297-8403-906

DMS-100 Family

# TOPS Internet Protocol (TOPS-IP)

## User's Guide

SN09 and up Standard 06.03 April 2006

NORTEL NETWORKS™

DMS-100 Family

# TOPS-IP

## User's Guide

Publication number: 297-8403-906
Product release: SN09 and up
Document release: Standard 06.03
Date: April 2006

# Publication history

**April 2006**

Standard 06.03 maintenance release for TOPS22/SN09 includes changes to the following technical content:

- updated Appendix A: DHCP Server Guidelines for NETID 4.5 and Oracle 10.1.0.2 installation.
- corrected NTP number and title to reflect the TOPS-IP user's guide.

**June 2005**

Standard 06.01 maintenance release for TOPS22/SN09 includes changes to the following technical content:

- four new parameters in table OFCENG: IPGW_SNMP_COMMUNITY_NAME, IPGW_SNMP_MANAGER, IPGW_SNMP_ENABLED, IPGW_TELNET_ENABLED
- changed table XPMIPMAP to add a new field, SNMP, which indicates whether SNMP is enabled on the IP-XPM. If so, it also enables the SNMP community name.
- updated the supported IP-XPM software loads to QTP22 for releases TOPS22/SN09 and up.

**March 2005**

Standard 05.01 maintenance release for TOPS21/SN08 includes changes to the following technical content:

- new TOPS 615 log.
- updated the supported IP-XPM software loads to QTP21 for releases TOPS21/SN08 and up.
- removed the OCMCCS register from the TOPSOC OM group.
- TOPS OC via ETMS functionality no longer available.
- TOPS Position via ETMS functionality no longer available.
- TDM-OC links must be replaced with CO-IP links prior to upgrade.

### March 2005

Standard 04.04 maintenance release for TOPS20/SN07 includes changes to the following technical content:

- warning to disable spanning tree algorithm under specific circumstances.
- updated the supported IP-XPM software loads to QTP20 for releases TOPS20/SN07 and up.

### December 2004

Standard 04.02 maintenance release for TOPS20 includes changes to the following technical content:

- updated the XIP600 log.

### November 2004

Standard 03.07 maintenance release for TOPS19 includes changes to the following technical content:

- updated XIP600 log.
- Added information on the cabinetized IP-XPM option.

### July 2004

Standard 03.06 maintenance release for TOPS19 includes changes to the following technical content:

- updated the xpm provisioning rules in the engineering section.
- updated DHCP requirements for SUN JRE and the NetID server.

### February 2004

Standard 03.05 maintenance release for TOPS19 includes changes to the following technical content:

- updated the operator position headset issues for Force Management
- updated DHCP requirements for SUN JRE and the NetID server.

### December 2003

Standard 03.04 maintenance release for TOPS19 includes changes to the following technical content:

- updated the supported IP-XPM software loads to QTP19 for releases TOPS 17 and up

### November 2003

Standard 03.03 release for TOPS19 and up also includes new material that applies to TOPS17. This is a major rewrite. It adds or changes the following technical content:

- adds information about the IP positions to most existing sections; also adds three new sections about to IP positions
- modifies the IP-XPM engineering rules, revising the earlier rules for OC-IP as well as adding information about IP positions
- changes the supported codecs, and table PKTVPROF

  ***Note:*** The supported codecs in TOPS15 were G.711 and G.729. In more recent releases, the supported codecs are G.711 and G.723. Changes in table PKTVPROF, where codec selection is datafilled, were not patched back to releases earlier than TOPS19/SN06. However, the existing fields of table PKTVPROF are interpreted differently in a patched load. See "Table PKTVPROF prior to TOPS19" on page 70.
- modifies the DHCP server guidelines to apply to Optivity NetID version 4.3.2

***Note:*** This book was not released in TOPS17. However, certain functionality did change in TOPS17. This release is a reference for changes and enhancements that were made between TOPS17 and TOPS19 inclusive.

## April 2002

Standard 02.04 release for TOPS15 and up, adds or changes the following technical content:

- adds information about the OCManB alarm to the maintenance section
- adds information about the IP-XPM diagnostic for default router connectivity, and a warning not to RTS FORCE an IP-XPM, to the maintenance section
- adds information about problem numbers in TOPS133 logs to the logs section
- adds information about maintaining NetID and Windows NT logs to the DHCP server guidelines section
- modifies the SNMP and DHCP server guidelines to indicate that the SNMP network management station is no longer, by default, able to initiate a Gateway reboot

## September 2001

Preliminary 02.03 release for TOPS15 and up, adds or changes the following technical content:

- adds information on 7X07AA Gateway card slot position and port numbering
- adds information on setting up the Gateway loadfile at the DHCP server
- adds information on upgrading the Gateway loadfile at the DHCP server

## July 2001

Preliminary 02.02 release for TOPS15 and up, adds or changes the following technical content:

- adds information on how to correct an IP address mismatch for the Gateway card
- replaces TOPS105 log with new TOPS133 log
- updates DHCP server guidelines

***Note:*** The 02.02 version is designated for training purposes.

## March 2001

Preliminary 02.01 release for TOPS15 and up, adds or changes the following technical content:

- adds description of new table PKTVPROF
- adds descriptions of two existing tables, TOPSTOPT and TQCQINFO
- adds description of new OFCENG parameter
- removes datafill examples for tables OCPARMS, OCHOST, and OCHOSTQ
- adds information on limiting the use of available dynamic voice links
- adds information on the IPGWSTAT tool
- adds two new logs, TOPS505 and TOPS614
- adds appendix on TOPS-IP support for SNMP (Simple Network Management Protocol)
- updates voice codec selection
- updates the datafilling of OC-IP data links
- updates the provisioning of C-side 14 links
- updates the engineering of QMS MIS-IP data links
- updates limitations and restrictions

## November 2000

Standard 01.03 release for TOPS13 and up, adds or changes the following technical content:

- removes TOPS-IP support of switches provisioned with junctored network (JNET)
- updates engineering guidelines for the following components:
  - C-side links
  - MIS-IP data links
  - 7X07AA Gateway cards

- updates datafill information for OC-IP data links
- adds information on OM group XPMMSGOC (XPM Messaging Occupancy)
- updates DHCP server guidelines

### September 2000

Beta 01.02 release for TOPS13 and up, adds or changes the following technical content:

- updates engineering information
- adds information on maintenance of IP Gateway nodes
- adds descriptions of XIPVER tool error messages
- adds information on the CONVERTCSLINKS utility
- adds preliminary information on DHCP server installation and configuration
- standardizes the following terms using hyphens:
  - TOPS-IP
  - IP-XPM
  - QMS MIS-IP
  - OC-IP
- changes the applicability designation from “LET0013 and up” to “TOPS13 and up”

### March 2000

Preliminary 01.01 release for LET0013 and up, contains preliminary information for the TOPS IP product, including engineering estimates for planning purposes.

# Contents

# About this document

The *TOPS Internet Protocol (TOPS-IP) User's Guide* accompanies the TOPS-IP product. The guide describes how TOPS-IP functionalities work together to deliver services. It provides the user with an overview of the TOPS-IP product, a detailed description of the software, and supplementary information on engineering, datafill, and maintenance activities.

This guide is intended for users who are familiar with DMS Traffic Operator Position System (TOPS) processing, Operator Centralization (OC), Intelligent Workstation System (IWS), and basic concepts of IP internetworking.

## Sections and chapters in this book

Following is a summary of each section and its chapters.

### Part 1: Introduction

This section introduces the components of the TOPS-IP network.

#### Chapter 1: TOPS-IP overview

This chapter provides an overview of the TOPS-IP network architecture and an introduction to key TOPS-IP components.

### Part 2: Functional description

This section describes the IP infrastructure for data and voice communication, and discusses the TOPS-IP applications that use this infrastructure.

#### Chapter 2: TOPS-IP data and voice communication

This chapter discusses the IP data and voice communication required for applications in the TOPS-IP network.

#### Chapter 3: TOPS OC-IP application

This chapter provides details on the functionality of TOPS OC-IP.

#### Chapter 4: TOPS IP position application

This chapter provides details on the functionality of the TOPS IP position application.

### Chapter 5: TOPS QMS MIS-IP application

This chapter provides details on the IP functionality of TOPS Queue Management System Management Information System (QMS MIS-IP).

## Part 3: Interactions

This section provides information on interactions, enhancements, limitations, and restrictions for the TOPS-IP product.

### Chapter 6: TOPS-IP feature impact

This chapter discusses limitations and restrictions for TOPS-IP capabilities in the network.

## Part 4: Planning and engineering

This section discusses TOPS-IP network planning and engineering considerations.

### Chapter 7: TOPS-IP engineering guidelines

This chapter provides requirements for performance, capacity, and provisioning for the TOPS-IP switch, operator service center (OSC), and packet data networks.

## Part 5: Provisioning

This section provides details and examples of TOPS-IP switch datafill, and information on related software ordering.

### Chapter 8: TOPS-IP data schema

This chapter describes datafill requirements for TOPS-IP.

### Chapter 9: TOPS-IP software ordering

This chapter discusses product ordering codes for TOPS-IP.

## Part 6: Billing

The TOPS-IP product does not affect or change billing.

## Part 7: OA&M

This section provides details on DMS switch maintenance activities for TOPS-IP applications, including user information on related command interface (CI) tools, log reports, and operational measurements (OM).

### Chapter 10: TOPS-IP maintenance activities

This chapter describes maintenance activities associated with TOPS-IP applications.

### Chapter 11: TOPS-IP CI tools

This chapter discusses related CI tools.

### Chapter 12: TOPS-IP logs

This chapter shows examples of switch log reports for TOPS-IP.

#### Chapter 13: TOPS-IP OMs

This chapter shows examples of switch OMs for TOPS-IP.

### Appendixes

The following appendixes provide additional information relevant to the TOPS-IP product.

#### Appendix A: DHCP server guidelines

Appendix A provides guidelines on how to install and configure the Dynamic Host Configuration Protocol (DHCP) server for TOPS-IP.

#### Appendix B: TOPS-IP support for SNMP

Appendix B discusses TOPS-IP support for the Simple Network Management Protocol (SNMP).

#### Appendix C: TOPS-IP Network Configuration

Appendix C provides information about planning and configuring a data network to support TOPS-IP applications.

#### Appendix D: IWS IP datafill quick reference

Appendix D provides a quick reference for IWS datafill that is mentioned throughout this book.

### List of terms

This chapter lists terms and definitions.

## References in this book

The following PCL-specific books are referred to in this book. The middle layer of the document number is represented by *nnnn* because this number is determined by the PCL to which the book belongs.

- Translations Guide, 297-*nnnn*-350
- Customer Data Schema Reference Manual, 297-*nnnn*-351
- Operational Measurements Reference Manual, 297-*nnnn*-814
- Log Report Reference Manual, 297-*nnnn*-840

The following other documents are referred to in this book:

- *Networks Maintenance Guide*, 297-1001-591
- *TOPS IWS Force Management Guide*, 297-2251-313
- *TOPS IWS Base Platform User's Guide*, 297-2251-010
- *TOPS and TMS Maintenance Manual*, 297-8341-550
- *OSSAIN User's Guide*, 297-8403-901
- *Command Interface Reference Manual*, 297-8991-824
- *Software Optionality Control User's Manual*, 297-8991-901

- *Engineering Change Manual 606*
- *Business Policy Switch 2000 Installation Instructions*, 209319-A
- *Using the Business Policy Switch 2000 Software Version 2.5*, 208700-D
- *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, 209570-D
- *Open Position Protocol Specification*, Q214-1

  ***Note:*** OPP is a licensed interface. To receive this document, please contact Nortel Networks Marketing.
- *TOPS QMS MIS Protocol*, Q220-1

  ***Note:*** QMS MIS Protocol is a licensed interface. To receive this document, please contact Nortel Networks Marketing.

This book also refers to the following standards, specifications, and sources of general information.

- *Internetworking with TCP/IP*, by Doug E. Comer (Prentice Hall)
- *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, by William Stallings (Addison-Wesley)
- ITU-T (G.711), *Pulse Code Modulation of Voice Frequencies*
- ITU-T (G.723.1), *Dual Rate Speech Coder for Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s*
- ITU-T (H.323), *Packet-based Multimedia Communications Systems*
- RFC768 (STC 6) *User Datagram Protocol*
- RFC791 (STD 5) *Internet Protocol*
- RFC792 (STD 5) *Internet Control Message Protocol*
- RFC793 (STC 7) *Transmission Control Protocol*
- RFC951 *Bootstrap Protocol*
- RFC1157 (STD 15) *Simple Network Management Protocol*
- RFC1213 *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
- RFC1643 *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC1889 *RTP: A Transport Protocol for Real-Time Applications*
- RCF1910 *User-based Security Model for SNMPv2*
- RFC2131 *Dynamic Host Configuration Protocol*
- RFC2338 *Virtual Router Redundancy Protocol*
- RFC2543 *SIP: Session Initiation Protocol*

- EN 300 386 V1.3.1 (2001-09). *Electromagnetic compatibility and Radiospectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements*
- EN 60950 *Safety of Information Technology Equipment Including Electrical Business Equipment*

# Part 1: Introduction

Part 1: Introduction includes the following chapter:

# Chapter 1: TOPS-IP overview

The DMS Traffic Operator Position System Internet Protocol (TOPS-IP) product provides a new technology for delivering operator services over a managed IP network. Using standard IP network components, TOPS-IP offers a unified solution for data and voice.

