-1 shows the initial steps you can take using CLI commands to trouble shoot any problem on the VXSM. These steps enable you to collect data and failure reports.

Table 8-1 Initial Troubleshooting Steps Using CLI Commands

Run these CLI commands on the PXM45:
1. **dspcds**
2. **dspcd**
3. **dsplog**
4. **dsperr**
5. **dspversion**
6. **dsprev**

Table 8-1 Initial Troubleshooting Steps Using CLI Commands

7.	**dspclksrc**

Run these CLI commands on the VXSM:
1. **dspcd**
2. **dspversion**

Troubleshooting Procedures

Table 8-2 provides a list of known types of problems, their possible causes, and their possible solutions. The problems are listed alphabetically by topic.

Table 8-2 VXSM Troubleshooting Procedures

Problem	Possible Cause	Possible Solutions
Access to Card—Cannot use the **cc** command to access VXSM card.	VSXM card is not in the active or standby state. If the VSXM card is not in the active or standby state, you cannot use the **cc** command to access the card.	Verify that the VXSM card is in either the active or standby state, by issuing the PXM45 CLI command, **dspcds**. See Possible Solutions for "Active Card—VXSM card did not become active".
Active Card—VXSM card did not become active.	VXSM card was inserted into the wrong slot. Slot 7, 8, 15 and 16 are reserved for other service modules.	Remove the VXSM card. Verify that the pins on the backplane are not bent and the power key is intact. Attempt to insert the VXSM card into a slot that is not reserved.
	PXM45 and VXSM run time images are not compatible	Check the latest Cisco MGX8850 Release Notes and make sure that the PXM45 and VXSM images are current and are compatible. If they are not, update the VXSM boot image and runtime image by issuing the following PXM45 CLI commands: 1. **burnboot** 2. **setrev**
	VXSM runtime image is not available from the PXM45 hard drive or is corrupted.	Download the correct VXSM image to PXM45-HD. Use the PXM45 **dsprevs** CLI command in order to verify that the image file name and size are correct. Then, issue the **clrsmcnf** command and the **setrev** command to clear and reload the correct image.
	The **setrev** command was not executed for the VXSM card.	Issue the PXM45 CLI command, **setrev.**
	The VXSM card is inserted in a slot that was previously configured for a different card type and the slot is still in the Reserved state.	Insert the VXSM card into a different slot or issue the **clrsmcnf** CLI command.

Table 8-2 VXSM Troubleshooting Procedures (continued)

Problem	Possible Cause	Possible Solutions
Alarm— PVC is in alarm.	The OC3 cable is bad, does not exist, or is not connected properly.	1. Check for alarms on the AXSM line associated with the VXSM PVC using the **dsplns** and **dsplnalm** CLI commands. 2. On the AXSM, issue the **addlnloop** command with the option for local loopback set. 3. Check whether the alarm is cleared using the **dspcons** command. 4. If the alarm is cleared, check the TX/RX connections between the AXSM and the router's ATM interface. 5. If the TX/RX connections are correct, replace the OC3 cable.
	The router's ATM interface is not configured.	On the router, issue the IOS command, **show run**, to verify whether the VPI/VCI and traffic parameters are correct. If necessary, reconfigure the VPI/VCI and traffic parameters.
	The PVC has been added on the VXSM, but not on the AXSM, or vice versa.	Verify that the PVC has been added on both cards by issuing the **dspcons** command on both the VXSM and the AXSM. If necessary, add the connection, using the **addcon** command.
MGC-Initiated Commands Ignored	An association does not exist between the MGC and the VXSM.	Display the H.248 association state using the **dsph248state** CLI command (or SNMP equivalent) and specifying the GatewayLinkID.

Table 8-2 VXSM Troubleshooting Procedures (continued)

Problem	Possible Cause	Possible Solutions
VXSM is Rejecting Call Attempts		
	TDM/SCN termination does not exist.	Display the VIFs (Voice Interfaces) using the **dspvifs** CLI command (or SNMP equivalent). If the VIF corresponding to the TDM/SCN termination does not exist, it must be added using the **addvif** CLI command (or SNMP equivalent).
	H.248 packages not associated with VIF.	Display the VIFs (Voice Interfaces) using the **dspvifs** CLI command (or SNMP equivalent). Verify that the appropriate H.248 packages have been added corresponding to the VIFs. H.248 packages can be added using **cnfvifterm** CLI command (or SNMP equivalent).
	Inadequate resources (CPU, memory, message queues...).	Display the system resources using the following CLI commands, • **dspconcacs** • **dspcrr** • **dspcpursc** • **dspmemrsc** • **dsprpcrsc** • **dspmsgqrsc**
	A H.248 Add TDM termination command from the CA may be rejected if the TDM termination is already associated with a (non-null) context.	The CA should attempt to clean up the orphaned TDM termination. In the event that the CA is not able to subtract the orphaned termination, the **cnfh248oos** CLI command (or SNMP equivalent) can be used to forcefully subtract ALL of the terminations (and calls) on the VXSM. This should be used as a second-to-last resort. In the event that the **cnfh248oos** CLI command won't subtract the termination, the card will need to be reset.
	The CA port has not been provisioned on the VXSM.	The CA port can be provisioned using the **addmgcgrpmgc** CLI command (or SNMP equivalent).
Echo— Echo is present in voice call.	Echo cancellation (ECAN) is either not enabled or is not configured properly.	Ensure that the ECAN feature is enabled.

Table 8-2 VXSM Troubleshooting Procedures (continued)

Problem	Possible Cause	Possible Solutions
Fail— **dspcds** command output on the PXM shows VXSM card as failed.	VXSM card is in the initial boot process.	Use the PXM45 CLI **dspcds** command in order to monitor the boot process and card bring-up. Allow time for the boot process to complete.
	VXSM boot flash or configuration file is corrupted.	Capture the output of the PXM45 **dsplog -sl** CLI command.Capture the console output. Issue the PXM45 CLI command **clrsmcnf** with the option *all* to clear the configuration for the slot. If the problem persists, contact Cisco Systems, Inc.
	VXSM slot is configured for another service module	Physically reset the VXSM card or move it to another slot. Issue the PXM45 CLI command, **clrsmcnf** with the option *all* to clear configuration for the slot.
Firmware— Firmware does not download to VXSM card.	VXSM card is not present or is not seated properly.	Make sure that the VXSM card is seated properly in the slot so that the top and bottom portions of card are making electrical contact with back plane.
	VSXM card is not in the active state or the standby state.	Verify that the VXSM card is in either the active or standby state, by issuing the PXM45 **dspcds** CLI command. Check for a card state of Boot/Init or Failed. Perform the PXM45 **dsprevs** CLI command to verify that the proper firmware image resides on the PXM. See Possible Solutions for "Active Card—VXSM card did not become active".
	VXSM card or MGX slot is defective.	Attempt to insert the VXSM card into another slot. If the problem persists, contact Cisco Systems, Inc.
LEDs— All VXSM front panel LEDs are off.	Card is not seated properly in the slot.	Make sure that the VXSM card is seated properly in the slot so that the top and bottom portions of card are making electrical contact with back plane.
Mismatch— Front card, back card mismatch.	Configuration mismatch	Use the **dspcds**, **dspcd** and **dsplog** CLI commands to identify the configuration mismatch.
Mismatch— T1/E1 mismatch.	Configuration mismatch	Issue the PXM45 **dspcds** and **dspsmcnf** CLI commands to identify a configuration mismatch. After the slot is identified, issue the PXM45 **dsplog** CLI command to show the card mismatch log entry.

Table 8-2 VXSM Troubleshooting Procedures (continued)

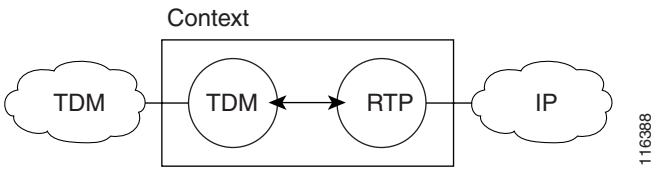
Problem	Possible Cause	Possible Solutions
Ping— Card does not respond to ping from router.	PVC connection is not established between VXSM and AXSM/RPM-XF.	Verifying that the physical connection between the AXSM and the router's ATM interface is properly connected. Verify that the LEDs for the ATM interface and the VXSM interface are green. Verify that the TX/RX cables are not crossed.
	PVC connection is in fail or alarm status.	Verify the alarm status by issuing the PXM45 **dspcons** or **dspalms** commands.
	The router's ATM interface is not configured.	From the router, issue the IOS **show atm pvc** and **show run** commands to verify that the ATM PVC status is up and that the VPI/VCI, traffic parameters and the IP address are configured properly.
	The IP address is incorrect.	From VXSM and AXSM, issue the PXM45 CLI command **dspcons** to verify that the VPI/VCI for the PVC between the VXSM and AXSM is correct. Issue the PXM45 **dspconips** CLI command and the IOS **route show** command to verify that the IP address and netmask for the PVC are correct.
	An IP address has not been provisioned corresponding to the AAL5 bearer PVC.	Issue the VXSM **addipcon** CLI command.
Resets— Card constantly reboots–becomes active and then resets again.	The MGX switch is fully loaded and the power is reaching its shut off threshold.	Issue the PXM45 **dspenvalms** and **dspndalms** CLI commands to see if the power and temperature for the shelf and the card are within acceptable limits. If the problem persists, contact Cisco Systems, Inc.
	VXSM card is getting too hot due to poor air circulation	
	The MGX fans are not functioning.	
Resets— Card resets occasionally.	Too many calls are made while a debugging command is enabled.	Minimize the number of calls when debugging is enabled, reduce the trace level in order to minimize the number of trace messages or turn off debugging altogether.
Slot— VXSM card is in place, but the **dspcds** command on the PXM shows that the slot is empty.	The pins on the back plane are bent or a power key is missing.	Remove the VXSM from the slot and observe the back panel to make sure that the pins on that slot are not bent and that the power key (the orange or yellow plastic cap in the center of the slot) exists. Insert the VXSM card into another slot. If the problem persists, contact Cisco Systems.