This chapter gives an overview of the TOPS-IP product, focusing on the following topics:

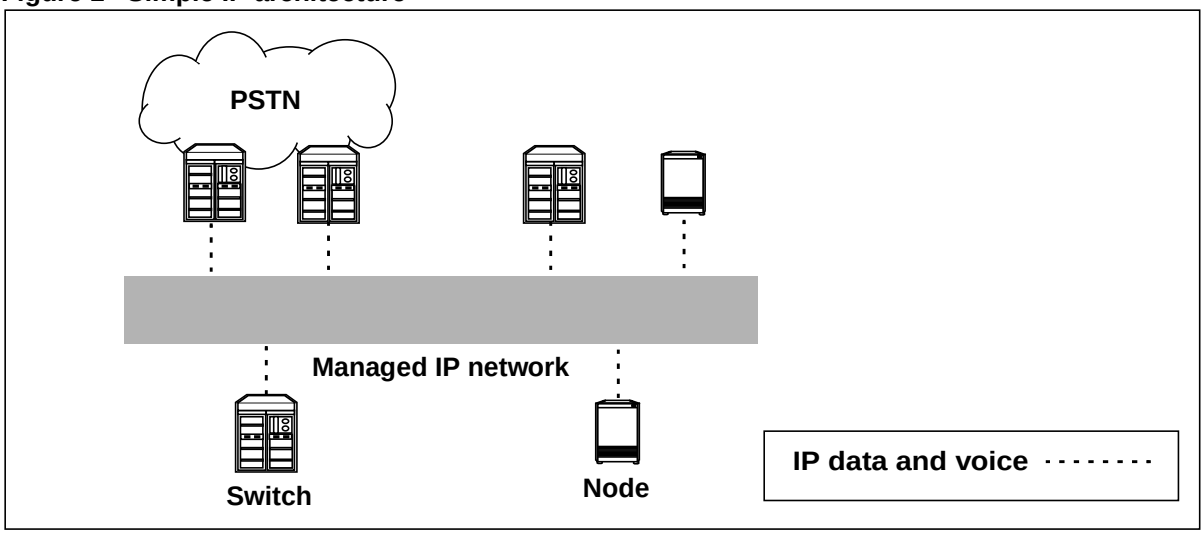
- benefits of IP networking
- components of the IP infrastructure
- capabilities of TOPS-IP

The last section provides a road map to detailed TOPS-IP information in this book, and to related IP information in other books.

## Benefits of IP networking

IP networking, which is implemented by the IP protocol suite and IP-related equipment, has a universal presence in networks today. IP telephony makes use of this presence by integrating data and voice traffic across the network. Figure 1 illustrates a simple IP architecture that integrates data and voice.

**Figure 1 Simple IP architecture**



The integrated IP approach provides an alternative to the traditional operator services network architecture, much of which relies on nailed-up time division multiplexed (TDM) trunking facilities to carry data and non-packetized voice traffic. Establishing a *common IP infrastructure*, on the other hand, can bring cost savings and more flexibility to the service provider's network. These benefits are especially notable in an operator services platform, which may have several switches configured in a centralized way to optimize operator resources.

The following paragraphs summarize the advantages of IP networking.

### Eliminates point-to-point provisioning

With IP networking, voice and data facilities are not provisioned point to point. The only requirements are that the managed IP network must have enough bandwidth to support the total network traffic, and that each switch must have enough bandwidth to support its combined traffic to and from the network.

This benefit lessens the need for reconfiguration of the network to accommodate changing traffic patterns. It also decreases costs and facilitates faster introduction of new services.

### Optimizes bandwidth consumption

IP networking reduces bandwidth consumption during times when no data or voice is sent. Voice compression technology can further reduce bandwidth requirements.

### Uses industry-standard IP network components

Standard IP components, some of which the operating company may already own, are used in the managed IP network. Standardization can lead to lower costs as components are reused in new IP-based services development.

***Note:*** The TOPS-IP product does not change the IP protocol.

## Components of the IP infrastructure

The IP infrastructure, which provides integrated data and voice for TOPS-IP, consists of the following two broad components:

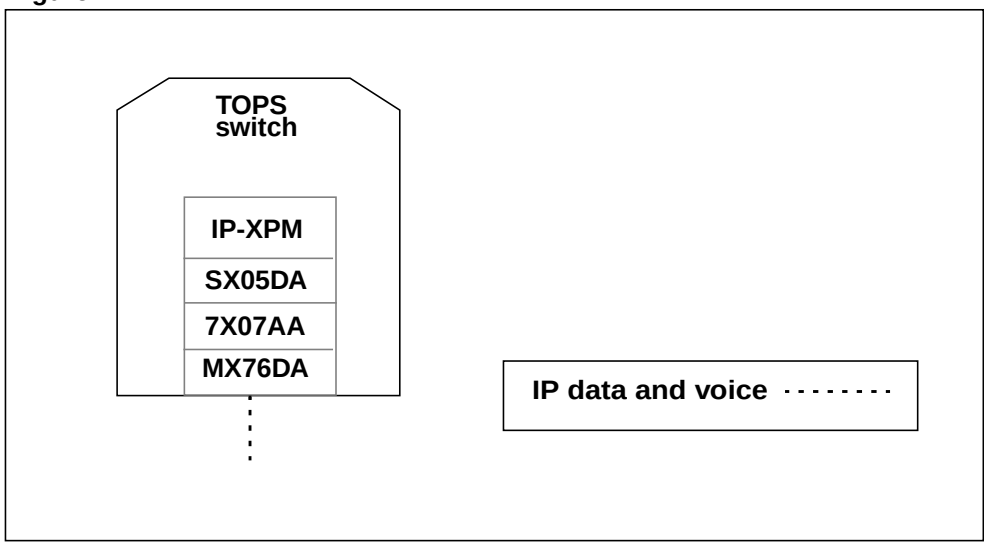
- an IP-based extended peripheral module (IP-XPM) at the DMS switch
- the managed IP network, or private intranet

This section introduces the key hardware for these two components. Chapter 2: “TOPS-IP data and voice communication” provides functional details and Chapter 7: “TOPS-IP engineering guidelines” discusses engineering details.

### Overview of the IP-XPM

The IP-XPM is a DTC (Digital Trunk Controller) peripheral equipped with several new or upgraded components that support the integrated IP architecture. Figure 2 illustrates the IP-XPM at the TOPS switch. The components are discussed following the figure.

**Figure 2 IP-XPM**




### SX05DA processor card

The SX05DA processor card is used for data communication over the managed IP network. It serves as the main processor, replacing the MX77 processor. The SX05DA has a full-duplex 10/100 Megabit per second (Mbps) Ethernet port. It greatly improves performance and increases system memory size. An IP-XPM has two SX05DA cards provisioned.

***Note:*** Versions of the SX05 card that are previous to the DA version do not have the Ethernet port and are not supported for TOPS-IP data communication.

### 7X07AA Gateway card

The 7X07AA Gateway card is used for voice communication over the managed IP network. It has two full-duplex 10/100 Mbps Ethernet ports. The 7X07 is responsible for conversion between circuit-switched voice and packet-switched voice. It also handles the call setup signaling associated with its voice channels.

An IP-XPM may have multiple 7X07 cards provisioned. Each card supports 60 voice channels. However, the DMS switch limits the number of channels that can be used on each 7X07 to 48.

***Note:*** TOPS-IP applications that do not use voice, such as QMS MIS-IP (see page 33), do not require 7X07 Gateway cards.

### MX76DA messaging card

The MX76DA messaging card supports the bandwidth requirements for enhanced C-side 14 messaging between the CM and the IP-XPM. C-side 14 messaging requires the use of an enhanced network (ENET) interface and DS512 fiber links to the IP-XPM.

### Other IP-XPM hardware

In addition to requiring the specialized cards, each IP-XPM also requires the following hardware:

- IP-XPM frame (NT6X01AF)
- two IP-XPM shelves (NT6X0261)
- two connector key brackets (P0912903)
- two IP-XPM cables (NT0X96NV or NT0X96NW) that connect the IP-XPM backplane either to an Ethernet patch panel (optional) or to a compatible Ethernet switch on the LAN

If the IP-XPM is installed in a cabinet instead of a frame, the following hardware is required:

- IP-XPM cabinet (NTRX46CG)
- two IP-XPM shelves (NT6X0261)
- two NTRX26HB cables to connect the cabinet backplane to the Ethernet switch
- TOPS-IP Ethernet cable kit (NTNX1236) to connect the shelf to the cabinet backplane

***Note:*** This list is not exhaustive; the IP-XPM requires other hardware and packfill. Also, existing XPMs *cannot* be retrofitted to provide IP functionality; rather, they must be replaced with an IP-XPM. For more information on IP-XPM hardware requirements, refer to Chapter 7: “TOPS-IP engineering guidelines.”

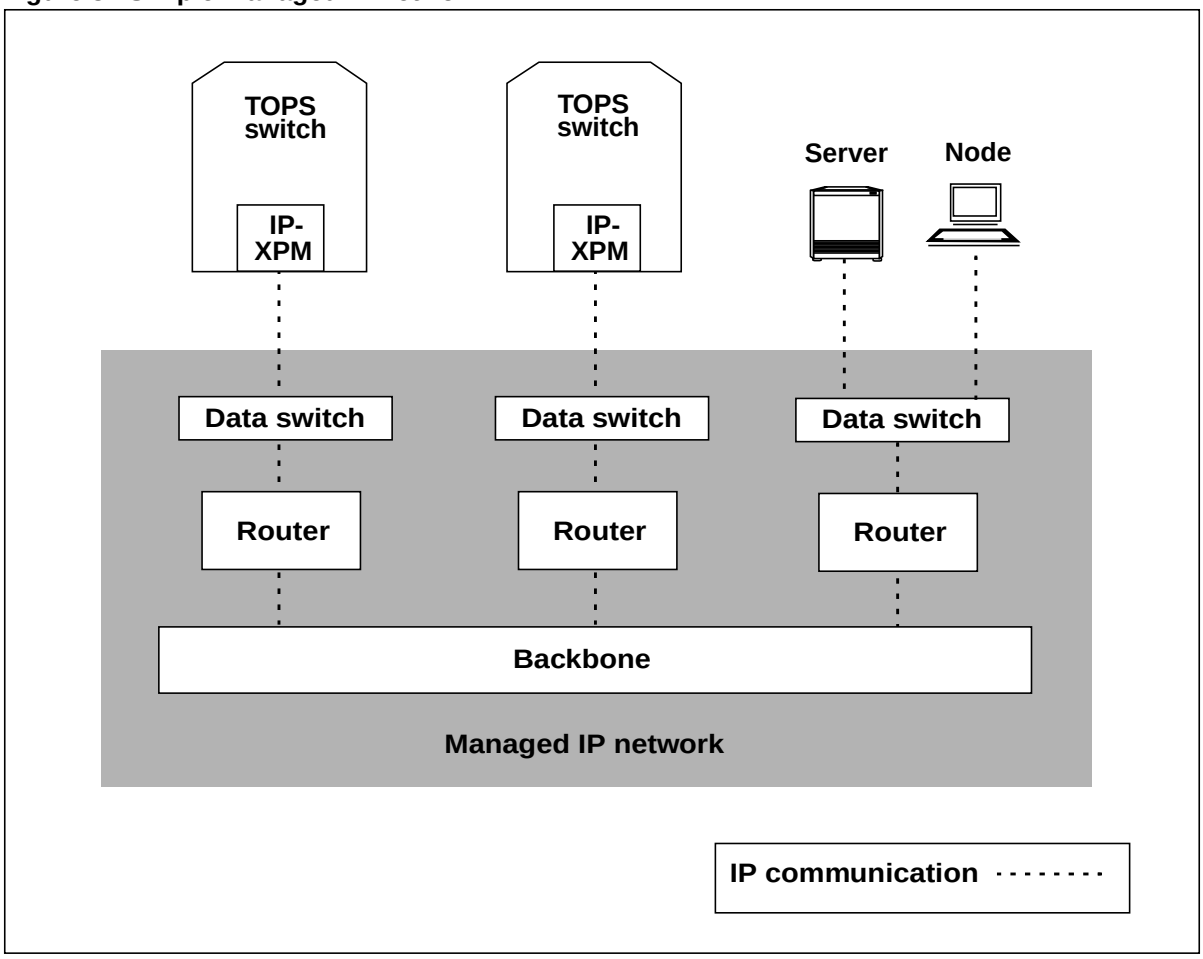
### DHCP/FTP server

A Dynamic Host Configuration Protocol/File Transfer Protocol (DHCP/FTP) server is required to load and configure the 7X07AA Gateway cards. For details, refer to Appendix A: "DHCP server guidelines."

## Overview of the managed IP network

The managed IP network is responsible for routing and delivering data and voice traffic between nodes in the private intranet. Figure 3 shows a simple, functional diagram of a managed IP network for TOPS.

**Figure 3 Simple managed IP network**




A managed IP network consists of several layers:

- *Data switches* act as hubs for the LANs of Ethernet ports on TOPS nodes (such as DMS switches, TOPS operator positions, servers, and other nodes used by TOPS). Data switches should be used instead of passive hubs to minimize latency and maximize throughput.
- *Routers* connect the LANs served by data switches to wide area backbone networks, and they direct data between TOPS nodes.

- The *backbone* provides wide area transport, which links geographically-distributed host and remote switches, servers, and other nodes. Backbone implementation uses technologies such as asynchronous transfer mode (ATM), Frame Relay, or point-to-point facilities.

***Note:*** Figure 3 does not address practical network considerations such as redundant connections to the data switches and the backbone. For more information, refer to Chapter 7: "TOPS-IP engineering guidelines," and Appendix C: "TOPS-IP Network Configuration."

Engineering the managed IP network for TOPS has the following objectives:

- to handle all IP traffic for a specified operator call volume
- to provide low latency for data traffic and especially for voice traffic
- to provide low message loss for voice packets and especially for call control messages

## Capabilities of TOPS-IP

The TOPS-IP product implements call processing, provisioning, and maintenance over an integrated IP infrastructure. Three TOPS-IP applications use the IP infrastructure:

- Operator Centralization (OC-IP)
- IP Operator Positions (IP position)
- Queue Management System Management Information System (QMS MIS-IP).