Obtaining Information on Current Voice Calls—H.248

With H.248, calls are modeled using a *context*. A context contains one or more terminations. In Release 5, a context can contain at most two terminations. In this release, there are two types of terminations: TDM (also referred to as SCN or Switched Circuit Network) and RTP.

A basic VoIP call leg is modeled as a context containing one TDM termination and one RTP termination.

Figure 8-1 VoIP Call Leg Model



A TDM hairpin call is modeled as a context containing two TDM terminations.

Figure 8-2 TDM Hairpin Model

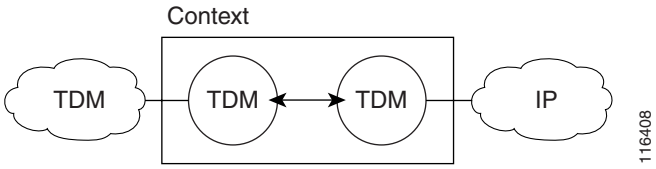


Table 8-3 lists commands for obtaining information about current voice calls on the VXSM.

Table 8-3 Displaying Current Voice Calls on the VXSM

Step	CLI Commands
1. Display all of the H.248 terminations on the VXSM card.	**dsph248calls <GatewayLinkId>**
2. Display the status of all the H.248 contexts on the VXSM card.	**dsph248status -cntxs**
3. Display the status of a particular H.248 context on the VXSM card.	**dsph248status -cntx <context ID>**
4. Display the status of a particular H.248 TDM/SCN termination on the VXSM card.	**dsph248status -term 1 1 <term_id>** **dsph248status -term 1 2 <term_name>** **dsph248status -term 1 3 <oc3> <ds1> <ds0>**
5. Display the status of a particular H.248 RTP termination on the VXSM card.	**dsph248status -term 3 1 <term_id>** **dsph248status -term 3 2 <term_name>**

Table 8-3 Displaying Current Voice Calls on the VXSM (continued)

Step	CLI Commands
6. Display information pertaining to all of the H.248 associations on the VXSM card.	**dsph248status -assoc**
7. Display information pertaining to a particular H.248 termination on the VXSM card.	**dsph248call -term**
8. Display counters corresponding to all of the H.248 physical (TDM/SCN) terminations on the VXSM card.	**dsph248cnts -phyterm**
9. Display H.248 command counters.	**dsph248cnt -cmd <association>**
10. Display counters pertaining to a particular H.248 physical (TDM/SCN) termination on the VXSM card.	**dsph248cnt -phyterm 1 <bay.line.path.vtg/ds3.vt/ds1:ds0>**
11. Display information regarding all of the H.248 contexts.	**dsph248cnt -cntx <association>**
12. Display counters pertaining to all H.248 ephemeral (RTP..) terminations on the VXSM card.	**dsph248cnt -ephterm**
13. Display counters pertaining to a particular H.248 association.	**dsph248cnt -assoc <association>**

Examples

The **dsph248calls** CLI command displays all of the H.248 terminations.

```
shelf.1.VXSM.a > dsph248calls

  TermId     TermType       Media       Codec          Vad         Ecan
  ------     --------      --------     -----         -----        ----
     1         SCN          'Voice'    'G.711 U'      -----       'Enabled'
  8067         RTP          'Voice'    'G.711 U'    'Enabled'     -----
     2         SCN          'Voice'    'G.711 U'      -----       'Enabled'
  8068         RTP          'Voice'    'G.711 U'    'Enabled'     -----
```

The **dsph248status -cntxs** CLI command displays the status of all H.248 contexts.

```
shelf.1.VXSM.a > dsph248status -cntxs
=====================================
     Status for all contexts
=====================================
Number of active contexts:2
List of contexts
Status of context 4:
       Creation date and time:02/03/2004, 17:31:21
       Number of terminations in context:2
       List of termination IDs:
              8068  2
Status of context 3:
       Creation date and time:02/03/2004, 17:31:21
       Number of terminations in context:2
       List of termination IDs:
              8067  1
```

The **dsph248status -cntx** CLI command displays the status of a particular H.248 context.

```
shelf.1.VXSM.a > dsph248status -cntx 1
=====================================
      Status of context 1
=====================================
Creation date and time: 07/04/2003, 13:55:45
Number of terminations in context: 2
List of terminations:
        term_id: 8065, term_type: MG_TERM_TYPE_PDN_IP, term_name: RTP8065
        term_id: 3, term_type: MG_TERM_TYPE_SCN, term_name: ds/1/1/3
```

The **dsph248status -term** CLI command displays the status of a particular H.248 termination.

```
shelf.1.VXSM.a > dsph248status -term 1 1 1
=========================================
 Status of termination with ID 1
=========================================
Termination type:MG_TERM_TYPE_SCN
Termination name:ds/1/1/1
Termination state:MG_TERM_STATE_INSERVICE
Termination test flag:False
Termination context id:3
Id of profile on termination:0
Number of streams on termination:1
Termination about to be deleted:False
Next state of termination:MG_NEXT_STATE_INSERVICE
Last modified/updated:02/03/2004, 17:31:21
NOTE:This timestamp is not preserved across switchovers.
It is independently generated on each card.
Supported packages:
H248_GENERIC_PKG H248_TDMC_PKG
```

The **dsph248call -term** CLI command displays information pertaining to a particular H.248 terminations:

shelf.1.VXSM.a > dsph248call -term 1

```
    Term Id              :1
    Term Type            :SCN

    Term Name            :ds/1/1/1
    connMode             :4 ('Send-recv')
    loopBackType         :1 ('None')

    RTP Encapsulation Parameters ...

    ssrc                 :424285698 (0x194a1602)
    RTCP Enable          :TRUE
    dspCodec             :2 ('G.711 U')
    packetPeriod         :'20 ms'

    vadMode              :2 ('Enabled')
    vadThreshold         :-38
    vadHangoverTime      :250 ms

    ecan enabled         :'Enabled'
    ecanTail             :128 ms
    ecanFlags            :0x0

Type <CR> to continue, Q<CR> to stop:
    upspeedCodec         :2 ('G.711 U')
    jitterMode           :2 ('Adaptive')
    jitterMinDelay       :5 ms
    jitterMaxDelay       :100 ms
    jitterNomDelay       :30 ms
    jitterFaxNomDelay    :0 ms

    txGain               :0
    rxGain               :0

    nsePayloadType       :100 (0x64)
    nteTxPayloadType     :0 (0x0)
    nteRxPayloadType     :0 (0x0)
    profileType          :0
    profileNum           :0

    hsRedCount           :0
    lsRedCount           :0

    toneDetect           :0x3c32
    toneDetectBitmap     :0x0

Type <CR> to continue, Q<CR> to stop:
    digitDetect          :1 ('DTMF')
    digitRelayMethod     :1 ('Send as Voice')

    icsEnable            :0 (FALSE)
```

```
    nx64FramePattern     :0 (CRML_PATTERN_NONE)

    trunkMode            :0 (CRML_MODE_NONE)

    nx64FrameFlagCnt     :0

    dtmfTransport        :0 (FALSE)

    trunkCond            :0 (FALSE)
```

The **dsph248cnts -phyterm** CLI command displays counters corresponding to all of the H.248 physical (TDM/SCN) terminations on the VXSM card:

```
shelf.1.VXSM.a > dsph248cnts -phyterm
================================================================
         All Gateway Physical Terminations Statistic

  DS1:DS0      Termination  Termination   Num of  Num of   Num of OOS  Num of OOS
    line         Id           Name         Add    Failure  from MGC    from OAM
============  ===========  ============  ======  =======  ==========
1.1.1.2.3:1   361          DS/1/16/1     1       0        0           0
1.1.1.2.3:2   362          DS/1/16/2     0       0        0           0
…...
1.1.1.2.3:23  383          DS/1/16/23    0       0        0           0
1.1.1.2.3:24  384          DS/1/16/24    1       0        0           0
```

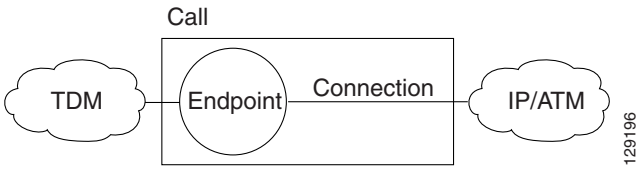
The **dsph248cnt -ephterm** CLI command displays counters corresponding to all of the H.248 ephemeral (such as RTP) terminations on the VXSM card:

```
shelf.1.VXSM.a > dsph248cnt -ephterm
=========================================================
        Gateway Ephemeral Terminations Statistic
=========================================================
Num of Add Commands      :              2
Num of Commands Failure  :              0
```

Obtaining Information on Current Voice Calls—xGCP

The Current Voice xGCP call (xGCP) model is based upon endpoints and connections. Connections have modes. Supported modes include Receive-Only, Send/Receive, Inactive, Loopback, and Continuity Test. The connection model is shown in Figure 8-3.

Figure 8-3 xGCP Connection Model



To obtain information regarding the status of TGCP activities. Use the PXM and VXSM commands as follows. The PXM CLI commands in Table 8-4 display the list of events and errors logged by the active and standby VXSM cards, starting with the most recent event or error.

Table 8-4 PXM CLI Commands for Troubleshooting VXSM

Command	Displays
dsperr –sl <primary slot>	Error for a primary VXSM.
dsperr –sl <secondary slot>	Error for a secondary VXSM.
dsplog –sl <primary slot>	Log for a primary VXSM.
dsplog –sl <secondary slot>	Log for a secondary VXSM.

Use the VXSM CLI commands in Table 8-5 to monitor the basic operation of the currently-active VXSM card and to check if calls are being processed after switchover:

Table 8-5 VXSM CLI Commands for Troubleshooting VXSM

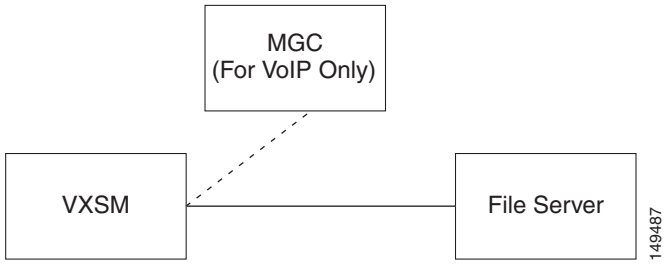
Command	Description
dspxgcpcnts	Displays xgcp command counts
dspxgcpdetailcnts	Displays xgcp details
dspxgcpendpts	Displays xgcp endpoints
dspxgcpendptcons	Dispaly xgcp endpoint connections

- **dspxgcpcnts**—Displays a static summary of the number of TGCP commands that failed/succeeded on the ACTV card at that moment; executing this command a few times will give the user an idea whether commands are being sent to the VXSM and whether VXSM is processing those commands.
- **dspxgcpdetailcnts**—Displays number of times a TGCP command is received/sent/retransmitted.
- **dspxgcpendpts** <endpt-name>—Displays all the endpt state if connection is present on that endpoint.
- **dspxgcpendpts** *—Can be used to display all.
- -**dspxgcpendptcons** <endpt-name>—Displays the connection ID. Call ID of the connection on that endpoint.

Bearer Tracing Feature

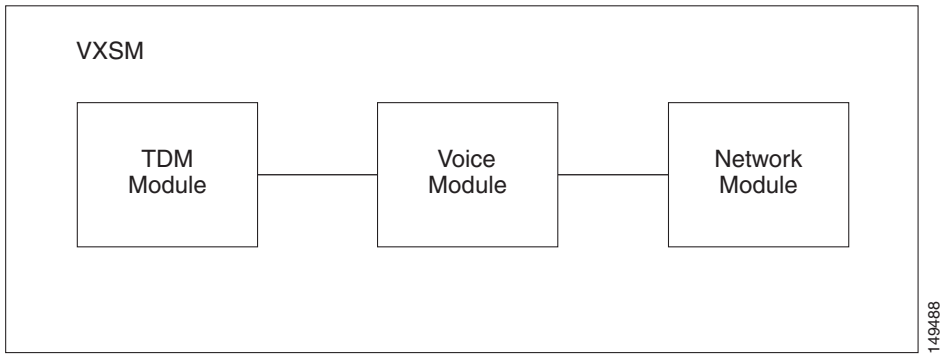
The VXSM card includes a useful troubleshooting tool that has the ability to collect fundamental information about the content of bearer streams and to transmit the information in real-time to an external file server for offline analysis. This feature, known as Bearer Tracing, involves the VXSM card, the Media Gateway Controller for VoIP applications, and a file server to receive the bearer traces (Figure 8-4).

Figure 8-4 Bearer Tracing Major Elements



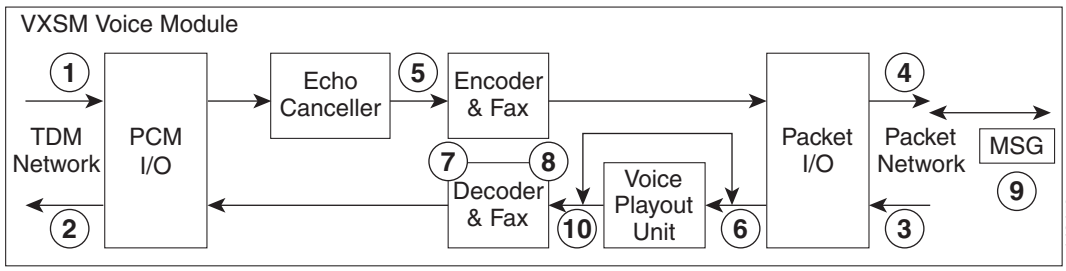
Within the VXSM card, the Bearer Tracing feature is performed in the voice module (Figure 8-5).

Figure 8-5 VXSM Bearer Tracing High-Level Function



The Voice Module contains a number of probes on the card that are situated at various points in the path of the bearer stream through the card. There are 10 probes (Figure 8-6).

Figure 8-6 Bearer Trace Probe Locations



Note The numbering used to identify the probes in the diagram above is the same numbering that the VXSM Bearer Tracing command use to identify the probes.

The probes are:

1 = PCM Input from TDM network

2 = PCM Output to the TDM network

3 = Input from the packet network

4 = Output to the packet network

5 = Output from echo canceller (Ecan/Sout)

6 = Voice Playout Unit - Jitter buffer events

7 = T.38 information at the Decoder—level 1

8 = T.38 information at the Decoder—level 2

9 = DIM Message Trace to and from DSP

10 = Voice Playout Unit—segments

Bearer Trace Operation

Step 1 To be able to collect bearer traces on a endpoint, VXSM must:

a. Have an active bearer channel

In VoIP—A call must be set up
or

In AAL2—An AAL2 nailed up connection must be added by adding a CID

And

b. Be connected to a computer where the trace files are to be stored (referred to as a file server, server, or network).

Note If a call agent is used, the same machine can be a call agent and a file server at the same time.

Step 2 To start collecting bearer traces:

a. If bearer tracing is set up and activated on an endpoint that has an active bearer channel, tracing starts immediately, otherwise, it starts as soon as a call (VoIP) or a connection (AAL2) is activated on the endpoint.

b. If bearer tracing is set up and *not* activated on an endpoint, tracing must be initiated manually even if there is an active call/connection on the endpoint.

Step 3 To stop collecting bearer traces:

a. End the active call/connection on the endpoint, or

b. Manually stop the trace

Note As long as the trace is not stopped, VXSM continues to send trace samples to the file server

Step 4 VXSM generates a trace filename each time a trace is started and active on an endpoint. The filename is based on the probe type, the endpoint index and on specific user input that constitutes the file signature.

Note The file signature could be set to remain the same from one trace session to another or, in some cases; it could be set to be specific to each session (see Trace Files, page 8-24).

If the connection to the file server cannot be established, bearer tracing is deactivated automatically. To reactivate bearer tracing:

a. Fix the network issues that prevent the network connection to be established.

And

b. Restart the call on the endpoint, or stop then start the trace manually.

Step 5 All trace probes can be activated on the same endpoint. Each probe initiates its own trace stream to the network and writes its data to its own file except for VPU traces where VPU event traces and VPU segment traces are written to the same file.

Step 6 The level 1 and level 2 T.38 probes (7 and 8) cannot be activated at the same time. These probes also need PCM trace to be on.

Step 7 The total number of probes activated at the same time is limited, but the amount of data transferred per probe is not limited.

Note a. Ensure that there is enough free space on the file server to store the trace files generated by VXSM. For an estimation of the required space per trace, see the "Per Trace Bandwidth and File Size Requirements" section on page 8-17.

b. If the network connection experiences problems while bearer tracing is writing trace data into the trace file, bearer tracing may be deactivated automatically. To reactivate bearer tracing:

1. Fix the network issues that are preventing the network connection to be established
2. Restart the call on the endpoint or stop then start the trace manually

Bearer Trace Types

Bearer Traces are transmitted to the server as files with file names that indicate the probe type, the endpoint being probed and, optionally, a timestamp. Files are assigned names by the Bearer Tracing feature that indicate these items. For more details on file naming see Trace Files, page 8-24.

PCM Traces

There are 2 PCM traces, pcmin and pcmout, to and from the voice network, respectively. In CLI, pcmin Probe 1 collects pcmin and probe 2 collects pcmout. The pcmin trace files generated by VXSM have the pcmin prefix and.pcm suffix, pcmout trace file have the pcmout prefix and the .pcm suffix.

The format for a PCM trace is either 8-bit PCM A-law or 8-bit PCM mu-law, depending on the physical interface being used. VXSM currently ties the PCM encoding to the physical interface.

Echo Canceller Traces—Sout

A sout trace is collected from the output of the echo canceller and is collected by probe 5.

The format of the sout stream is a big-endian signed 16-bit linear format. The value 32757 represents full scale. The sout trace file generated by VXSM has the sout prefix and .pcm suffix

The sout stream is synchronized to the PCM In and PCM Out signals.

The sout tracing cannot be enabled if the Ecan is not enabled on the given connection

Packet Traces

The packet traces are collected at the input and output of the packet IO interface.

The current implementation focuses on RTP traces. The packet trace is in raw IP pcap format that is readable by packet sniffers such as Ethereal.

Voice Playout Unit Traces

There are two type of voice playout unit (VPU) traces:

- VPU event on probe 6—VPU Event trace (vpevt) reports jitter-related events when they happen.
- VPU segment on probe 10—The Voice Playout Unit (jitter buffer) segment trace (vpseg) reports jitter-related data every segment (that is, every 5 ms).

Although there are 2 types of VPU traces, only one file is created on the server for both traces. The vpu file generated by VXSM has the vpu prefix and the vpu suffix.

T.38 Traces

When a fax call is active using T.38 fax relay, traces can be gathered from the Fax module within the DSP. The user can select to gather 2 levels of traces:

- Level 1—Basic events to decipher T.30 and other signaling progress
- Level 2—Proprietary Telogy format

When enabling the tracing functionality for T.38 the user can chose to monitor any DS0 in a DS1 or a specific DS0 in a DS1. When monitoring any DS0 in a DS1 the first fax relay session activated on the monitored span will have tracing enabled. User can choose to monitor any DS0 in a DS1 by choosing a special DS0 attribute in the **addbearertraceendpt** CLI.

A total of 10 simultaneous DS0 can be monitored at any one time. In addition to this, a maximum number of 10 trace sessions can be activated simultaneously.

The file containing the T38 traces will have a header that provides some information about the fax relay session. It contains ds1 and ds0 information, tcid/dsp information, and the timestamp indicating when the file was created.

In CLI, the T38 level l trace 1is activated by probe 8 and T38 level 2 trace is activated by probe 7.

The file created on the server for T38 level 1 trace has the suffix DBG1.

The file created on the server for T38 level 2 trace has the suffix DBG2.

Both level 1 and level 2 traces have the prefix FaxRelayTrace.

After the filename base is entered by the user, the filename is also appended to the endpoint prefix, followed by the DS0 number.