This section introduces the capabilities of each application. Further details are in the separate chapters that discuss each application.

***Note:*** The OC-IP and IP position applications can share the resources of a single IP-XPM, although each 7X07 Gateway card must be dedicated to one application or the other. Because of the high messaging throughput and burstiness of the QMS MIS-IP application, it requires a dedicated IP-XPM.

### TOPS OC-IP application

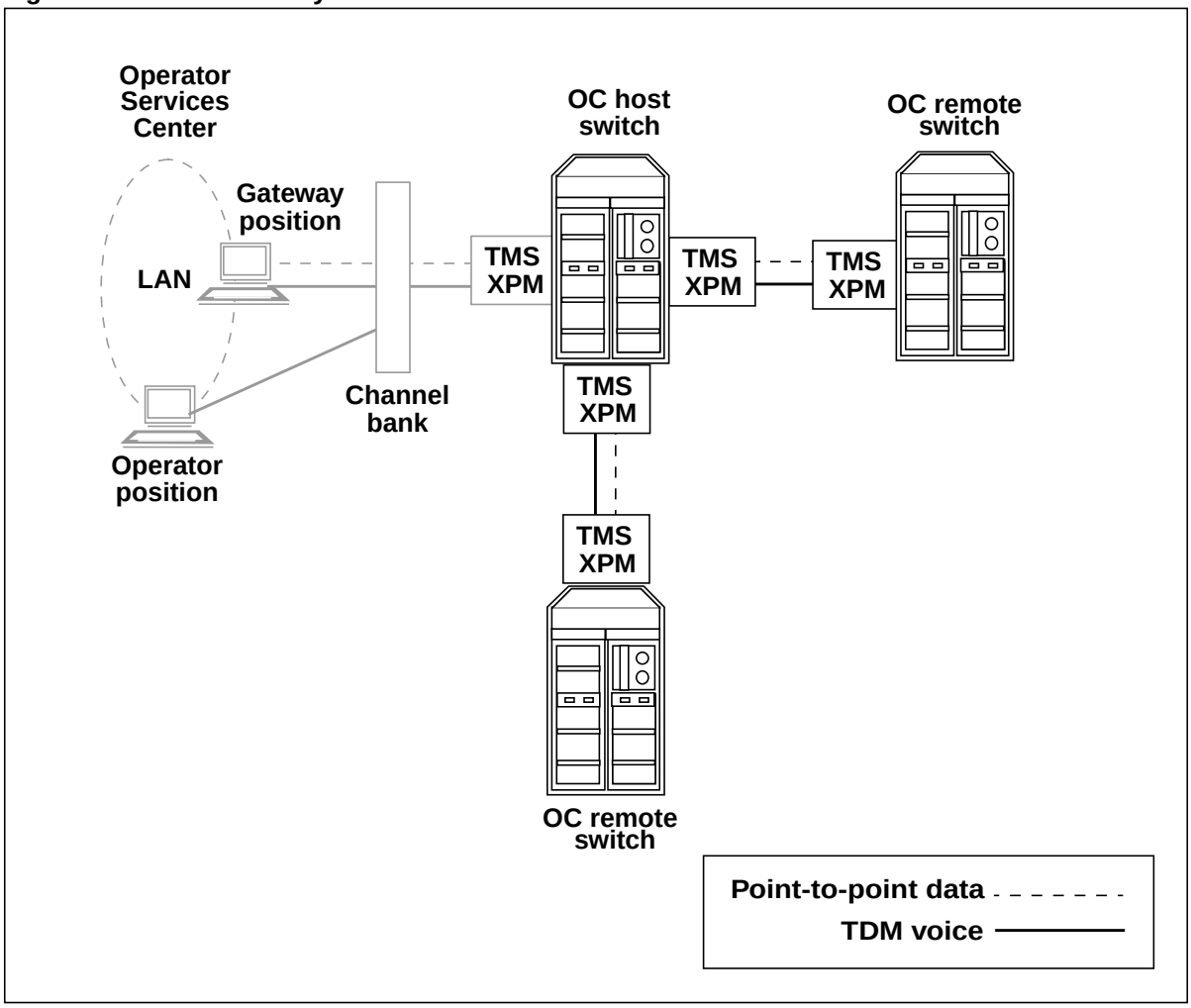
In a centralized operator network, a number of TOPS remote switches share the operator positions provided by a TOPS host switch. Calls originate in a remote switch, which is responsible for call control. The host switch provides the operator positions and is responsible for call and agent queue management, force management, and position maintenance.

Traditionally the OC host and OC remote communicate over voice links and data links to process a call. The OC voice links provide a speech path between the operator in the host and the calling and called parties in the remote. In a traditional configuration, each call must have a *dedicated* voice link while the operator services the call. The OC data links are used for call control messages, key function messages, and screen update messages. One data link can be shared by many calls in progress.

## OC connectivity without TOPS-IP

Figure 4 shows an example of a traditional, simple OC network. In the figure, OC data and voice connectivity are provisioned point to point between the remotes and the host through XPM peripherals. Data communication is through dedicated point-to-point data links. Voice communication is through nailed-up TDM trunks.

**Figure 4 OC connectivity without TOPS-IP**

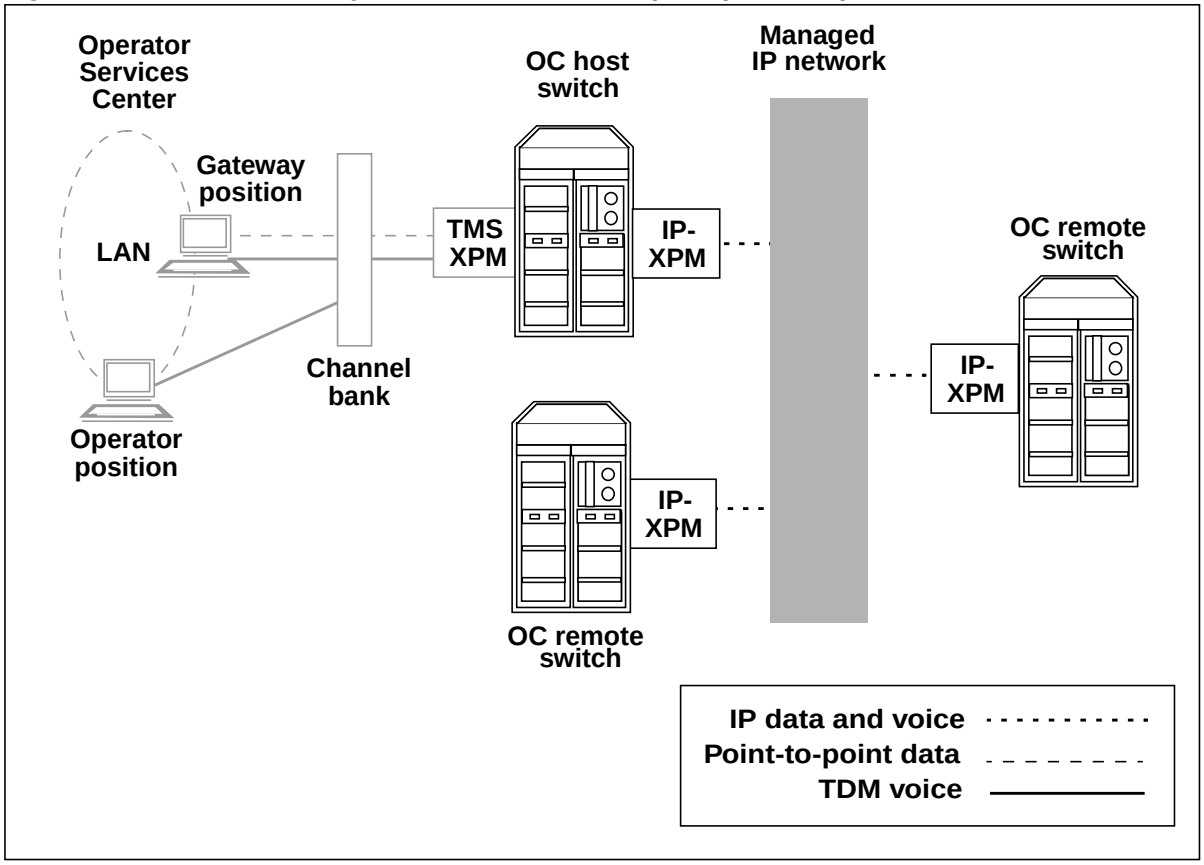



***Note:*** Although not shown in the figure, the three TOPS switches are also connected to the PSTN in the traditional way.

## OC connectivity with TOPS-IP (TDM positions)

Figure 5 shows an example of a simple OC-IP network. With OC-IP, the IP-XPM provides a common IP infrastructure to replace the point-to-point provisioning of data and voice between OC switches. All OC data and voice traffic is transported over the managed IP network; however, operator positions still have TDM connectivity with the OC host switch.

**Figure 5 OC-IP connectivity in a TOPS-IP network (TDM positions)**




***Note:*** Although not shown in the figure, the three TOPS switches are also connected to the PSTN in the traditional way.

## Benefits of OC-IP

OC-IP adds flexibility to the configuration and management of the OC network. Because connections between OC hosts and OC remotes are logical rather than physical, the traffic from a remote can be moved to another host more easily. The integration of voice and data allows OC-IP to take advantage of high bandwidth wide area networks (WAN) for cost-effective transport.

In addition, when IP positions are used in conjunction with OC-IP, the logical voice connection is directly between the OC remote and the position, bypassing the host. This means that 7X07 Gateway resources are not used in the host for OC-IP calls that also use IP positions.

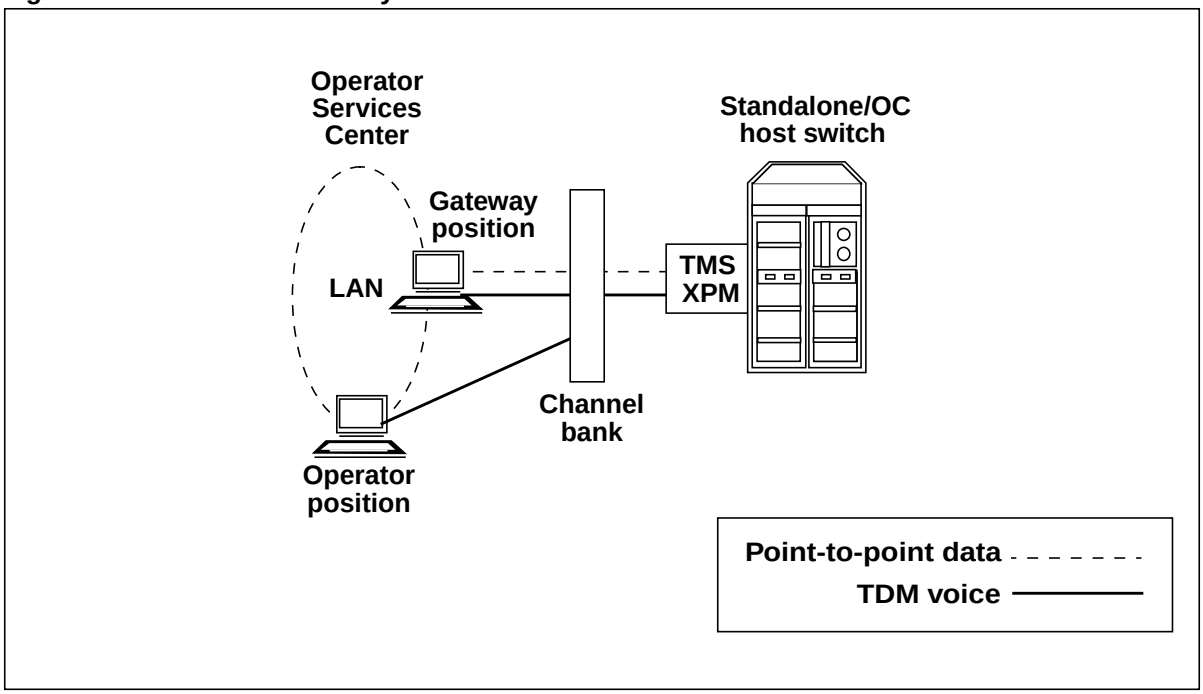
## TOPS IP position application

In a TOPS network, teams of TOPS operators service a variety of calls from the public switched telephone network (PSTN). Operator positions located at Operator Services Centers (OSC) communicate voice and data with the TOPS switch, which is responsible for call control, call and agent queue management, force management, and operator position maintenance.

### Position connectivity without TOPS-IP

Figure 6 shows an example of a traditional, simple TDM-based network of operator positions. In the figure, the dedicated TDM voice path to the position is through a TOPS Message Switch (TMS) XPM peripheral and a channel bank. The data path is also through a TMS and a channel bank, but it must pass through a gateway position, which transmits data to and from the other positions on the LAN. The gateway position is also responsible for maintenance of the positions in its cluster.