For example, in the case of ftp where the timestamp is used as a filename base, the filename for a level 1 trace on endpoint 2 ds0 1 is: FaxRelayTrace_022306172604_2_1.DBG1. See Table 8-9 for details.

MSG Traces

Probe 9 collects MSG traces. The message trace file generated by VXSM has the msg prefix and the msg suffix.

Message traces contain the information within DIM traces. MSG Traces are asynchronous and depend on whether or not the activity on the card generates DIM traces.

Bearer Tracing Connectivity

External Interface

VXSM can be connected to the file server either through the control PVC or through the VXSM Ethernet port.

If the control PVC is used, the provisioning of the control PCV needs to include the bandwidth required for the transfer of trace data to the network.

Per Trace Bandwidth and File Size Requirements

Bearer tracing requires that enough bandwidth be available to accommodate the bearer trace traffic data and the transport protocol packet and control overhead. Table 8-6 and Table 8-7 below show the estimate per-trace bandwidth requirements in the case of ftp and tftp. The file size of the accumulated bearer trace data on the server is also provided so that enough space is set aside for the trace files to be stored in the ftp server. The file size of the trace files is limited only by the free space on the file server. To make sure that trace files have no loss of data, provide enough space on the file server for the trace files.

Table 8-6 FTP Bandwidth and File Sizes

Probe Type	AAL5 Bandwidth per Trace in cells/s	Ethernet Bandwith in Bytes/s	File Size for 5 min of tracing in Bytes
PCM in, PCM out, Sout	200	9000	2400000
Pkt in, Pkt out	250	11000	3600000
VPU segment	100	3000	920000
Sout	400	18000	4800000

Table 8-7 FTP Bandwidth and File Sizes

Probe Type	AAL5 Bandwidth per Trace in cells/s	Ethernet Bandwith in Bytes/s	File Size for 5 min of tracing in Bytes
PCM in, PCM out, Sout	210	9500	2400000
VPU Segment	90	4300	920000
Sout	420	19000	4800000

Bearer Tracing for AAL2 Connections

FTP and TFTP protocols run on an IP network. For Voice over IP, VXSM inherently uses an AAL5 control PVC to communicate with the MGC. The same control PVC can be used to communicate with the external FTP/TFTP server.

Control PVC is not inherent in an AAL2 configuration (for example, AAL2 trunking). To access the IP cloud in such a situation, either a control PVC or the Ethernet console need to be configured. Unless pinging the file server is possible, tracing does not operate.

IPSec and Bearer Tracing

The Bearer Tracing mechanism uses FTP/TFTP connections to transfer the traces to the server. The trace data are carried over the control PVC, which is also used to communicate with MGC. For many solutions, IPSec is used to secure the communication with the MGC over control PVC. In such cases, the FTP/TFTP traffic is bypassed by IPSec to transfer trace data to the bearer tracing server.

Bearer Trace CLI Requirements

Persistency

The operational state of bearer tracing is not saved in disk database. Hence, all the information is lost if the card resets. All the bearer tracing commands are non-MIB commands.

Backward Compatibility

Commands introduced in the PCM tracing functionality in the earlier VXSM releases are no longer functional. They are replaced by the new bearer tracing commands in VXSM Release 5.3.

Bearer Trace Configuration

After a bearer trace or a server profile is added, the only way to change its configuration is by deleting the trace or the server profile and adding it again with the new configuration.

Note For bearer tracing to occur, there must be a connection between VXSM and the file server. An ftp/tftp server need to be running on the file server and access permission to the directory (and in the case of tftp, to the files) must be granted.

Note Before you delete either configuration, make sure that the trace is stopped.

Considerations and Limitations

1. A VXSM card supports up to 32 simultaneous trace sessions.
2. A VXSM card supports the following max number of traces per probe type (Table 8-8):

Table 8-8 Trace Limitations

Probe Type	Maximum Number of Traces
Pcmin	5
Pcmout	5
Pkt in	5
Pkt out	5
Ecan/Sout	5
VPU	5
MSG	2

3. Only one trace per DSP core is possible, consequently, adding tracing on an endpoint will fail if the dsp core is found to have tracing enabled for a different endpoint.
4. Network latencies beyond 20 seconds have an impact on the quality of traces. To avoid loss of data during the trace collection, have the file server on the same LAN segment as VXSM.
5. Bearer tracing requires about 1 percent of CPU use. For tracing to operate properly, only enable the number of traces that the system CPU use can manage. Also, under a heavy call-rate, there might not be enough CPU bandwidth to accommodate the maximum number of traces.
6. In Packet Trace, to capture events such as DTMF or Tones in a trace file, stop bearer tracing before using the trace file in an offline processing.
7. ftp sessions time out after 30 seconds of inactivity so that dead network connections do not affect the system adversely.
8. All traces must be set up at the same time as there is no provision to set up each one individually.
9. We recommend that bearer traces and T.38 traces are run separately.

Configuring the Bearer Tracing Feature

Configuration Summary

The following steps provide a quick summary of the procedure for configuring the Bearer Tracing feature.

Step 1 In a typical network scenario, identify the ds0 that needs to be monitored for bearer trace collection. Use **addbearertraceendpt** to define the endpoint and the trace probes that need to be enabled.

Step 2 Use **addbearertracesrvprof** to add TFTP or FTP server profile.

Step 3 Use **addbearertrace** to tie the endpoint to the defined server profile.

Step 4 Make sure that the necessary files are created on the server with correct write permissions if TFTP transfer mode is to be used.

Step 5 Use **bearertracestart** to enable the tracing on the given endpoint if it is not already enabled using addbearertrace or simply start a call on the endpoint

Step 6 Use **bearertracestop** to stop the tracing on the given endpoint, or simply stop the call in a VOIP configuration or delete the connection in an AAL2 configuration

Detailed Configuration

To set up bearer tracing, use the following procedure.

Step 1 Set up a connection to an external server to receive the trace information. See Bearer Tracing Connectivity, page 8-17 for connectivity details

Step 2 Use the **addbearertraceendpt** command create the TDM segment of a bearer trace session.

This command is used to create a session with a specified DS0 or DS1 endpoint for bearer tracing. See T.38 Traces, page 8-16 for T.38 endpoints.

The format of this command is:

addbearertraceendpt <endptIndex> <LineNum> <ds0> **-trace** <probe>

For <endptIndex> enter a number in the range 1 to 32. This parameter uniquely identifies the bearer trace session.

For <LineNum>, enter line number of the endpoint in one of the following formats.

Interface Type	Line Number Format	Values
OC3/SDH	bay.line.path.vtg.vt or bay.line.path.ds1	bay {1 - upper} line (range=1..4) path (range=1..3) vtg (range=1..7) vt (range=1..4)(ds1) (range=1..3)(e1) ds1 (range=1..28)
T1/E1	bay.line	bay {1 - upper} line (range=1..24)
T3	bay.line.ds1	bay {1 - upper} line (range=1..6) ds1 (range=1..28)

For <ds0>, enter:

A number in the range 1 to 24 or all for a T1 interface.

A number in the range 1 to 32 or all for an E1 interface.

For **-trace**<probe>, enter the probe number(s) to be used in the session. Enter either a single number or multiple numbers, for example, 1,3,5,7)

1 = PCM Input
2 = PCM Output
4 = Network Input
5 = Network Output
3 = Sout (echo canceller output)
6 = VPU - Events
7 = T38 Level 2
8 = T38 Level 1
9 = Message Events
10 = VPU - Segments

Note The line number all option can be used only when one of the probes 7 and 8 is chosen.

To verify the creation of the session, use the **dspbearertraceendpt** command. The format of this command is:

dspbearertraceendpt <endptIndex>

Step 3 Use the **addbearertracesrvprof** command to create the network segment of a bearer trace session.

The syntax of this command is:

addbearertracesrvprof <profIndex> <srvIP> <xferMode> <fileNameBase>[<uploadPath> <portNumber/login><password>]

For <profIndex>, enter a number in the range 1 to 10. This parameter uniquely identifies the bearer trace server profile.

For <srvIP>, enter the IP address of the server to receive the bearer trace reports. The IP address can be provided using either IP dot-notation (nnn.nnn.nnn.nnn) or a name (alpha.beta.com) with a proper DNS support.

For <xferMode>, specify the transfer mode for communicating with the server. Enter **0** for FTP, or **1** for TFTP.

For <fileNameBase>, specify a fileNameBase. For FTP, the user can also enter **#** to indicate the default fileNameBase is to be used (default is not allowed for TFTP).

VXSM generates filenames as follows (Table 8-9):

Table 8-9 Generated Bearer Trace Filenames

xferMode	fileNameBase	Filenames
1 = TFTP	FILENAMEBASE specified by user	PCM In - pcminFILENAMEBASE_EndPtID.pcm PCM Out - pcmoutFILENAMEBASE_ EndPtID.pcm Sout - soutFILENAMEBASE_ EndPtID.pcm VPU - vpuFILENAMEBASE_ EndPtID.vpu Network In - netwrxFILENAMEBASE_ EndPtID.pkt Network Out - netwtxFILENAMEBASE_ EndPtID.pkt T.38 level 1 - FaxRelayTrace_FILENAMEBASE_EndPtID_DS0.DBG1 T.38 level 2 - FaxRelayTrace_FILENAMEBASE_EndPtID_DS0.DBG2 MSG - msgFILENAMEBASE_EndPtID.msg (to and from DSP)
1 = TFTP	# for default	Not allowed
2 = FTP	FILENAMEBASE specified by user	PCM In - pcminFILENAMEBASE_EndPtID.pcm PCM Out - pcmoutFILENAMEBASE_ EndPtID.pcm Sout - soutFILENAMEBASE_ EndPtID.pcm VPU - vpuFILENAMEBASE_ EndPtID.vpu Network In - netwrxFILENAMEBASE_ EndPtID.pkt Network Out - netwtxFILENAMEBASE_ EndPtID.pkt T.38 level 1 - FaxRelayTrace_FILENAMEBASE_EndPtID_DS0.DBG1 T.38 level 2 - FaxRelayTrace_FILENAMEBASE_EndPtID_DS0.DBG2 MSG - msgFILENAMEBASE_EndPtID.msg (to and from DSP)
2 = FTP	# for default	PCM In - pcminMMDDYYHHMMSS_EndPtID.pcm PCM Out - pcmoutMMDDYYHHMMSS_ EndPtID.pcm Sout - soutMMDDYYHHMMSS_ EndPtID.pcm VPU - vpuMMDDYYHHMMSS_ EndPtID.vpu Network In - netwrxMMDDYYHHMMSS_ EndPtID.pkt Network Out - netwtxMMDDYYHHMMSS_ EndPtID.pkt T.38 level 1 - FaxRelayTrace_MMDDYYHHMMSS_EndPtID_DS0.DBG1 T.38 level 2 - FaxRelayTrace_MMDDYYHHMMSS_EndPtID_DS0.DBG2 MSG - msgMMDDYYHHMMSS_EndPtID.msg (to and from DSP)

For <uploadPath>, specify the path of the file in the server. For example. /pcm/tes

Note The server root directory is used if the path is not specified.

For <portNumber/login>, enter a TFTP port number if xferMode = 1 or the FTP login name If xferMode = 0.

The TFTP port number is a number in the range 1 to 255 with a default of 69.

For login, use the FTP login name, default is guest.

For <password>, use the FTP password, default is guest.

The creation of the profile can be verified by using the **dspbearertracesrvprof** command. The format of this command is:

dspbearertracesrvprof <profIndex>

Step 4 Use the **addbearertrace** command to link the TDM segment and the network segment of the bearer trace session. Optionally, this command can also start the bearer trace function.

The format of the **addbearertrace** command is:

addbearertrace <endptIndex> <profIndex> <active>

For <endptIndex>, enter the endpoint index number of the bearer trace session. A number in the range of 1 to 32.

For <profIndex>, enter the profile number of the bearer trace profile. A number in the range of 1 to10.

For <active>, specify 1 for enable or 0 for disable. If this parameter is omitted, the default is enable.

Note If the bearer tracing is enabled, tracing starts automatically whenever a call is added on the given bearer endpoint. If the bearer tracing is not enabled, then it must be explicitly started using the **bearertracestart** command (see also the corresponding **bearertracestop** command).

The creation of the association can be verified by using the **dspbearertrace** command. The format of this command is:

dspbearertrace<endptIndex>

Bearer Trace Configuration Examples

Example 1

This sample procedure sets up the bearer tracing endpoint, the ftp/tftp server, and a method of mapping them to each other before making and tracing a call. The call is on ds0=1 on ds1=1. Configure the bearer tracing endpoint and the servers:

Step 1 Configure the bearer trace endpoint with appropriate trace probes.

martler.2.VXSM.a > addbearertraceendpt 1 1.1.1.1.1 1 -trace 1,2,5

Step 2 Configure the bearer trace server with appropriate parameters.

martler.2.VXSM.a > addbearertracesrvprof 1 172.17.38.159 0 sarang/root password

Step 3 Map the bearer trace endpoint using the bearer trace server.

martler.2.VXSM.a > addbearertrace 1 1 1

Step 4 Verify that the mapping is successful.

martler.2.VXSM.a > dspbearertraceendpts

```
==========================================
         BEARER TRACE ENDPT PROFILES
==========================================

   Index                  : 1
   line                   : 1.1.1.1.1
   lineNo                 : 1
   ds0No                  : 1
   bearerTraceSrvProf     : 0x1   <--Server Profile is added
   bearerTraceProbes      : 0x13
```

Step 5 Verify that the parameters for bearer trace server are correct.

martler.2.VXSM.a > dspbearertracesrvprofs

```
==========================================
         BEARER TRACE SERVER PROFILES
==========================================

Server Profile Index            : 1
Bearer Trace Server IP          : 172.17.38.159
Server upload directory         : /
TFTP/FTP Mode                   : FTP
File Name Base                  : sarang
FTP server login                : root
FTP server password             : password
------------------------------------------
```

Step 6 Place a call on ds0=1 and ds1=1, and then delete it after some time. On the FTP server the following files are created.

```
-rw-r--r--   1 root     other     690480 Oct 16 12:17 pcminsarang_1.pcm
-rw-r--r--   1 root     other     690480 Oct 16 12:17 pcmoutsarang_1.pcm
-rw-r--r--   1 root     other    1380960 Oct 16 12:17 soutsarang_1.pcm
```

Example 2

The following example shows how to collect PCM traces for a call with both endpoints on the same card:

Step 1 Configure the bearer tracing endpoint for PCMin and PCMout traces.

addbearertraceendpt 1 1.1.1.1.1 1 -trace 1,2

addbearertraceendpt 2 1.1.1.1.1 2 -trace 1,2

Step 2 Add a Bearer Trace File Server.

addbearertracesrvprof 1 172.17.38.159 0 rxie /tftpboot root password

Step 3 Map the bearer endpt to the server profile.

addbearertrace 1 1 1

addbearertrace 2 1 1

When you make a call on endpoints 1 and 2, the PCM tracing starts automatically because of the last parameter in the **addbearertrace** command above.

However, If you use a different last parameter as in the following commands,

addbearertrace 1 1 0

addbearertrace 2 1 0

Tracing does not start automatically and the following commands are needed to start the tracing after the call is up:

bearertracestart 1

bearertracestart 2

Step 4 To stop bearer tracing at any time, use the following CLIs:

bearertracestop 1

bearertracestop 2

Trace Files

Server File Requirements

1. Before you enable bearer tracing, files corresponding to the trace files that will be generated by VXSM need to be created on the file server.
2. Write access to both the created traces files and to the directory where they reside must be set.
3. If a directory is specified when adding a server profile on VXSM, this directory is relative to the default tftp directory specified in the tftp config file (in UNIX, the default is set to /tftpboot in /etc/inet.conf.

FileNames

Bearer trace information is saved to the server as data chunks that will be stored in a file of which the name is generated by VXSM. The file naming scheme is slightly different depending upon whether TFTP or FTP are used as the transport protocol.

TFTP Filenames

Filenames used with TFTP consist of the following parts:

- A probe type
- A FILENAMEBASE
- The endpoint index being probed
- A file extension

For example, a trace for PCM In on a bearer trace endpoint of index 1 and with a Filename Base Mytrace yields a filename of:

pcminMytrace_1.pcm

Before enabling the bearer trace function, filenames corresponding to trace files must be created on the server. Further, VXSM must have write access to the trace files and the directory in which they reside. The path to the file is relative to the default tftp directory (usually set as /tftpboot).

Note When using the FILENAMEBASE, subsequent traces for the same probe and same endpoint overwrite the previous file in the server. It is the responsibility of the server to take action to prevent this occurrence.

FTP Filenames

For systems using FTP, the use of a FILENAMEBASE is optional. If a FILENAMEBASE is specified, the same file naming scheme used for TFTP is used (see previous paragraphs). If a FILENAMEBASE is not specified, VXSM generates a filename having the following parts:

- A probe type
- A timestamp MMDDYYHHMMSS based upon a 24-hour clock)
- The endpoint index being probed
- A file extension

For example, a trace for PCM In on a bearer trace endpoint of index 1 yields a filename of:

pcmin111205104520_1.pcm

Note The filename method using timestamps automatically prevents the overwriting of previous trace files.

Note Make sure there is enough space on the server to store all the different trace files for the same probe. The files can get very large if tracing is on for a long time.

Troubleshooting a Bearer Trace Operation

A number of issues can cause the trace to lose samples. When tracing is enabled on an endpoint, always check the trace error counters on both the motherboard and the daughter card to track the status of the trace stream.

The commands to use are:

- btresetstats—Reset motherboard bearer trace stats
- dcbtresetstats—Reset daughter card bearer trace stats
- dspbtstats—Display motherboard bearer trace stats
- dspdcbtpktstats—Display daughter card bearer trace packet stats
- dspdcbtstats—Display daughter card bearer trace stats

In the bearer tracing infrastructure, the user needs to define the bearer tracing endpoints (ds0) on which bearer traces are to be collected. The user needs to define bearer trace server where the bearer traces will be stored using FTP or TFTP. Any given bearer trace endpoint needs to be mapped to a bearer trace server, so that the bearer traces for that endpoint are stored at the mapped bearer trace server. The user can specify which directory the bearer traces can be stored and the base for the file names in which the traces are to be stored.

The user must make sure the following conditions exist:

1. The bearer trace server can be pinged from the VXSM card.
2. The VXSM control PVC IP address can be pinged from the bearer trace server.
3. If there is no control PVC (example: AAL2 trunking), the Ethernet console connection should be used. In any case, step 1 should pass.
4. The bearer trace server supports FTP and TFTP protocol.
5. In case of TFTP protocol, appropriate files are created with proper rwx permissions.
6. If the bearer trace transfer takes place through control PVC, the control PVC should have sufficient bandwidth allocated (Table 8-10).

Table 8-10 Bearer Trace Troubleshooting

Problem	Possible Cause	Potential Solution
Cannot add tracing on an endpoint	Tracing already enabled on the same DSP	Remove existing trace or enable tracing on a different endpoint
Cannot enabled a fax trace	Max number of fax session exceeded	Remove an existing trace before adding a new one
Trace files do not increase in size	Tracing might have been turned off because of network issues	Check your network connection and restart the tracing

Bearer Trace Command Summary

The commands for the Bearer Trace feature are listed below. For detailed descriptions of these commands, refer to the *Cisco Voice Switch Services (VXSM) Configuration Guide for MGX Switches and Media Gateways, Release 5.3*.