**Figure 6 Position connectivity without TOPS-IP**




***Note:*** Although not shown in the figure, the TOPS switch is also connected to the PSTN in the traditional way.

### Position connectivity with TOPS-IP

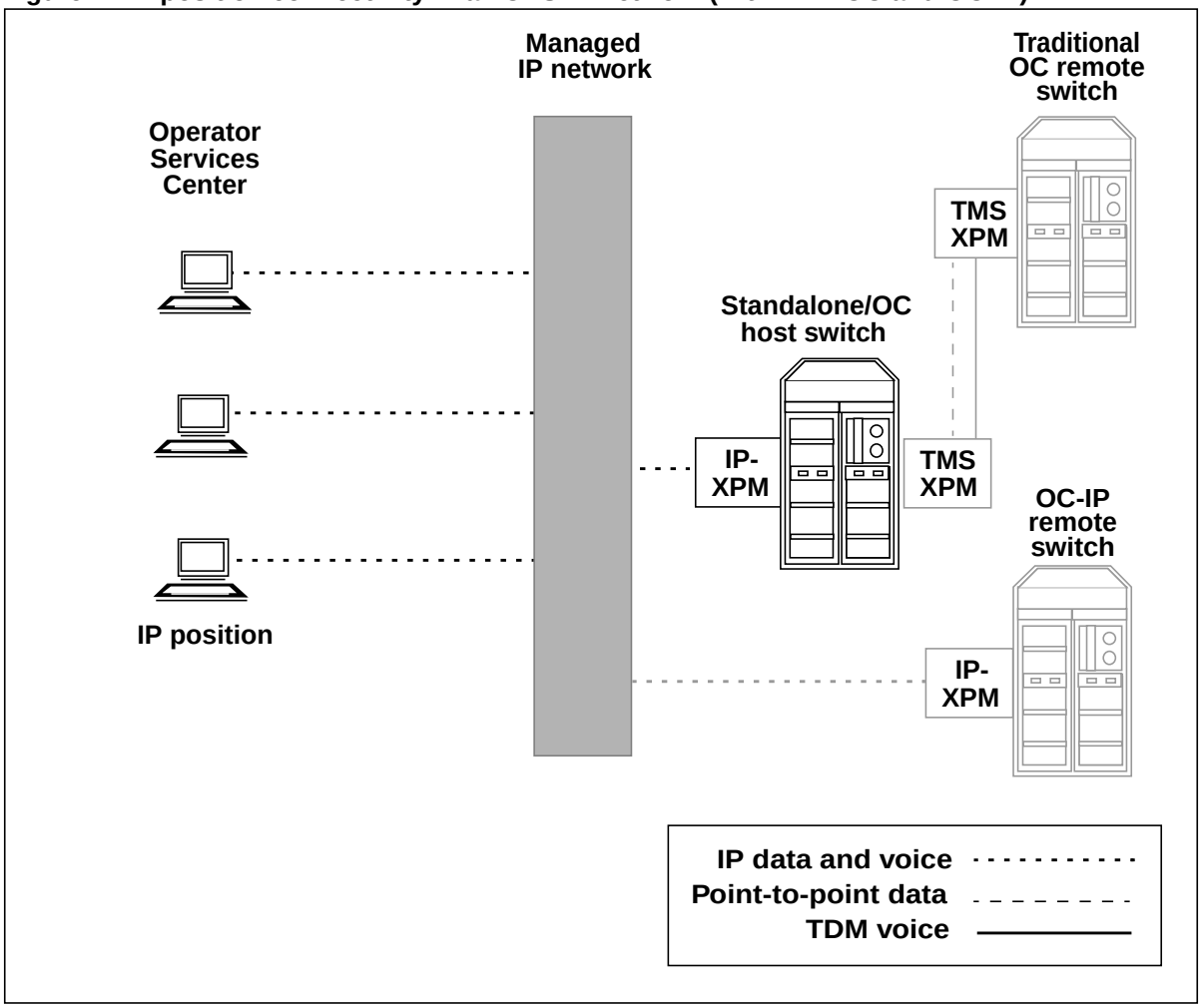
IP positions have IP data and voice connectivity to the managed IP network, and they use this connectivity to communicate with TOPS-IP switches.

The common IP infrastructure replaces the point-to-point provisioning of data and voice between a TOPS switch and an operator position. The IP positions are still part of a LAN (Ethernet, not token ring). The LAN is considered to be part of the managed IP network.

Figure 7 shows an example of a simple TOPS-IP network with IP positions and TOPS switches. The positions are datafilled and maintained at the standalone/OC host switch, and they can process standalone TOPS calls that route to that switch. They can also process calls routed to the two OC remote switches (one traditional and one OC-IP).

Note: As of SN08, TDM OC links must be replaced by OC-IP links.

**Figure 7 IP position connectivity in a TOPS-IP network (with TDM OC and OC-IP)**




***Note:*** Although not shown in the figure, the TOPS switches are also connected to the PSTN in the traditional way.

### Benefits of IP positions

Because IP positions do not require all the specialized hardware of traditional IWS positions, more attractive pricing arrangements are possible. IP positions also eliminate the need for channel banks in the OSC, and for gateway positions with maintenance and data messaging responsibility for other positions. The integration of voice and data allows IP positions to take advantage of high bandwidth wide area networks (WAN) for cost-effective transport.

Use of IP positions adds flexibility to the configuration of OSCs and to management of the operator workforce. It is easier both to set up new OSCs and to relocate positions within an existing OSC. And since connections between positions and switches are logical rather than physical, it is possible for a position to be brought into service at different switches (at different times) without moving the positions or re-wiring the connections.

When IP positions are used in conjunction with OC-IP, the logical voice connection on OC calls is directly between the OC remote and the position, bypassing the host. This means that 7X07 Gateway resources are not used in the host for OC-IP calls that also use IP positions.

## TOPS QMS MIS-IP application

***Note:*** This application is not currently supported. Customers with an interest in the application should discuss it with their QMS MIS vendors and with TOPS Marketing.

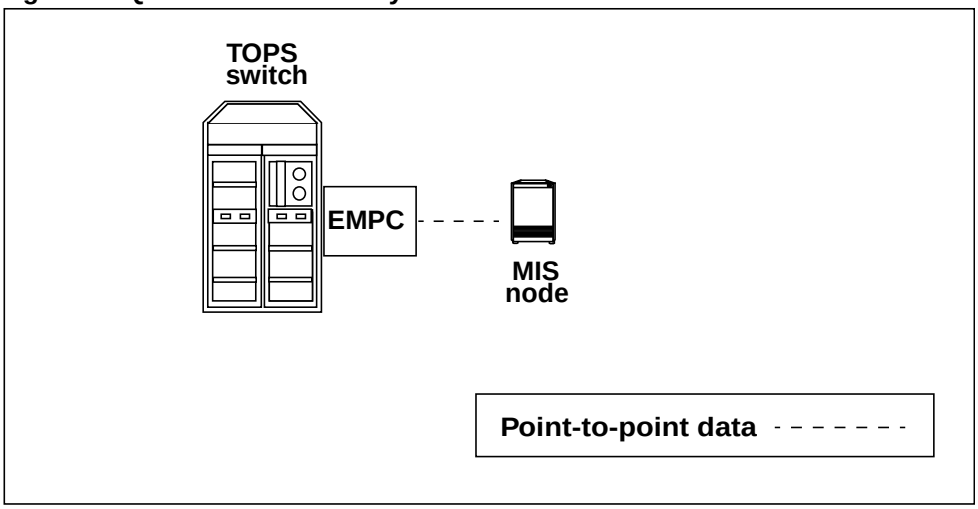
TOPS QMS MIS is a switch application that collects event-driven data about TOPS calls and positions. The switch sends this data to an external reporting facility, such as an MIS vendor node. The external facility may use the data to provide real time displays and report statistics on call queues and operator positions. The flow of QMS MIS data is one-way only, from the switch to the MIS node.

### QMS MIS connectivity without TOPS-IP

Figure 8 illustrates the traditional connectivity for TOPS QMS MIS. Data connectivity is through a point-to-point (X.25) interface and an enhanced multiprotocol controller (EMPC) card.

***Note:*** TOPS QMS MIS connectivity differs from OSSAIN QMS MIS connectivity. OSSAIN QMS MIS provides data about OSSAIN sessions and queues, and it uses an Ethernet interface unit (EIU) at the switch rather than an EMPC. The TOPS-IP product does not change the existing OSSAIN QMS MIS functionality or connectivity.

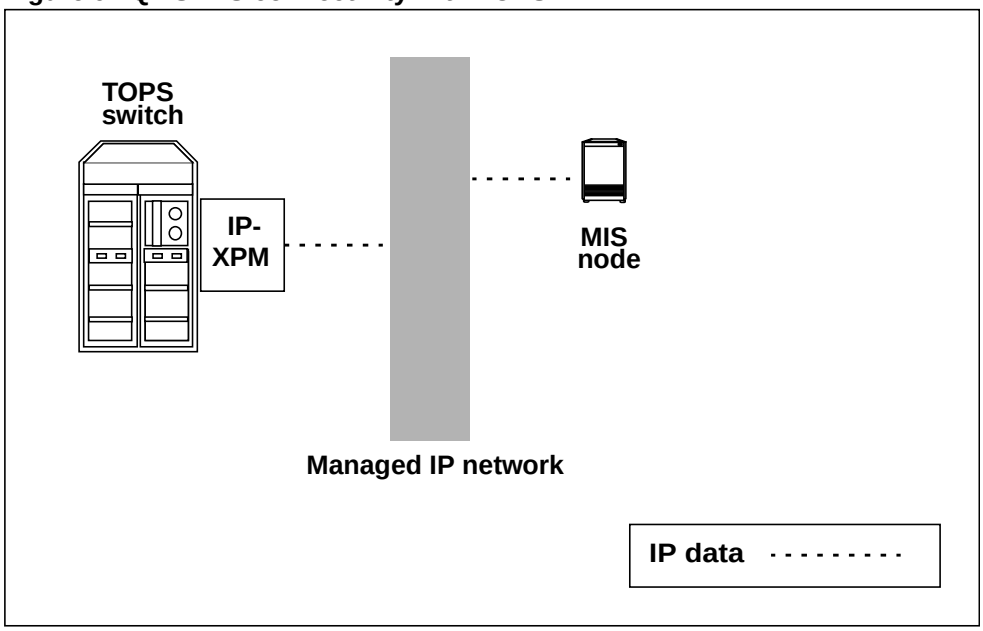
**Figure 8 QMS MIS connectivity without TOPS-IP**




## QMS MIS connectivity with TOPS-IP

Figure 9 illustrates QMS MIS-IP connectivity in a TOPS-IP network. The common IP infrastructure replaces the provisioning of X.25 data for the TOPS QMS MIS-IP application.

**Figure 9 QMS MIS connectivity with TOPS-IP**




***Note:*** TOPS QMS MIS-IP requires a dedicated IP-XPM. This IP-XPM cannot be used to support other TOPS-IP applications such as OC-IP and IP positions. It need not contain any 7X07 Gateway cards, since the Gateways are used for voice.

### Benefits of QMS MIS-IP

With QMS MIS-IP, the TOPS switch can have up to two TCP connections that transmit the same MIS data across the network. This capability allows the TOPS switch to send MIS data to more than one vendor or to increase the reliability of the MIS data sent to a single vendor.

## Information road maps

For detailed information on the TOPS-IP product as well as on related topics, refer to the following road maps.

### TOPS-IP road map

The following list points to specific TOPS-IP user information in this book:

- Chapter 2 describes the infrastructure for integrated IP data and voice communication.
- Chapter 3 provides details on the OC-IP application.
- Chapter 4 provides details on the IP position application.
- Chapter 5 provides details on the TOPS QMS MIS-IP application.
- Chapter 6 discusses the limitations and restrictions of TOPS-IP capabilities in the network.
- Chapter 7 provides information on planning and engineering for TOPS-IP, focusing on requirements for performance, capacity, and provisioning.
- Chapter 8 describes datafill requirements for TOPS-IP. It focuses on the CM datafill needed to provision the IP infrastructure and TOPS-IP applications.
- Chapter 9 discusses ordering codes for the TOPS-IP product.
- Chapter 10 describes DMS switch maintenance activities associated with TOPS-IP applications.
- Chapter 11 describes related command interface (CI) tools.
- Chapter 12 shows examples of switch log reports.
- Chapter 13 shows examples of switch operational measurements (OM).
- Appendix A provides procedures used to install and configure the Dynamic Host Configuration Protocol (DHCP) server for TOPS-IP.
- Appendix B discusses TOPS-IP support for Simple Network Management Protocol (SNMP).
- Appendix C provides practical information to assist in planning and configuring the TOPS-IP data network.
- Appendix D is a quick reference for IWS configuration information that is mentioned in this book.

The following reference provides information about IP capabilities and configuration of the IWS operator workstation:

- *TOPS IWS Base Platform User's Guide*, 297-2251-010

## Related information road map

The following list points to other sources of related information:

- For information on the Enhanced Network (ENET) interface, refer to *Networks Maintenance Guide*, 297-1001-591.
- For details on IP networking, refer to any standard industry book, such as *Internetworking with TCP/IP*, by Doug E. Comer (Prentice Hall).
- For details on SNMP-based network and internetwork management, refer to any standard industry book, such as *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*, by William Stallings (Addison-Wesley).
- For details on recommendations for telecommunications, refer to the following International Telecommunication Union (ITU) documents:
  - ITU-T (G.711), *Pulse Code Modulation of Voice Frequencies*
  - ITU-T (G.723.1), *Dual Rate Speech Coder for Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s*
  - ITU-T (H.323), *Packet-based Multimedia Communications Systems*

***Note:*** These and other ITU-T documents can be accessed at the following Web site: www.itu.int.

- For details on standards and specifications for the Internet, refer to the following Request for Comments (RFC) documents:
  - RFC768 (STC 6) *User Datagram Protocol*
  - RFC791 (STD 5) *Internet Protocol*
  - RFC792 (STD 5) *Internet Control Message Protocol*
  - RFC793 (STC 7) *Transmission Control Protocol*
  - RFC951 *Bootstrap Protocol*
  - RFC1157 (STD 15) S*imple Network Management Protocol*
  - RFC1213 *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
  - RFC1643 *Definitions of Managed Objects for the Ethernet-like Interface Types*
  - RFC1889 *RTP: A Transport Protocol for Real-Time Applications*
  - RFC2131 *Dynamic Host Configuration Protocol*
  - RFC2338 *Virtual Router Redundancy Protocol*
  - RFC2543 *SIP: Session Initiation Protocol*

***Note:*** These and other RFC documents can be accessed at the Internet Engineering Task Force (IETF) Web site: www.ietf.org.