- **addbearertraceendpt** <*endptIndex*> <*LineNum*> <*ds0*> -trace <*probe*>
- **addbearertracesrvprof** <*profIndex*> <*srvIP*> <*xferMode*> <*fileNameBase*>[<*uploadPath*> <*portNumber/login*><*password*>]
- **bearertracestart** <*endptIndex*>
- **bearertracestop** <*endptIndex*>
- **delbearertrace** <*endptIndex*>
- **delbearertraceendpt** <*endptIndex*>
- **delbearertracesrvprof** <*profIndex*>
- **dspbearertraceendpt** <*endptIndex*>
- **dspbearertraceendpts**
- **dspbearertracesrvprof** <*profIndex*>
- **dspbearertracesrvprofs**
- **btresetstats** <*endptID*><*probe*>
- **dcbtresetstats** <*endptID*><*probe*>
- **dspbtstats** <*endptID*><*probe*>
- **dspdcbtstats** <*endptID*><*probe*>

- **dspdcbtpktstats** <*endptID*><*probe*>

Troubleshooting Commands

Table 8-11 lists CLI commands for troubleshooting the VXSM.

Table 8-11 Troubleshooting VXSM—Commands

Command	Description
dspcputhreshold	Displays data about the current CPU use.
dsplog	Displays the log file that lists the current errors on the switch.
dsperr	Displays the error for a specific slot.
addlnloop	Enables a local line loopback.
dellnloop	Disables a local line loopback.
cnfbert	Configures a bit error rate test.
addconloop	Enables a VC remote loopback.
delconloop	Disables a VC remote loopback.

Media Gateway Clocking

Clocking Basics

Network clocking is a means by which a clock signal is generated or derived and distributed through a node for the purpose of insuring synchronized network operation. Clocking and its configuration is at the gateway (or node) level. As such the clocking functions in an MGX 8850 media gateway reside in the PXM 45 card.

The MGX 8850 supports the following types of internal and external clock sources.

- A BITS (Building Internal Timing Source) clock. This type is an external clock source connected to one of two RJ-48 type female connectors on the PXM-UI-S3 back card (see Figure A-1).
- A SETS (Synchronous Equipment Timing Source) clock. This type is an external clock source connected to one of two RJ-48 type female connectors on the PXM-UI-S3 back card (see Figure A-1).
- An external clock source derived from a service module line (for example, a VXSM line).
- An internal clock source consisting of a Stratum 3 clock circuit in the internal clock oscillator on the PXM back card - PXM-UI-S3.This clock source is distributed to all cards in the gateway.

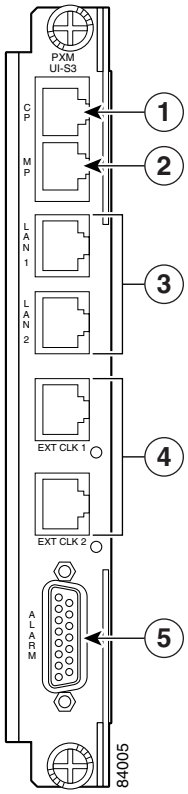
If possible, the recommended clock source for a VXSM based MGX 8850 media gateway is BITS.

Note The two RJ-48 connectors for clock input are indicated as “4” in Figure A-1. One is labeled EXT CLK 1 and the other as EXT CLK 2. Each connector has an associated LED which is lit green when the clock source is active. If the LED is not lit, the clock source is either inactive or not in use.

From the above list of possible clock source types, the gateway can accept two clock sources. One source is designated as primary and is mandatory, the second source is designated a secondary and is optional. If a primary source fails, the secondary takes over.

If neither a primary or secondary source is specified, the default primary source becomes the Stratum 3 internal clock source (Free-running). Likewise, if no secondary is specified, the default secondary becomes the Stratum 3 internal clock source.

Figure A-1 PXM 45 UI S3 Back Card Connectors



Clock Configuration

Use the following steps to configure clocking on an MGX 8850 media gateway.

Step 1 Telnet onto the gateway. Check that you are logged in to the active PXM 45 card.

Step 2 Use the **cnfclksrc** command to configure the primary clock source.

The syntax of this command is:

cnfclksrc <*priority*> <*portid*>[-**bits** { e1|t1 } *][-**revertive** { enable|disable }]*

where:

priority This is either primary or secondary (default=primary)

portid The specification of the port ID depends upon the selected clock source.

If he BITS clock source is selected portid is specified as:

[shelf.]slot.port

shelf —always 1 and is optional.

•slot—the logical slot number 7 for a BITS circuit on the PXM UI S3 (regardless of where the active PXM resides).

•port—a logical number that indicates the upper or lower external clock connector on

the UI S3 back card. The logical port number for the upper connector is 35. The lower connector is 36.

If a VXSM is selected as the source, portid is specified as:

[shelf.]slot:subslot.port:subport

shelf—Always 1 and optional

•slot—Slot number of the service module

•subslot—Identifies the upper or lower bay of the back card, either a 1 for the upper bay or 2 for the lower bay (default is 1)

•port—Line number on the service module back card plus 10. The specified line must already be active (see upln).

•subport—Logical port number, plus 10. This value is the logical port (or ifNum) that you must assign using the **addport** command. Also, the logical port must be known to PNNI (see **dsppnports**).

Note When you specify a clock source on a VXSM card, the value 10 must be added to both the line and logical port numbers. For example, a primary clock source on a VXSM in slot 3, upper shelf, line 1, logical port 1 is specified as:

cnfclksrc primary 3:1.11:11

•bits—This keyword parameter is required if slot number 7 and port number of 35 or 36 are specified in portid (indicating BITS as the clock source) Type the string -bits,followed by a space, then either e1 or t1.

•revertive—An option that applies to only the BITS clock. Type the string -revertive, followed by the complete word enable or disable. The default is disable.

Step 3 Use the **cnfclksrc** command to configure the secondary clock source.

Step 4 Use the **cnfclkparms** command to configure the signal type and cable type for BITS sources (if applicable). The configuration applies to both (upper and lower) lines.

The syntax of this command is:

cnfclkparms <*signal type*> <*cable type*>

where:

signal type - [1-2]; 1 - data; 2 - syn (this parameter is not supported in this release)

cable type - [1-2]; 1 - twisted; 2 - coaxial

Note E1 lines can be either twisted pair or coaxial cable. T1 lines must always be specified as twisted pair.

Below is an example of a sequence of clock configuration commands.

```
8850japan.7.PXM.a > cnfclksrc primary 7.35 -bits t1 -revertive enable
8850japan.7.PXM.a > cnfclksrc secondary 7.36 -bits t1 -revertive enable
8850japan.7.PXM.a > cnfclkparms 1 1
```

Displaying Clock Configuration

On the PXM card, use the **dspclksrcs** command to display the clocking configuration.

```
8850japan.7.PXM.a > dspclksrcs
Primary clock type:     bits t1
Primary clock source:   7.35
Primary clock status:   bad
Primary clock reason:   no clock
Secondary clock type:   bits t1
Secondary clock source: 7.36
Secondary clock status: bad
Secondary clock reason: no clock
Active clock:           internal
source switchover mode: revertive
```

On the VXSM card, use the **dspln** command to display clocking on a VXSM line. The values are loopclock (when clock is derived from a VXSM line) or local (when derived from BITS).

```
M8850_NY.3.VXSM.a > dspln 1.4
=====================================================
             Sonet Line Information
=====================================================
Sonet Line             :                1.4
Medium Type            :                sonet
Interface Name         :                sonet.3.1.4
Admin Status           :                down
Operational Status     :                down
Time Elapsed(seconds)  :                0
Valid Intervals        :                0
Invalid Intervals      :                0
Line Type              :                sonetSts3
Loopback Config        :                lineLocal
Transmit Clock Source  :                localTiming
Frame Scramble         :                disabled
RDIV Type              :                onebit
RDIP Type              :                onebit
Section Transmit Trace :                0000000000000000000000000000000000000000a
Section Expect Trace   :                0000000000000000000000000000000000000000a
Section Trace Failure  :                false
Section Received Trace :                0000000000000000000000000000000000000000a

archer.5.VXSM.a > dspln 1.1
=====================================================
               DS1/E1 Line Information
=====================================================
DS1/E1 Line            :      1.1
Interface Name         :      ds1.5.1.1
Admin Status           :      up
Operational Status     :      up
Time Elapsed(seconds)  :      256
Type                   :      dsx1ESF
Send Code              :      none
Loopback Config        :      dsx1NoLoop
Signal Mode            :      none
Transmit Clock Source  :      localTiming
Line Coding            :      dsx1B8ZS
Line length (m)        :      0
Line Mode              :      csu
Line Build Out         :      zerodB
Loopback State         :      NoLpbk
Trunk Condition Enable :      false
Loopback Code Detection:      false
```

```
Status                  :       NoAlarm
```

Clocking Guidelines

- The network should have the least possible number of independent clock sources. The best arrangement is to have one network clock source that is distributed to all nodes in the network.
- There can only be one clock source per VXSM card.
- Different VXSM cards, in the same chassis or different chassis, that are part of the same network should get their clocks from sources traceable to the same reference source.
- Do not use separate clock sources unless you can confirm that they will remain closely phase locked. This prevents large changes in clock phase when a clock interface switchover occurs. It is best to take two separate feeds from the same clock source or same clock distribution system.
- Preferred clock sources for a VXSM equipped media gateway are:
  - An external clock from the same source that the switch is connected to (BITS)
  - An external clock from the switch (dedicated source or T1/E1 line)
- Prevent reflections that can produce noise. These are usually caused by:
  - Unterminated connections
  - Cables with long legs on the Y connections

Note MGX systems are designed to work with Y cables. The backup UI interface is always unterminated until it becomes the primary. This mode of operation insures that only one of the legs of a Y cable is terminated preventing both terminations from being on at the same time. If both terminations are on at the same time, the termination resistance (impedance) becomes half its expected value.

  - Too many connectors in the line path
- Use good quality wiring techniques for clock source cables. Use shielded UTP if possible, UTP at a minimum, for balanced (100 or 120 ohm) cables. Make sure you have good grounds on the unbalanced coax clock cables. Keep clock cables as short as possible.
- Clocking problems typically cause Packet Errors, HEC (Header Error Check) errors, PLCP (Physical Layer Convergence Protocol) errors, or frame-sync errors. The error depends upon the type of trunk interface used.
- Clock slips on voice circuits can result in dropped calls, hissing, scratchiness, and echo problems.

Qualifying a Clock Source

When a primary clock source is configured it is qualified by sampling the clock for its frequency at 1 sample per second and analyzing 24 batches each consisting of 16 samples. For a clock to be qualified as a “narrow-band compliant” source, all 16 samples in a batch must have a frequency of within ±4.66 parts per million. after a clock source is qualified, it is deemed Lockable.

A primary Lockable clock source is monitored at one second intervals to ensure that it continues to be qualified. A clock source configured as secondary, is also qualified as Lockable but it is not monitored (unless it becomes the primary source).

A clock source is considered bad if there is a loss-of-activity/loss-of-signal or it becomes Unlockable. When the active clock source is detected to be bad, the active clock source is switched to an alternative good clock source.

Switching to an Alternative Clock Source

Table A-1 summarizes the choice of the alternative clock source:

Table A-1 Next Active Clock Source

Configuration	Current Active Clock Source	Next Active Clock Source
Only Primary	Primary	Holdover if enough samples available. Otherwise, Free-running (internal local oscillator).
Primary and Secondary	Primary	Secondary.
	Secondary	Holdover if enough samples available. Otherwise, Free-running.
	Holdover (stored samples)	Free-running.
	Free-running	None.

The decisions to switch from a bad clock source to an alternative clock source depend on the current active clock source, the nature of failure and the configuration.

Basically there are three major situations.

- Only a primary clock source is configured.
- A primary and secondary clock source are configured with auto-revertive mode enabled.
- A primary and secondary clock source are configured with auto-revertive mode disabled.

Note Auto-revertive mode monitors the failed primary clock source and automatically reverts to that source if it recovers and becomes qualified. The auto-revertive mode is available only if the primary clock source is configured to be an external BITS clock source.

Table A-2 summarizes failure scenarios and recovery actions taken when only a primary clock source is configured:

Table A-2 Clock Failure and Recovery: Primary Source Only

Clock Source Failure	Actions
Primary is the Active clock source and is in LOA/LOS	Raise *minor* alarm to indicate that primary clock source is lost. Switch to Holdover if enough samples available. Switch to free-running if enough samples are not available. Raise *major* alarm to indicate that the node's clock is in holdover or free-running mode. Continue to monitor primary. Once it is out of LOA/LOS, switch to free-running, if it is in holdover mode. Then, re-qualify the primary and revert to the primary when becomes Lockable and clear the alarms.
Primary clock source is the Active clock source and it becomes Unlockable	Raise *minor* alarm to indicate that the primary clock is lost. Switch to free-running. Raise *major* alarm to indicate that the clock is in free-running mode. Note: The primary clock source will be monitored. If it becomes lockable, the primary clock source will be the active clock source This behavior is possible in Release 4.0 and later.
Holdover mode time expires (beyond 24 hours)	Switch to free-running. Continue to monitor the primary clock source. After it goes out of LOA/LOS, requalify the primary clock source and switch to the primary when it becomes Lockable and clear the alarms.
In Free-running mode, local oscillator fails.	TBD: Should raise a critical alarm. Note: This may cause a traffic outage if this happens on the Active PXM. Manual PXM switchover is necessary to recover from the outage. If this happens on the Standby PXM, failure/manual switchover to the Standby PXM may cause an outage.

Table A-3 summarizes failure scenarios and recovery actions taken when both a primary clock sources are configured with Autorevertive enabled.

Table A-3 Clock Failure/Recovery: Primary and Secondary—Revertive Enabled

Clock Source Failure	Action
Primary clock source is the active clock source and it goes into LOA/LOS	Raise *minor* alarm to indicate the primary clock source is lost. Switch to secondary clock source if it is not in LOA/LOS and is Lockable. The secondary clock source becomes the active clock source. Switch to Holdover mode if secondary clock source is not available, and there are enough clock samples collected from the primary clock source. Switch to Free-running mode and use the internal oscillator if neither the secondary clock source is available nor switching to Holdover mode is possible. Raise *major* alarm if the clock is in holdover or free-running mode. Once the primary goes out of LOA/LOS, switch to free-running, raise *major* alarm to indicate that the clock is in free-running mode and start re-qualifying the primary clock source. Switch to the primary once it becomes Lockable after the re-qualification procedure and clear the alarms.
Primary clock source is the active clock source and it enters out-of-lock state. That is, the frequency of the clock sample goes out of range of ±4.66 ppm.	Raise minor alarm to indicate that the primary clock is lost. Continue monitor the primary clock source. If 12 out of 16 samples have the frequency with in the range of ±4.66 ppm, declare it Lockable again and clear the alarm. Otherwise, if more than 6 samples have the frequency with in the range of ±4.66 ppm, declare it Unlockable and start the re-qualification process. During this re-qualification, switch to the secondary or the free-running, if secondary is not available. Raise *major* alarm if it is in free-running mode. Once the re-qualification process is complete and the primary is Lockable, revert to the primary, else, declare the primary Unlockable. Otherwise (if there only less than 6 samples having the frequency with in the ±4.66 ppm), declare the primary Unlockable.
Primary clock source is the active clock source and it becomes Unlockable after requalification in out-of-lock state failed. Note: The primary clock source enters out-of-lock state before becoming Unlockable. If it became Unlockable after requalification, the active clock should have been already switched to the secondary or the free-running mode.	Note: The primary clock source is monitored/qualified, and switched over to the primary clock source if the clock source is good.

Table A-3 Clock Failure/Recovery: Primary and Secondary—Revertive Enabled (continued)

Primary clock source is the active clock source and it becomes Unlockable because the number of samples with frequency with in ±4.66 ppm out of the 16 collected samples is less than 6. Note: In this case, the active clock source is still the primary and is in the out-of-lock state.	Switch to secondary clock source if it is not in LOA/LOS and is lockable. The secondary clock source becomes the active clock source. Switch to Free-running mode and use the internal oscillator if the secondary clock source is not available. Raise *major* alarm if the clock is in free-running mode.
Secondary clock source is the active clock source and it goes into LOA/LOS.	Raise *minor* alarm to indicate that secondary clock source is lost. Switch to holdover mode if there are enough samples. Switch to Free-running if there are not enough samples to switch to holdover mode. Raise major alarm to indicate that the active clock is either holdover or free-running mode. Switch back to the primary or the secondary once one of them becomes available.
Secondary clock source is the active clock source and it enters out-of-lock state. That is, the frequency of the clock sample goes out of ±4.66 ppm range.	Raise minor alarm to indicate that the secondary clock is lost. Continue monitor the secondary clock source. If 12 out of 16 samples have the frequency with in the range of ±4.66 ppm, declare it lockable again and clear the alarm. Otherwise, if more than 6 samples have the frequency with in the range of ±4.66 ppm, declare it Unlockable and start the re-qualification process. During this requalification, switch to the free-running mode. Raise *major* alarm to indicate that it is in free-running mode. Once the requalification process is complete and the secondary is lockable, revert to the secondary, else, declare the secondary Unlockable. Otherwise (if there only less than 6 samples having the frequency with in the ±4.66 ppm), declare the secondary Unlockable.
Secondary clock source is the active clock source and it becomes Unlockable after requalification in out-of-lock state failed. Note: The secondary clock source enters out-of-lock states before becoming Unlockable. If it became Unlockable after requalification, the active clock should have been already switched to the free-running mode.	Note: The primary and the secondary clock sources are no longer monitored/qualified and no switchover to the secondary or the primary clock source occurs. The clock sources must be manually reconfigured to initiate the switchover to the primary or the secondary clock source.

Table A-3 Clock Failure/Recovery: Primary and Secondary—Revertive Enabled (continued)

Secondary clock source is the active clock source and it becomes Unlockable because the number of samples with frequency with in ±4.66 ppm out of the 16 collected samples is less than 6. Note: In this case, the active clock source is still the secondary and is in the out-of-lock state.	Switch to Free-running mode and use the internal oscillator. Raise *major* alarm to indicate that the clock is in free-running mode. Note: The primary and secondary clock sources are no longer monitored/qualified and no switchover to the primary or the secondary clock source occurs. The clock sources needs to be manually reconfigured to initiate the switchover to the primary or the secondary clock source.
Holdover expires (more than 24 hours since clock source is switched to the holdover mode)	Raise *major* alarm. Switch to free-running mode.
In Free-running mode, local oscillator fails.	TBD: Should it raise critical alarm? Note: This may cause a traffic outage if this happens on the Active PXM. Switchover to Standby PXM should be initiated manually to recover from the outage. If this happens on the Standby PXM, failure/manual switchover to the Standby PXM may cause an outage.

Table A-4 summarizes failure scenarios and recovery actions taken when both a primary clock sources are configured with Auto-revertive disabled

Table A-4 Clock Failure/Recovery: Primary and Secondary—Revertive Disabled

Clock Source Failure	Action
Primary clock source is the active clock source and it enters LOA/LOS.	Raise *minor* alarm to indicate that primary clock source is lost. Switch to secondary clock source if it is not in LOA/LOS and is lockable. The secondary clock source becomes the active clock source. Switch to Holdover mode if secondary clock source is not available, and there were enough clock samples collected from the primary clock source. Switch to Free-running mode and use the internal oscillator if neither the secondary clock source is available nor switching to Holdover mode is possible. Raise *major* alarm if the active clock is in holdover or free-running mode. After the primary comes out of LOA/LOS, initiate the requalification of the primary. If the active clock source is in holdover or free-running mode, then, switch to the primary after the requalification process is complete and is lockable.