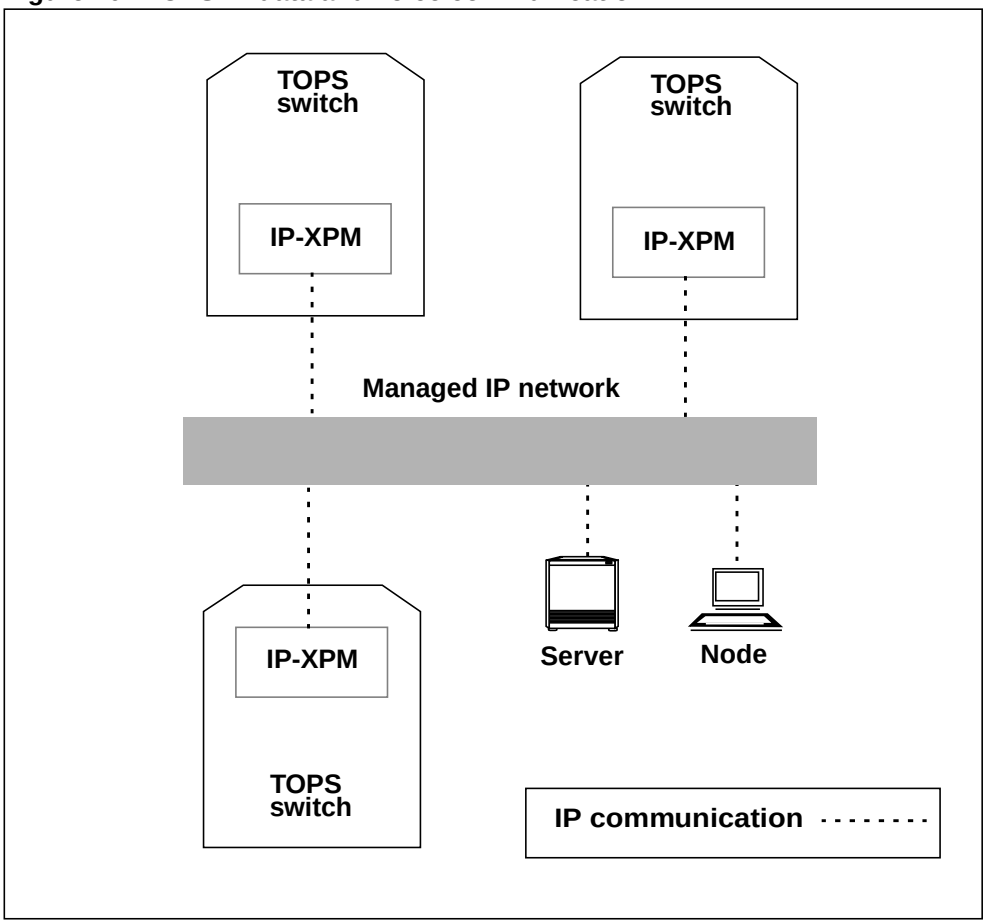
# Part 2: Functional description

Part 2: Functional description includes the following chapters:

# Chapter 2: TOPS-IP data and voice communication

As discussed in Chapter 1, the common IP infrastructure integrates data and voice packet delivery for TOPS-IP applications. The IP-XPM component of the infrastructure, with its IP-specific circuits, provides the necessary interfaces for data and voice communication between nodes over the managed IP network. Refer to Figure 10 for a simple topology.

**Figure 10 TOPS-IP data and voice communication**



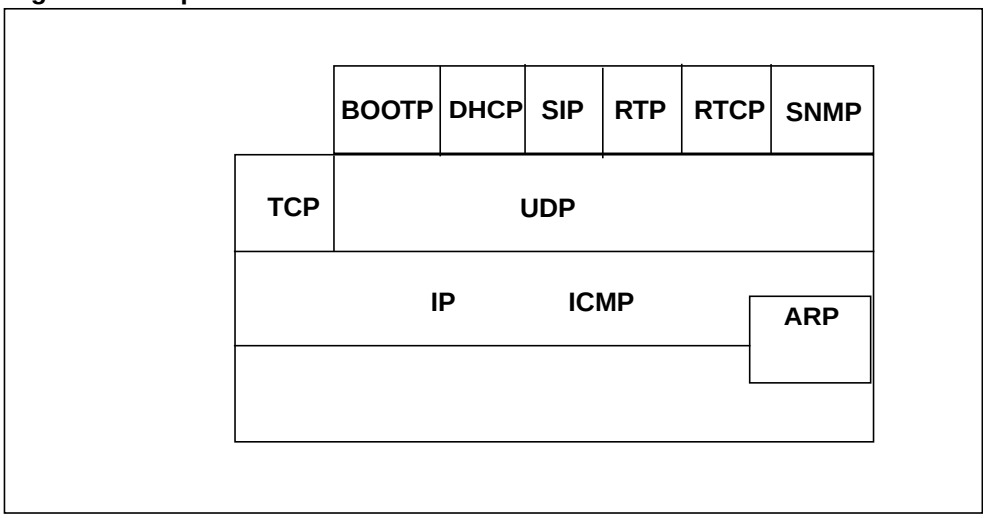
This chapter discusses how the IP-XPM provides data and voice communication, focusing on the following areas:

- overview of the IP protocol suite
- IP data communication infrastructure
- IP voice communication infrastructure
- overview of the switch datafill for IP data and voice

## Overview of the IP protocol suite

Figure 11 shows the IP protocol stack that resides on the IP-XPM. A brief description of each protocol follows the figure.

**Figure 11 IP protocol stack on the IP-XPM**




- Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP). BOOTP and DHCP use servers to configure nodes in the network with necessary IP information (IP addresses, subnet masks, routers).
- Session Initiation Protocol (SIP) is a signaling protocol for creating, modifying and terminating sessions with one or more participants. The sessions include multimedia conferences, IP telephone calls, and multimedia distribution.
- Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP). RTP is used to transport data with real-time characteristics, including audio and video. RTCP augments RTP to allow monitoring of data delivery and to provide minimal control and identification.
- Simple Network Management Protocol (SNMP). SNMP is used to manage and monitor network activity and performance.

- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are used at the transport layer. TCP is a connection-oriented protocol that builds on the underlying IP delivery service. TCP adds reliability through sequencing, timeouts, and retransmissions. It provides acknowledgments and checks for missing, out-of-sequence, and duplicated packets.

  UDP is a connectionless protocol that permits packets to be sent with a minimum of protocol overhead. With UDP, message delivery is not guaranteed. It provides neither acknowledgments nor checks for missing, out-of-sequence, or duplicated packets.

- IP and Internet Control Management Protocol (ICMP) are used at the network layer. IP is the delivery service of the IP suite. ICMP provides an echo transaction (ping).

- Address Resolution Protocol (ARP) is used at the data link layer to associate the IP address with a physical address.

## IP data communication infrastructure

IP data communication, provided by the SX05DA processor card in the IP-XPM, allows the TOPS switch to send and receive data traffic over the managed IP network. Data communication interfaces in the IP-XPM give the switch the following capabilities:

- It can perform IP addressing and configuration for the XPM.
- It can perform port and service configuration for TOPS-IP applications.
- It can use the standard IP messaging protocols.

### SX05DA functions

The SX05DA card, which replaces the MX77 unified processor, has a full-duplex 10/100 Megabit per second (Mbps) Ethernet port through the backplane. One SX05DA card is provisioned in each unit of an IP-XPM, for a total of two.

The SX05DA performs the following functions for each unit of the IP-XPM:

- It provides the main processing, including CPU, MMU, boot and ROM-level memory, program memory, and data memory.
- It communicates with the other circuit packs of the unit through the A-bus.
- It provides unit activity control.
- It provides the mate unit interface.
- It provides two receptacle sockets for additional enhancements to the processor.

***Note:*** Each SX05DA card requires a Flash Memory Packlet (SX06BA), which is used in IP-XPM recovery.

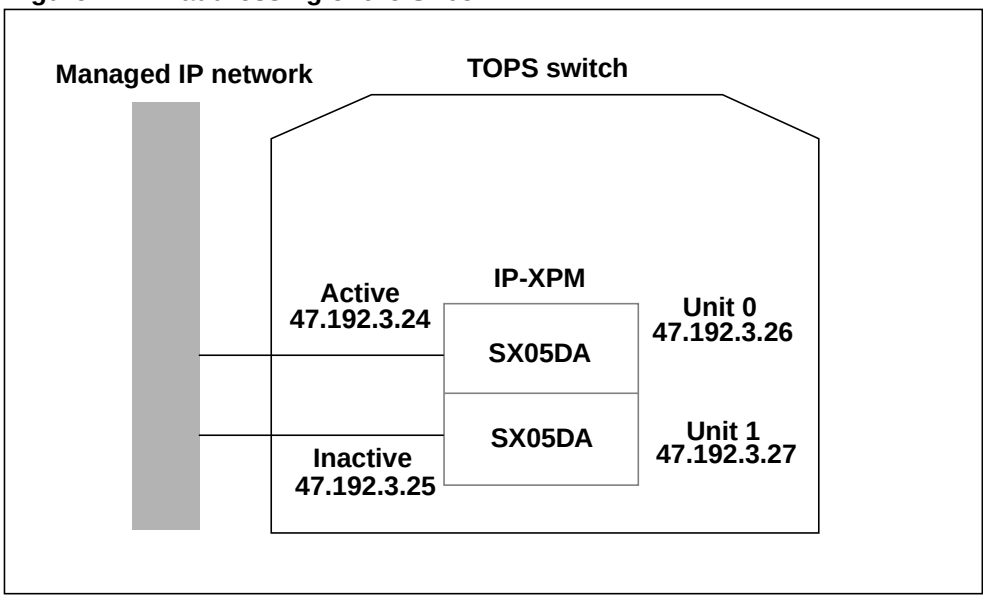
## IP addressing of the SX05DA card

IP addresses are used to route IP packets to the correct node on the network. These addresses must be assigned to hardware before any messaging can occur.

The SX05DA serves as an IP-addressable network endpoint. The SX05DA and the CM appear as a *single entity* to other nodes on the network.These nodes use the IP address of the SX05DA to route messages to CM applications.

A single IP-XPM peripheral consists of two units, unit 0 and unit 1. One SX05DA card corresponds to one unit, for a total of two SX05DA cards per IP-XPM. Each SX05DA card has a single Ethernet interface with a fixed MAC (media access control) address. Only one SX05DA is active at a time and the other is in standby mode. Figure 12 shows IP addressing of the SX05DA cards.

**Figure 12 IP addressing of the SX05DA**




As shown in the figure, one IP address is used by the active SX05DA and another IP address is used by the inactive SX05DA. Also, the SX05DA software internally assigns IP addresses to unit 0 and unit 1. So, IP addressing of the SX05s requires a block of *four consecutive* IP addresses.

The last octet of the first address must be divisible by four, for example, 47.192.3.24. This address is bound to the current active unit, and is always used to address the IP-XPM, even after it initializes or switches activity (SWACT). For the IP-XPM, the available base address range for the last octet is from 4 to 248.

The other three addresses are bound as follows:

- second address (N+1) is bound to the inactive unit
- third address (N+2) is bound to Unit 0
- fourth address (N+3) is bound to Unit 1

### Gratuitous ARP broadcast message

When the IP-XPM initializes or SWACTs, it dynamically swaps the active/inactive IP addresses of its two units to ensure that the current active unit is addressed correctly. Then, the IP-XPM sends a gratuitous Address Resolution Protocol (ARP) broadcast message to notify local hosts that the swap occurred.

### Port assignments

Software ports are used in routing messages to the correct application after the correct node on the network has been reached. These ports are unrelated to hardware ports, and are assigned as applications need them.

The managed IP network can use port assignments to manage the quality of service for applications. Refer to Chapter 7: “TOPS-IP engineering guidelines” for more information including recommended port values.

## Bootstrapping and configuring the SX05DA card

When the IP-XPM initializes, specific IP information—such as IP addresses, subnet masks, and gateway routers—is needed to configure the IP stack on the XPM. Datafill in the switch table XPMIPMAP (XPM IP Mapping) identifies which configuration method to use for a particular IP-XPM when it is brought into service, as follows:

- DHCP method
- CM method

### DHCP method

- With the DHCP method (also referred to as the *network* method), the IP-XPM receives IP information from a network server other than the CM. The DHCP server provides the IP-XPM with the following information:
- the IP addresses of both units
- the subnet mask for the local network, which is used to determine the broadcast address

Also, the server may provide the following optional information:

- the IP address (or addresses) of the default gateway router, if IP data will be routed to other networks
- the IP address (or addresses) of the DNS server and the default domain name, if DNS is provided

### CM method

With the CM method, the necessary IP information comes from additional datafill in table XPMIPMAP and from gateway router datafill in table XPMIPGWY (XPM IP Gateway). This information is downloaded from the CM to the IP-XPM when it is brought into service. (Refer to page 51 for more details on this CM datafill.)

***Note:*** The term *gateway* in the context of routers does *not* refer to the 7X07 Gateway card in the IP-XPM. A gateway router is a component of the managed IP network and is used to forward IP packets to other networks.

## SX05DA redundancy

The IP-XPM contains duplicates of all components that are used for IP data links. Each of the two mated units has its own SX05DA card and its own Ethernet LAN interface. For more information on redundancy issues, refer to "IP-XPM maintenance, diagnostics, and troubleshooting" on page 322 and to Chapter 7: "TOPS-IP engineering guidelines."