Table A-4 Clock Failure/Recovery: Primary and Secondary—Revertive Disabled (continued)

Primary clock source is the active clock source and it enters out-of-lock states. That is, the frequency of the clock sample goes out of ±4.66 ppm range.	Raise minor alarm to indicate that the primary clock is lost. Continue monitor the primary clock source. If 12 out of 16 samples have the frequency with in the range of ±4.66 ppm, declare it lockable again and clear the alarm. Otherwise, if more than 6 samples have the frequency with in the range of ±4.66 ppm, declare it Unlockable and start the re-qualification process. During this requalification, switch to the secondary or the free-running, if secondary is not available. Raise *major* alarm if it is in free-running mode. After the requalification process is complete and the primary is lockable, revert to the primary if the active clock source is in free-running mode. If the primary is not lockable, declare the primary Unlockable. Otherwise (if there only less than 6 samples having the frequency with in the ±4.66 ppm), declare the primary Unlockable.
Primary clock source is the active clock source and it becomes Unlockable.	Raise the alarm. Switch to secondary clock source if it is not in LOA/LOS and lockable. The secondary clock source becomes the active clock source. Switch to Free-running mode and use the internal oscillator if the secondary clock source is not available.
Secondary clock source is the active clock source and it goes into LOA/LOS.	Raise the alarm. Switch to Free-running. Switch back to the primary or the secondary once one of them becomes available.
Secondary clock source is the active clock source and it becomes Unlockable.	Raise the alarm. Switch to Free-running. Switch back to the primary or the secondary once one of them becomes available.
In Free-running mode, local oscillator fails.	Raise the alarm. Note: This may cause a traffic outage if this happens on the Active PXM and the PXM switchover is not initiated manually. If this happens on the Standby PXM, failure/manual switchover to the Standby PXM may cause an outage.

Numerics

1
  1 APS line redundancy **2-31**
  1 front/back card redundancy **2-28**
  1 front card/back card redundancy **2-31**
1+1 APS line redundancy **2-30**

A

AAL2 trunking **2-24**
AAL5 trunks for Nx64 format **4-18**
alarms and statistics **2-38**
algorithms **2-18**
announcement feature **2-20**
announcement files **5-15**
applications
  signaling gateway **1-2**
  trunking nonswitching **1-2**
authentication header **2-17**
automatic switchover **2-13**
AXSM Card Configuration **4-4**
AXSM card configuration **3-7**

B

back cards **2-1**
backhaul feature **2-13**
backhauling signaling channels **2-12**
bearer amd signaling security **3-50**
bearer channel **8-14**
bearer path **5-18**
bearer streams **2-18**
Bearer Trace feature **xi, 8-13**
bearer tracing
  CLI requirements **8-18**
  configuration **8-19**
  configuration examples **8-22**
  connectivity **8-17**
  trace files **8-24**
  trace types **8-15**
  troubleshooting **8-25**
boot code **7-6**

C

CAC check **4-18**
CALEA
  configuration **3-34**
  surveillance **2-19**
  switching applications **2-18**
CALEA and non-CALEA image numbering **7-6**
card redundancy **5-7**
card slots **2-6**
CIDs **4-16**
cipher suites **2-18**
clocking
  configuration **A-2**
  displaying the configuration **A-4**
  guidelines **A-5**
  qualifying a clock source **A-5**
  switching to an alternative source **A-6**
clocking basics **A-1**
CNG tone **2-25**
collecting bearer traces **8-14**

Communications Assistance for Law Enforcement Act **2-18**
Configuration
VXSM card **4-5**
configuring
AAL2 trunks **4-16**
announcements **5-14**
APS SONET line redundancy **5-7**
AXSM card **3-7, 4-4**
bearer amd signaling security **3-50**
CIDs **4-16**
clocking **5-5**
differentiated services **5-17**
E911 Emergency services **3-43**
fax/modem **5-18**
fax and modem **5-18**
HDLC signaling **4-18**
jitter compensation **5-46**
LAPD **3-39, 3-41, 5-12**
MGC interface **3-21**
MGC redundancy **3-34**
network bypass **5-16**
online diagnostic feature **5-45**
PRI backhaul **3-36, 5-10**
PVC channel protection **5-9**
PXM card **3-5, 4-3**
redundancy **5-7**
RPM card **3-8**
RUDP **3-36, 5-10**
SONET lines and paths **5-1**
T.38 fax relay profiles **5-24, 5-27**
T1/E1 lines **5-1**
T1 lines **2-6, 5-1**
T3 lines **5-1**
TDM interface **3-11**
TDM lines **3-16**
TTY data profiles **5-22**
voiceband data profiles **5-20**
voiceband event mapping **5-18**
VXSM card **3-10**
VXSM features **5-1**
congestion avoidance **2-15**
Connection Admission Control **5-7**
control path **5-18**
control protocol extended reports **2-21**
CPU bandwidth **8-19**
creating trunk connections **4-12**
creating VXSM trunks **4-12**
current voice calls (TGCP) **8-11**

D

DASS user adaptation layer **2-15**
data stream **4-18**
denied connection **5-7**
differentiated services **2-10**
DiffServ **5-17**
digital access signaling system **2-13**
digital private network signaling system **2-13**
displaying configuration **5-2**
DPNSS/SCTP backhauling **2-15**
DSP resources **5-48**
DUA **2-15**

E

E911 Emergency services **2-19, 3-43**
event-handling **5-18**
event mapping and voice interfaces **5-29**

F

Failed-U state **7-5**
fault-tolerance, configuring **2-13**
fax/modem
services **5-18**
traffic **2-33**
TTY passthrough **2-33**

firmware images **2-6**
flags **4-18**
flooding **2-15**
fragmentation **5-48**
front/back card redundancy **5-7**
front cards **2-1**
fw extension **7-6**

G

gateways
  using H.248 MGC protocol **3-21**
  using XGCP MGC protocol **3-30**

H

H.248
  media gateway controller setup **3-21**
  protocol configuration **3-23**
hard disk, PXM **7-5**
HDLC
  data stream **4-18**
  frames **4-18**
History Index parameter **5-43**
history reports **2-23**

I

identifying voice circuits **3-11, 4-6**
image
  filenames **7-5**
  revision numbers **7-5**
image-numbering **7-6**
index number **4-18**
interframe flag **4-18**
Internet key exchange protocol **2-17**
IPSec **2-16**
ISDN/SCTP backhauling **2-14**
ISDN signaling (PRI backhaul) **2-13**

J

jitter
  compensation **5-46**
  parameters **2-34**
  removing **2-9**
jitter delay
  AAL2 applications **5-47**
  fax/TTY/modem traffic **5-47**
  voice codecs **5-46**

L

line redundancy **2-30**
loading VXSM code images **xii, 7-1**

M

mapping **5-4**
mapping announcements **5-15**
media gateways
  clocking **A-1**
  controllers and controller groups **3-21, 3-30**
MGC
  H.248 profile configuration **3-27**
  interface configuration **3-21**
  XGCP profile configuration **3-32**
MGX chassis **2-2**
mixed codecs **5-48**
modes
  transport **2-17**
  tunnel **2-17**
  VoIP switching **3-27**
multihoming **2-15**

N

Network Bypass feature **2-36, 5-16**
nonswitching operation **2-24**

nonvoice calls **2-33**
null algorithms **2-18**
Nx64
  data **4-18**
  packet **4-18**

O

online diagnostic feature **5-45**
outage, power **7-5**
out of service. **5-2**
override **2-34**

P

packetization period **2-34**
patch numbers **7-6**
peak cell rate **5-7**
phase identifier **7-6**
phase reversal **4-18**
physical description **2-1**
PNNI resource partition configuration **3-8**
power outage **7-5**
PRI backhaul **5-10**
primary VXSM card **7-5**
protocols
  H.248 call control **2-36**
  IKE **2-16**
  IPSec **2-16**
  operator services package **2-19**
  streaming control transmission **2-13, 2-15**
  TGCP gateway control **2-18**
  user adaptation layer **2-13**
PVC channel protection **5-9**
PXM card configuration **3-5, 4-3**
PXM hard disk **7-5**

Q

quality monitoring feature **2-21**

R

RCON card **2-27**
redundancy **2-27, 5-7**
related VXSM documents **1-3**
reliable UDP **2-13**
revision numbers **7-6**
RFC 3611 **2-21**
routing voice calls **2-24**
RPM card configuration **3-8**
RUDP **2-13**
runtime code **7-6**

S

SDH systems **3-12, 4-7**
secondary VXSM card **7-5**
security
  algorithms **2-16**
  features **2-16, 3-50**
service level agreements **2-23**
service type **5-7**
setting up
  H.248 media gateway controller **3-21**
signaling gateway
  configuration **6-4**
  description **6-1**
  statistics **6-2**
signaling message **2-12**
signaling systems **2-13**
signal security **2-17**
sout trace **8-15**
SS7
  ASP and AP configuration **6-10**
  Configuration - IP side **6-8**

Configuration - SS7 side **6-4**
SCCP-GTT configuration **6-15**
Statistics **6-2**
statistics collection **2-19**
subcell multuplexing **4-17**
surveillance **2-19**
sustained cell rate parameter **5-7**
switching
configuring **3-1**
mode **2-7**
mode features **2-8**
switchover, configuring **2-13**

T

T.38
fax relay **2-35**
fax relay profiles **5-24**
fax relay statistics **2-36**
probe **8-15**
TFTP directory **5-15**
TGCP **2-16**
titan numbering scheme **5-3**
tones **2-25**
modem/fax **4-18**
preamble fax **4-18**
trace files **8-15**
trace session **8-14**
transport mode **2-17**
trunk connections **4-12**
trunking
operation **2-24**
quickstart **4-2**
trunking mode features **2-24**
TTY data profiles **5-22**
tunnel mode **2-17**

U

UDP **2-13**
upgrade errors **7-5**
upgrading
VXSM card software **7-3**
VXSM code images **7-1**
upspeed **4-18**
user adaptation layer **2-13, 2-15**
user-state control packets **4-18**

V

version number **7-6**
voiceband data **4-18**
event mapping **5-18**
profile **5-20**
voice circuit identification **3-11, 4-6**
voice interfaces (VIF) **3-14**
voice quality
configuring **5-30**
monitoring **2-21**
voice quality monitoring feature **2-21**
VoIP
operation **2-7**
Quickstart **3-1**
security features **2-16**
VQM History Index parameter **5-43**
VTG **5-2**
VTG/VT to DS1 mapping scheme **5-2**
VTG-VT pair **5-3**
VT number pair **5-3**
VXSM
Card Configuration **4-5**
card configuration **3-10**
first-time image load **7-2**
version upgrade procedure **7-3**

X

XGCP media gateway controller setup **3-30**
XGCP protocol configuration **3-31**