## MX76DA messaging

The MX76DA messaging card supports the bandwidth requirements for enhanced C-side 14 messaging between the CM and the IP-XPM. C-side 14 messaging requires ENET, DS512 fiber links to the IP-XPM, and the NT6X40FC network interface card.

## IP transport services

IP networks provide transport services to applications. A transport service is defined by assigning it a name, a software port number, and a transport-layer protocol. After the appropriate transport services have been defined, an application can specify which one it wants to use.

For example, Web browsers use a transport service named "HTTP" (Hypertext Transfer Protocol), and the HTTP service is most often defined to use port 80 and the TCP or UDP protocol. TOPS-IP applications use transport services that are datafilled in the switch table IPSVCS (IP Services). For information on how each TOPS-IP application uses IP transport services, refer to the separate chapter on the application.

## Ports

Ports associated with IP transport services are used in routing messages to the correct application after the correct node on the network has been reached. For information on how each TOPS-IP application uses port values, refer to the separate chapter on the application.

## Sockets

An IP connection endpoint is represented by a socket, which is a software entity identified by an IP address and a port, for example, 47.192.3.40:8600.

### Communication identifier (COMID)

Local data link connectivity information is represented by a COMID, which is datafilled against the data link. COMIDs, introduced by TOPS-IP data communication software, are not transmitted over the IP network. While it is not an industry-standard entity, the COMID is recognized by the IP-XPM and by the CM, where it is visible in datafill, logs, and OMs. For information on how each TOPS-IP application uses COMIDs, refer to the separate chapter on the application.

### Remote socket interface (RSI)

TOPS-IP CM applications use the IP-XPM as a proxy to the managed IP network. The applications communicate with the network by exchanging RSI messages with the XPM. The XPM invokes the RSI calls made by the applications.

## IP voice communication infrastructure

IP voice communication, provided by the 7X07AA Gateway card in the IP-XPM, allows the TOPS switch to send and receive packetized voice traffic over the managed IP network. Voice communication interfaces in the IP-XPM give the switch the following capabilities:

- It can convert between TDM voice and packetized voice.
- It can use industry-standard codecs and VoIP signaling.
- It can support up to 480 simultaneous voice connections on each IP-XPM.

  ***Note:*** C-side and inter-mate link capacities, however, may not allow use of all 480 connections for TOPS-IP applications. Details are in Chapter 7: “TOPS-IP engineering guidelines.”

### 7X07AA functions

The 7X07AA Gateway card represents an integrated P-side node that has characteristics of both a P-side interface card (such as the 6X50) and a subtending node. Each card can support 48 voice connections.

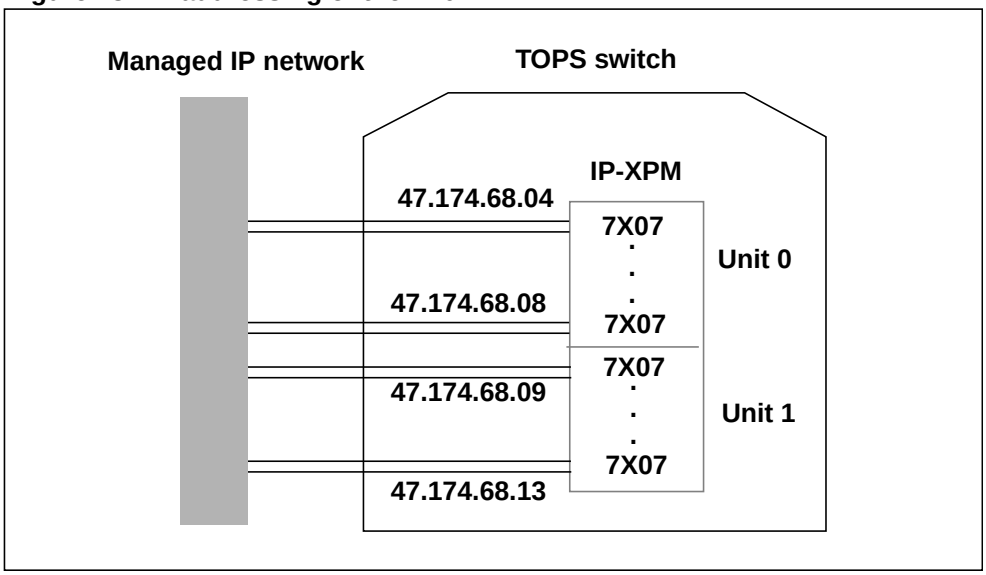
As with the 6X50 interface cards, all 7X07 Gateway cards provisioned in an IP-XPM are used by the active unit regardless of the physical unit location of the cards. They perform the following functions for the IP-XPM:

- They provide packetized voice over the network.
- They provide call setup signaling associated with the voice connections in the network.

## IP addressing of the 7X07AA card

The 7X07AA card has two Ethernet interfaces, only one of which is active at a time. One IP address and one MAC address are used by the active Ethernet interface. Figure 13 shows IP addressing of the 7X07AA cards.

**Figure 13 IP addressing of the 7X07AA**




### Port assignments

Port values for the 7X07AA card are fixed. The managed IP network can use these port assignments to manage the quality of service for voice traffic. Refer to Chapter 7: "TOPS-IP engineering guidelines" for information on port values used by the 7X07AA card.

## Loading and configuring the 7X07AA card

A DHCP server is required to configure the 7X07AA Gateway cards. This server provides each Gateway card with its loadfile name and IP address. For information on using the DHCP server, refer to Appendix A: "DHCP server guidelines."

## 7X07AA redundancy

The 7X07 Gateway cards should be provisioned for N+1 redundancy for each voice link group. For more information on redundancy issues, refer to Chapter 7: "TOPS-IP engineering guidelines."

## Protocols for voice over IP (VoIP)

For the voice media stream and its associated control packets, the TOPS-IP product uses the industry-standard RTP and RTCP protocols.

There are two competing industry standards for VoIP call signaling: SIP and signaling protocols from the H.323 suite. The Gateway card uses industry-standard SIP when signaling with IP positions. When signaling with another 7X07 Gateway, it uses a streamlined subset of SIP.

## Voice encoding and packetization

For voice encoding, TOPS-IP applications use industry-standard audio codecs. A codec, or coder/decoder, is used to transform speech data from one representation to another. These transformations are used in audio applications to compress and decompress speech data in order to lower bandwidth requirements. The 7X07 Gateway is capable of transcoding between supported TOPS-IP codecs.

In addition, the 7X07 gateway provides a voice packetizer. The packetizer's function is to convert between coded TDM and packetized speech data.

As an example, a TOPS-IP voice link could be G.711 mu-law encoded on the TDM side and G.723 encoded on the IP network side. The 7X07 gateway receives the G.711 TDM sample from the DMS network, transcodes to G.723, and then packetizes the sample for transmission over the TOPS-IP network. Incoming packetized G.723 samples are first converted to TDM samples, transcoded to G.711, then sent back to the TDM side of the connection.

TOPS-IP applications support the following codecs:

- G.711 Mu-law (uncompressed)
- G.711 A-law (uncompressed)
- G.723 (compressed)

G.711 provides carrier grade voice if quality of service requirements for the IP network are met. G.723 requires considerably less bandwidth while still attempting to provide acceptable voice quality. Testing in Nortel Networks labs indicates that many people can distinguish between G.711 and G.723, but most do not notice the difference unless specifically asked to focus on it. Service providers are encouraged to try both and reach their own conclusions.

Codec selection for TOPS-IP applications is determined by CM datafill and, for applications that support auto-compression, by network conditions.

***Note:*** Refer to Chapter 4: "TOPS IP position application" for information about auto-compression.

Regardless of the codec selection, all TOPS-IP applications use UDP at the transport layer for voice packets.

## Dynamic trunking

Dynamic trunking is the method used by DMS switch trunking applications to send voice traffic over a data packet protocol. With dynamic trunking, there is no fixed connection to the far end. In fact, when the trunk is not in use, there is no far end.

Dynamic trunk members resemble TDM trunks from a CM perspective, but with a few exceptions as described in the following paragraphs.

### Trunk member datafill

The 7X07 Gateway does not keep track of its individual C-side trunk member states. So to prevent the possibility of the Gateway presenting a call on an incoming circuit that has not been datafilled in the CM, all possible members of the card must be datafilled in the CM. The switch accomplishes this by automatically datafilling blocks of trunk members when the Gateway card is datafilled. Manual additions and deletions of individual trunk members are *not* allowed for TOPS dynamic trunk groups.

### Trunk member maintenance

Because the Gateway does not keep track of the C-side states of the members, the state of the Gateway itself determines the state of each trunk member as viewed from the CM. So members cannot be individually maintained at the MAPCI;MTC;TRKS;TTP level. Instead, when the Gateway on the IP-XPM is maintained from the MAPCI;MTC;PM level, the CM states of the associated trunk members are automatically updated. It is possible to post trunk members at the TTP level of the MAP and view their states and connections.

***Note:*** Many TTP level commands are not supported for dynamic trunks. For a list of supported and unsupported commands, refer to Chapter 10: "TOPS-IP maintenance activities."

### Usage limits

Although TOPS-IP dynamic trunk groups are datafilled and maintained in blocks of 48 trunks, users can reduce through datafill the total number of dynamic trunks used in call processing. Refer to "Limiting the use of dynamic voice links" on page 200 for details.

### Carrier maintenance

The switch views the 7X07 Gateway as a remote node with respect to carrier maintenance. So the commands and functions that may be used at the MAPCI;MTC;TRKS;CARRIER level correspond to those of a standard remote carrier. As with trunk members, it is possible to post and view carriers from the CARRIER level.

***Note:*** For a list of supported and unsupported carrier states, refer to Chapter 10: "TOPS-IP maintenance activities."

### ISUP call processing

From the CM perspective, dynamic voice trunks appear as ISUP trunks that use the Q.764 protocol. This capability takes advantage of the existing ISUP signaling interface between the CM and the IP-XPM.

Traditional ISUP call processing routes and receives messages from the SS7 network through the LIU7. Also, some dynamic trunking applications other than TOPS-IP ones may use the SS7 network for call control (and either IP or ATM for bearer).

However, TOPS-IP applications do not use the LIU7 or the SS7 network. They route and receive messages through the IP-XPM, which handles TOPS-IP calls differently from SS7 ISUP calls. The 7X07 Gateway card in the IP-XPM converts both the ISUP call control and the voice into data packets for the managed IP network.

## Overview of datafill for IP data and voice infrastructure

This section introduces the switch datafill needed to provision the IP data and voice infrastructure for TOPS-IP. It discusses both new and existing tables and gives example datafill.

***Note:*** Application-specific information about how the infrastructure tables are used is in the individual chapters that discuss the applications (along with other application-specific tables). Details on table dependencies and the range of valid datafill for every table affected by TOPS-IP are in Chapter 8: "TOPS-IP data schema."

The tables are described in the following order:

1 Hardware provisioning tables:
   - LTCINV (Line Trunk Controller Inventory)
   - CARRMTC (Carrier Maintenance)
   - LTCPSINV (LTC Peripheral-side Inventory)

2 Data provisioning tables:
   - XPMIPGWY (XPM IP Gateway)
   - XPMIPMAP (XPM IP Mapping)
   - IPSVCS (IP Services)
   - IPCOMID (IP Communication Identifier)

3 Voice provisioning tables:
   - CLLI (Common Language Location Identifier)
   - TRKGRP (Trunk Group)
   - TRKSGRP (Trunk Subgroup)
   - TRKOPTS (Trunk Options)
   - SITE (Site)
   - IPINV (IP Inventory)
   - TRKMEM (Trunk Members)
   - TOPSTOPT (TOPS Trunk Options)
   - OFCENG (Office Engineering)
   - PKTVPROF (Packetized Voice Profile)

### LTCINV

Table LTCINV specifies hardware inventory information for each IP-XPM (excluding the P-side link assignments). Datafill values include the IP-XPM type and number and other data associated with its processors, C-side links, and software loads.

For TOPS-IP applications, the IP-XPM must be a DTC. The following other fields also require datafill specific to TOPS-IP:

- LOAD (for the QTP22 load, or latest)
- OPTCARD (MX76C14 HOST, for the messaging card)
- TONESET (NORTHAA)

  ***Note:*** This value is required only to satisfy table control and diagnostics. The IP-XPM does not use this toneset to generate tones.
- PROCPEC (for the SX05DA card)
- EXTLINKS (for the C-side 14 link pairs)

  ***Note:*** The EXTLINKS value is datafilled automatically by the CONVERTCSLINKS utility.
- E2LOAD (latest IP-XPM firmware load)
- OPTATTR (CCS7)

  ***Note:*** This value is required only to satisfy table control. The IP-XPM does not use the SS7 network.
- PEC6X40 (6X40FC, for IP-XPM ENET interface)

The following example shows LTCINV datafill for three IP-XPMs.

**Figure 14 MAP display example for table LTCINV**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
------------------------------------------------------------------------
DTC 10   1001   LTE    0    51    0     C   0    6X02AF  QTP22xx (ABTRK DTCEX)$
(0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5) (0 11 0 6) (0 11 0 7)
(0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11) (0 11 0 12) (0 11 0 13) (0 11 0 14)
(0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0    6X02AF   QTP22xx (ABTRK DTCEX)$
(0 11 1 0) (0 11 1 1) (0 11 1 2) (0 11 1 3) (0 11 1 4) (0 11 1 5) (0 11 1 6) (0 11 1 7)
(0 11 1 8) (0 11 1 9) (0 11 1 10) (0 11 1 11) (0 11 1 12) (0 11 1 13) (0 11 1 14)
(0 11 1 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
DTC 20  1002   LTE    0    51    0     C   0    6X02AF   QTP22xx (ABTRK DTCEX)$
(0 27 16 0) (0 27 16 1) (0 27 16 2) (0 27 16 3) (0 27 16 4) (0 27 16 5) (0 27 16 6)
(0 27 16 7) (0 27 16 8) (0 27 16 9) (0 27 16 10) (0 27 16 11) (0 27 16 12) (0 27 16 13)
(0 27 16 14) (0 27 16 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
```

## CARRMTC

Table CARRMTC specifies maintenance control information for peripheral modules (PM), such as the DTC. Datafill values include the PM type, Gateway template name, and refinements specific to the DS-1 selector.

The alphanumeric value in field TMPLTNM (template name) is referenced by table LTCPSINV. For TOPS-IP voice applications, the following fields require specific datafill:

- CSPMTYPE (DTC)
- TMPLTNM QTP22or 7X07 Gateway cards)

  Any unique template name may be used. TGWY (TOPS Gateway) is suggested.
- ATTR (attribute) refinements:
  - — selector set to DS1
  - — card set to NT7X07AA
  - — frame format set to SF
  - — zero logic set to ZCS
  - — bit error rate base set to BPV

***Note:*** Other values for FF, ZLG, and BERB may or may not interfere with TOPS-IP functionality. The values listed here are known to work.

The following example shows carrier maintenance information for the XPM type (DTC) used for TOPS-IP voice applications.

**Figure 15 MAP display example for table CARRMTC**

```
CSPMTYPE TMPLTNM  RTSML  RTSOL  ATTR
-------------------------------------------------------------------------------
DTC      TGWY     255    255    DS1 NT7X07AA  MU_LAW SF ZCS BPV NILDL N 250 1000
50 50 150 1000 3 6 864 100 17 511 4 255
```

## LTCPSINV

Table LTCPSINV specifies the P-side link assignments that are associated with voice over IP at the DTC. Tuples in this table use the same key as table LTCINV. Datafill values include port numbers and signaling interface data for the 7X07 Gateway cards (defined in table IPINV).

Each pair of P-side links corresponds to one Gateway card (node). The lower P-side link number used for a Gateway corresponds to the port number in table IPINV (page 63).

The following example shows the P-side link assignments for DTCs 10, 11, and 20. DS-1 signaling and TGWY (template name from table CARRMTC) are datafilled for P-side links that correspond to 7X07 Gateways.

In this example, DTC 20 does not require P-side link datafill in table LTCPSINV, because it does not perform any voice over IP (for example, it is dedicated to the QMS MIS-IP application). No Gateway cards are installed, so the P-side links remain NILTYPE.

**Figure 16 MAP display example for table LTCPSINV**

```
LTCNAME   PSLINKTAB
-------------------------------------------------------------------------
DTC 10    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N) (8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 DS1 TGWY N) (13 DS1 TGWY N) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $

DTC 11    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N)(8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 DS1 TGWY N) (13 DS1 TGWY N) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $

DTC 20    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 NILTYPE) (7 NILTYPE)(8 NILTYPE) (9 NILTYPE)
(10 NILTYPE) (11 NILTYPE) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $
```

***Note 1:*** An entry in table LTCPSINV is added automatically when an XPM is datafilled in table LTCINV. All the P-side link types initially default to NILTYPE. P-side links that do not have hardware assigned must remain NILTYPE. Unequipped software-assigned P-side links generate service-affecting problems.

***Note 2:*** Until the 7X07 Gateway card has correct datafill in both table LTCPSINV and table IPINV, the IP-XPM will have inconsistent information about its packfill and so diagnostics may be affected. Table IPINV must contain the appropriate number of TOPS Gateways that correspond to the P-side links assigned in LTCPSINV.

***Note 3:*** After datafilling a new Gateway or changing the datafill for an existing Gateway, users should update the static data for the SX05DA. For details, refer to "Updating static data" on page 299.

### XPMIPGWY

Table XPMIPGWY specifies gateway router information for the SX05DA card. A gateway router is a component of the managed IP network and is used to forward IP packets to other networks. This datafill associates the IP address of a router with destination node or network IP addresses.

***Note:*** A gateway router is not the same thing as a 7X07 Gateway card.

When the CM method is used to configure the SX05DA (specified in table XPMIPMAP, page 57), the switch downloads appropriate router information from table XPMIPGWY to the IP-XPM when it is brought into service. Datafill in table XPMIPGWY is never used, however, when the DHCP method is specified.

***Note 1:*** The actual number of gateway routers to provision depends on administrative factors, network configuration, and capacity issues. For information on engineering, refer to Chapter 7: "TOPS-IP engineering guidelines."

***Note 2:*** Additional tuples in XPMIPGWY may be needed for special routing requirements.

The following example shows datafill for two tuples. In both cases, a default route is specified. A brief description of each field follows the example.

**Figure 17 MAP display example for table XPMIPGWY**

```
GWINDEX   DESTADDR       RTEMASK           GWIPADDR       METRIC
-------------------------------------------------------------------
0         0 0 0 0        0 0 0 0           47 192 3 1     0
1         0 0 0 0        0 0 0 0           47 192 3 2     0
```

***Note:*** An IP address in switch datafill consists of four octets delimited by a single space (no periods).

### GWINDEX field

GWINDEX specifies an index number. This number is referenced by table XPMIPMAP.

### DESTADDR field

DESTADDR specifies the IP address of a possible destination. The destination IP address indicates either a specific destination host or an entire destination network, depending on the value in the RTEMASK field. By convention, the default route includes both the address and mask with values of zero.

### RTEMASK field

RTEMASK specifies the mask that is applied to the destination IP address. A mask is used to determine which part of the address pertains to the subnetwork and which pertains to the host. A DESTADDR of 0.0.0.0 with a RTEMASK of 0.0.0.0 indicates a default route.

### GWIPADDR field

GWIPADDR specifies the IP address of the gateway router used to route IP data to its destination.

### METRIC field

METRIC specifies the number of hops (between routers) required to reach the gateway. A value of 0 indicates a local host, or direct route; a value greater than 0 indicates a remote gateway.

***Note:*** This field is reserved for future functionality.

## XPMIPMAP

Table XPMIPMAP specifies various IP information for the SX05DA, including the configuration method used when the IP-XPM is brought into service.

The following example shows datafill for three IP-XPMs. Both DTC 10 and DTC 11 use the CM method, so the switch downloads the IP information to the XPM. On the other hand, DTC 20 uses the DHCP method, so IP information is sent from the DHCP server in the IP network. A brief description of each field follows the example.

***Note:*** The XPMNAME, AUTONEG, and SUBNMASK fields are always downloaded to the XPM, regardless of the configuration method.

**Figure 18 MAP display example for table XPMIPMAP**

```
XPMNAME  AUTONEG  SUBNMASK       IPCONFIG  SNMP     ACTADDR       INADDR
      UNIT0         UNIT1          GWINDEX           DNSINFO
-------------------------------------------------------------------------------
DTC 10   AUTO     255 255 255 0  CM         N        47 192 3 24   47 192 3 25
      47 192 3 26   47 192 3 27     (1) (2) (4) $    N
DTC 11   AUTO     255 255 255 0  CM         Y  public  47 192 3 116  47 192 3 117
      47 192 3 118   47 192 3 119   (0) (1) $        N
DTC 20   AUTO     255 255 240 0  DHCP
```

### XPMNAME field

XPMNAME specifies the IP-XPM datafilled in table LTCINV. This value is referenced in table IPCOMID (page 60).

### AUTONEG field

AUTONEG specifies the Ethernet speed used by the XPM. If AUTONEG is 10BT, the XPM runs at 10Base-T speed. If AUTONEG is AUTO, the XPM automatically selects (by negotiating with the network) either 10Base-T or 100Base-T, whichever is appropriate.

### SUBNMASK field

SUBNMASK specifies the subnet mask used for the local subnet network.

### IPCONFIG field

IPCONFIG specifies whether XPM bootstrapping information is provided by the network or by the CM. If IPCONFIG is DHCP, the network configures the XPM and no further datafill is needed in table XPMIPMAP.

If IPCONFIG is CM, the CM configures the XPM, and datafill is required in the following other fields:

- ACTADDR (active address)
- INADDR (inactive address)
- UNIT0 (unit 0 address)
- UNIT1 (unit 1 address)

- GWINDEX (gateway index)
- DNSINFO (domain name system information)

### ACTADDR field

ACTADDR specifies the IP address of the active unit of the XPM. The last octet of the active address must be divisible by four (for example, 47.192.3.24).

***Note:*** The active address is *always* used when a node on the network (such as an IP position or another TOPS-IP switch) communicates with an application on the CM. This is the case even after a SWACT in the XPM. The XPM is responsible for maintaining the correct IP addressing after a SWACT. (Refer to "Gratuitous ARP broadcast message" on page 45.)

### INADDR field

INADDR specifies the IP address of the inactive unit of the XPM. The inactive address is always ACTADDR + 1 (for example, 47.192.3.25).

### UNIT0 field

UNIT0 specifies the IP address of unit 0. The unit 0 IP address is always ACTADDR + 2. The XPM uses the UNIT0 address internally for diagnostics.

### UNIT1 field

UNIT1 specifies the IP address of unit 1. The unit 1 IP address is always ACTADDR + 3. The XPM uses the UNIT1 address internally for diagnostics.

### GWINDEX field

GWINDEX specifies the possible gateway routers for each XPM. This value references one or more GWINDEX values in table XPMIPGWY. A value of $ indicates that no gateway router is needed. An XPM can be configured with up to 10 routers.

***Note:*** After changing the datafill for GWINDEX, users should update the static data for the SX05DA. For details, refer to "Updating static data" on page 299.

### DNSINFO field

The DNSINFO field specifies the domain name and its associated IP addresses. A value of N indicates that DNS is not supported.

***Note:*** This field is not currently used.

## IPSVCS

Table IPSVCS defines IP transport services for the SX05DA. Each service name represents a software port and transport protocol. The service name is referenced by table IPCOMID (page 60).

Each tuple in table IPSVCS can be used for only one TOPS-IP application. For example, the OC-IP and IP position applications cannot be datafilled to share the same IP transport service. On the other hand, a single TOPS-IP application may use more than one IP transport service. Refer to the individual application chapters for application-specific information about the use of this table.

The following example shows datafill for five IP transport services. A brief description of each field follows the example.

**Figure 19 MAP display example for table IPSVCS**

```
SERVICE           PORT       PROTOCOL
-----------------------------------------------------------------
FREEPORT          0          TCP_UDP
OCIPSVC           8600       UDP
POSIPSVC          8700       UDP
QMSMIS            0          TCP
XIPVER            11777      TCP_UDP
```

### SERVICE field

SERVICE names are chosen by the operating company and are used only to enable table IPCOMID to reference tuples in table IPSVCS. Service names in table IPSVCS must be unique.

### PORT field

PORT numbers are selected by the operating company. They are used to route incoming messages to the correct application software. They are unrelated to any hardware port. Port numbers apply to all IP-XPMs that are datafilled at the switch.

The switch can use port values in the range 2048 to 12287. Port numbers outside this range are reserved for non-CM IP applications. Port numbers in table IPSVCS must be unique, with the exception of port number 0. A port number of 0 is used to request the IP-XPM to randomly assign a port number (32768 to 65535) to the application. More than one tuple may datafill a 0 in the PORT field.

***Note 1:*** Port numbers 1 to 1024 are well-known industry-defined port numbers that are reserved for applications such as FTP (File Transfer Protocol), Telnet, and HTTP (Hypertext Transfer Protocol).

***Note 2:*** See Chapter 7: “TOPS-IP engineering guidelines” for recommendations on port ranges for TOPS-IP applications.

### PROTOCOL field

PROTOCOL specifies the transport layer protocol used in data communication. Valid values include TCP, UDP, and TCP_UDP. A value of TCP_UDP indicates that either TCP or UDP may be used. Each TOPS-IP application specifies which protocol or protocols it supports. See the separate chapters that describe the applications.

***Note:*** ICMP is a required part of IP and does not need to be datafilled explicitly.

## IPCOMID

Table IPCOMID defines communication identifiers (COMID). Each COMID represents local connection information for a TOPS-IP application. This information includes the port and protocol (specified by the service name in table IPSVCS) and the name of the IP-XPM used for data communication.

COMIDs are referenced by application-specific tables. Each COMID can be used for only one TOPS-IP application. For example, the OC-IP and IP position applications cannot be datafilled to use the same COMID. On the other hand, a single TOPS-IP application may use more than one COMID. Refer to the separate application chapters in this book for application-specific information about the use of COMIDs.

The following example shows datafill for several COMIDs. A brief description of each field follows the example.

**Figure 20 MAP display example for table IPCOMID**

```
COMID     SERVICE          XPMNAME
-----------------------------------------------------------
1         OCIPSVC          DTC 10
2         OCIPSVC          DTC 11
10        POSIPSVC         DTC 10
11        POSIPSVC         DTC 11
30        QMSMIS           DTC 20
40        XIPVER           DTC 10
```

### COMID field

COMID identifies the tuple. The COMID is referenced by application-specific tables.

***Note:*** Although a particular COMID is associated with a service name in table IPCOMID, the COMID is not assigned (*bound)* to a particular application until the COMID is datafilled in the application-specific table.

### SERVICE field

SERVICE specifies a tuple in table IPSVCS, which identifies the port and protocol. Multiple COMIDs can use the same service name only if the COMIDs are associated with different XPMs.

### XPMNAME field

XPMNAME specifies the IP-XPM datafilled in table XPMIPMAP that is used for the particular COMID. Multiple COMIDs can use the same XPM only if they use different IP transport services.

***Note:*** For all TOPS-IP applications, COMIDs represent *local* information about the *switch end* of a logical data connection. They do not embody any information about the far end of the logical connection. Depending on the application, additional switch datafill may be needed to specify an IP address and port for the far end, and/or parallel datafill at the far end may be needed to specify the switch (IP-XPM) IP address and port.

## CLLI

Table CLLI specifies trunk group names and the maximum number of members in any given trunk group. The following example shows datafill for a switch that uses three TOPS-IP dynamic trunk groups.

**Figure 21 MAP display example for table CLLI**

```
CLLI            ADNUM      TRKGRSIZ     ADMININF
-----------------------------------------------------------------
OCIPTOREMOTE    356        2016         OCIP_TOREMOTE_VOICE_LINK
OCIPTOHOST      367        2016         OCIP_TOHOST_VOICE_LINK
POSIPVL         484        2016         POSIP_VOICE_LINK
```

For most trunk groups, the maximum number of members is 2048. But for the dynamic trunks used for TOPS-IP applications, each 7X07 Gateway card adds 48 members to the trunk group associated with that card. Therefore, the actual number of members in a TOPS-IP dynamic trunk group is always a multiple of 48, and 2016 is the largest multiple of 48 that does not exceed 2048. So no TOPS dynamic trunk group can have more than 2016 members.

## TRKGRP

Table TRKGRP specifies the trunk group type, direction, member selection algorithm, and translations and screening attributes for each trunk group. Dynamic trunks used for TOPS-IP applications use the IT (intertoll) trunk group type. Table TRKOPTS, where trunk groups are defined as dynamic, enforces this restriction.

The direction of the dynamic trunk group is important for TOPS-IP voice communication. Each application has its own requirements for the trunk group direction. For more information, refer to the separate chapters that describe each application.

The MIDL trunk selection algorithm is recommended for all TOPS-IP dynamic trunking applications.

TOPS-IP applications do not use the translations and screening information in table TRKGRP, so those fields should be datafilled with default values.

The following example shows datafill for the three dynamic trunk groups defined in table CLLI.

**Figure 22 MAP display example for table TRKGRP**

```
GRPKEY        GRPINFO
------------------------------------------------------------------------
OCIPTOREMOTE IT 0 NPDGP NCRT 2W OA  MIDL 000 NPRT NSCR 619 619 000 N N $
OCIPTOHOST   IT 0 NPDGP NCRT OG OA  MIDL 000 NPRT NSCR 619 619 000 N N $
POSIPVL      IT 0 NPDGP NCRT OG OA  MIDL 000 NPRT NSCR 619 619 000 N N $
```

## TRKSGRP

Table TRKSGRP defines additional trunk group information such as signaling. Because dynamic trunks are defined as ISUP trunks, the following datafill must be present (enforced in table TRKOPTS):

- subgroup number set to 0
- card code set to DS1SIG
- signaling selector set to C7UP
- trunk direction must match table TRKGRP
- protocol set to Q764
- continuity testing set to 0
- glare set to CIC, if the refinement for the trunk group direction includes a glare field

Additional information in table TRKSGRP is not used for TOPS-IP applications, and should be set to nil or default values.

The following example shows datafill for the three trunk groups.

**Figure 23 MAP display example for table TRKSGRP**

```
SGRPKEY          CARDCODE SGRPVAR  SGRPVAR
------------------------------------------------------------------------------
OCIPTOREMOTE 0   DS1SIG   C7UP      2W N N UNEQ NONE Q764 THRL 0 NIL $ NIL CIC
OCIPTOHOST 0     DS1SIG   C7UP      OG N N UNEQ NONE Q764 THRL 0 NIL $ NIL
POSIPVL 0        DS1SIG   C7UP      OG N N UNEQ NONE Q764 THRL 0 NIL $ NIL
```

## TRKOPTS

Table TRKOPTS specifies additional trunk group options including the dynamic option required for TOPS-IP voice trunks. Datafill in TRKOPTS is used to define entire trunk groups as IP trunks. This table also enforces various ISUP signaling-related datafill in table TRKGRP and table TRKSGRP.

***Note:*** TOPS-IP does not use the SS7 network.

The following datafill must be present:

- option set to DYNAMIC
- call control signaling set to ISUP
- network used for call control signaling set to IP
- network used for voice (bearer) set to IP
- application that uses dynamic trunking (OC or POS)

  Refer to the separate chapters on the OC-IP and IP position applications for more information about OC and POS datafill in table TRKOPTS.

The following example shows datafill for the three trunk groups.

**Figure 24 MAP display example for table TRKOPTS**

```
OPTKEY                 OPTINFO
-------------------------------------------------------------
OCIPTOREMOTE DYNAMIC   DYNAMIC ISUP IP IP OC
OCIPTOHOST DYNAMIC     DYNAMIC ISUP IP IP OC
POSIPVL DYNAMIC        DYNAMIC ISUP IP IP POS
```

## SITE

Table SITE identifies a site name associated with the 7X07 Gateway cards datafilled at the switch. The Gateways are used in TOPS-IP voice communication. The site name is referenced by table IPINV and is visible at the PM level of the MAP.

***Note:*** Gateway does not refer to a gateway router.

The following example shows datafill for the TGWY site name.

**Figure 25 MAP display example for table SITE**

```
NAME    LTDSN  MODCOUNT OPVRCLLI ALMDATA
-----------------------------------------------------------
TGWY    0      0        VER90    $
```

***Note 1:*** As Gateways are added to and removed from table IPINV, the system automatically updates the MODCOUNT field to reflect the number of Gateways on the site.

***Note 2:*** The site name is selected by the operating company. The same site name may be used for all TOPS-IP applications, or different site names may be used for different TOPS-IP applications. This is an administrative decision, and it does not affect performance.

## IPINV

Table IPINV defines the individual 7X07AA Gateway cards (nodes) at the switch. Datafill values include the site name, the XPM name and P-side port, the Gateway IP address, and Gateway type and refinements.

For TOPS Gateways, the refinements specify a dynamic trunk group and starting member number. When a tuple is added to table IPINV, the switch *automatically* datafills a block of 48 trunk members for that group in table TRKMEM.

The following example shows the TGWY site datafilled with a total of eight Gateway cards. Three trunk groups—OCIPTOREMOTE, OCIPTOHOST, and POSIPVL—are datafilled across two IP-XPMs (DTC 10 and DTC 11). Each of the OC-IP trunk group supports 144 members, and the one used for IP positions supports 96 members. A brief description of each field follows the example.

**Figure 26 MAP display example for table IPINV**

```
IPNO       PMTYPE PMNO IPPEC  LOAD PORT IPZONE               GWTYPE
-------------------------------------------------------------------------------
TGWY 10 3  DTC    10   7X07AA  $   6    47 174 68 7  0 0 0 0  TOPS OCIPTOREMOTE 0
TGWY 10 4  DTC    10   7X07AA  $   8    47 174 68 8  0 0 0 0  TOPS OCIPTOHOST 0
TGWY 10 5  DTC    10   7X07AA  $   10   47 174 68 9  0 0 0 0  TOPS OCIPTOREMOTE 48
TGWY 10 6  DTC    10   7X07AA  $   12   47 174 68 10 0 0 0 0  TOPS POSIPVL 0
TGWY 11 3  DTC    11   7X07AA  $   6    47 174 69 7  0 0 0 0  TOPS OCIPTOHOST 48
TGWY 11 4  DTC    11   7X07AA  $   8    47 174 69 8  0 0 0 0  TOPS OCIPTOREMOTE 96
TGWY 11 5  DTC    11   7X07AA  $   10   47 174 69 9  0 0 0 0  TOPS OCIPTOHOST 96
TGWY 11 6  DTC    11   7X07AA  $   12   47 174 69 10 0 0 0 0  TOPS POSIPVL 144
```

### IPNO field

IPNO associates the name of a site (from table SITE) with a unique Gateway frame and unit number pair. It is recommended that the DTC number be entered as the frame number, and the PORT divided by 2 be entered as the unit number.

### PMTYPE field

PMTYPE specifies the XPM type (DTC) datafilled in table LTCINV.

### PMNO field

PMNO specifies the XPM number datafilled in table LTCINV.

### IPPEC field

IPPEC specifies the 7X07AA Gateway product engineering code (PEC).

### LOAD field

LOAD specifies the name of the loadfile for the Gateway card.

***Note:*** This field is reserved for future functionality.

### PORT field

PORT specifies the P-side port for the Gateway card. The port corresponds to the lower-numbered of the two P-side links datafilled for the Gateway in table LTCPSINV. (The P-side links must be assigned in table LTCINV first.)

Each DTC port supports 24 channels. So when a Gateway card is datafilled in table IPINV, 24 channels are allocated against the port number in the tuple, and the other 24 channels are allocated against the next port number (PORT + 1). To prevent inadvertent overlap, only even port numbers may be datafilled in IPINV for TOPS-IP applications.

For more details, refer to "LTCPSINV-to-IPINV port mapping" on page 249.

### IPZONE field

IPZONE specifies a primary and a secondary IP address for the Gateway card.

TOPS Gateways require the correct primary IP address in the IPZONE field. The primary IP address must match the one assigned to the Gateway by the DHCP server, if a DHCP server is used. Any mismatch between DHCP datafill and CM datafill for a Gateway will prevent the Gateway from coming into service. The secondary IP address is unused and should be datafilled with 0 0 0 0.

### GWTYPE field

GWTYPE defines the type of Gateway and includes refinements based on the Gateway type. For TOPS-IP applications, the Gateway type must be datafilled as TOPS.

Two refinement fields are present for the TOPS Gateway type selector:

- TRKCLLI - The CLLI of a dynamic trunk group that is datafilled for a TOPS-IP application, such as OC or POS, in table TRKOPTS. This is the trunk group from which the switch will automatically allocate 48 members in table TRKMEM.
- MEMSTART - the *starting* trunk member number in a block of 48 associated with the trunk group. Because each Gateway card can support 48 voice circuits, the starting member must be 0 or a multiple of 48.

The example datafill in Figure 26 causes automatic datafill of the following trunk members in table TRKMEM:

- OCIPTOREMOTE 0 to 47, 48 to 95, and 96 to 143
- OCIPTOHOST 0 to 47, 48 to 95, and 96 to 143
- POSIPVL 0 to 47 and 144 to 191

***Note 1:*** Removing TOPS entries from table IPINV automatically removes the associated TRKMEM members. Table TRKMEM does not allow members associated with a Gateway card to be manually added or removed.

***Note 2:*** There is no restriction that the 48-member blocks be adjacent.

***Note 3:*** Trunk groups typically have a maximum of 2048 members. Since IPINV allocates 48 members at a time, this maximum is limited to 2016 for TOPS-IP trunk groups. 2016 is the highest multiple of 48 that is less than 2048.

***Note 4:*** Refer to table TOPSTOPT (page page 67) for datafill that limits the number of trunks that may be used by call processing.

### TRKMEM

Table TRKMEM defines the individual trunk members associated with a trunk group. In the case of trunks defined as DYNAMIC in table TRKOPTS and used for TOPS-IP applications, table IPINV *automatically* datafills table TRKMEM, so manual datafill is not allowed.

The following example shows partial datafill for the dynamic trunk groups. This corresponds to the example IPINV datafill example on page 64.

**Figure 27 MAP display example for table TRKMEM**

```
CLLI          EXTRKNM SGRP MEMVAR
-------------------------------------------------
OCIPTOREMOTE    0     0    DTC 10 6 1
OCIPTOREMOTE    1     0    DTC 10 6 2
OCIPTOREMOTE    2     0    DTC 10 6 3
 . . . . . .
OCIPTOREMOTE   23     0    DTC 10 6 24
OCIPTOREMOTE   24     0    DTC 10 7 1
 . . . . . .
OCIPTOREMOTE   47     0    DTC 10 7 24
OCIPTOREMOTE   48     0    DTC 10 10 1
 . . . . . .
OCIPTOREMOTE   95     0    DTC 10 11 24
OCIPTOREMOTE   96     0    DTC 11 8 1
 . . . . . .
OCIPTOREMOTE 143     0    DTC 11 9 24
OCIPTOHOST     0     0    DTC 10 8 1
 . . . . . .
OCIPTOHOST   143     0    DTC 11 11 24
POSIPVL        0     0    DTC 10 12 1
POSIPVL        1     0    DTC 10 12 2
 . . . . . .
POSIPVL       23     0    DTC 10 12 24
POSIPVL       24     0    DTC 10 13 1
 . . . . . .
POSIPVL       47     0    DTC 10 13 24
POSIPVL      144     0    DTC 11 12 1
 . . . . . .
POSIPVL      191     0    DTC 11 13 24
```

## TOPSTOPT

Table TOPSTOPT specifies options for TOPS trunk groups. The MAXCONNS field can be used to specify the maximum number of trunks in a trunk group that can be used by call processing. This value applies only to TOPS-IP dynamic trunk groups.

Limiting the number of usable members in a TOPS-IP dynamic trunk group may be desirable for two reasons. The first reason would occur if the managed IP network has been provisioned to handle less traffic than the automatically-datafilled members of the trunk group could generate. The second reason is to ensure that the spare capacity engineered for the trunk group really is spare.

When the MAXCONNS function is used, the total number of available trunks is distributed evenly over the in-service Gateways in the trunk group. The system automatically adjusts this distribution as Gateway cards go into and out of service. It may take several minutes of call processing after the limit is set before it is fully in effect.

If the MAXCONNS function is not desired for a TOPS-IP dynamic trunk group, either the trunk group should not be added to table TOPSTOPT or its MAXCONNS value should be set to 2016. This will avoid unnecessary CPU real-time consumption on each TOPS-IP call.

Other fields in table TOPSTOPT are not used for dynamic trunks, they and should be datafilled with default values.

***Note:*** For more information about the use of the MAXCONNS functionality, refer to “Limiting the use of dynamic voice links” on page 200.

The following example shows datafill for the three trunk groups.

**Figure 28 MAP display example for table TOPSTOPT**

```
GRPKEY    ORGAREA  DISPCLG  ADASERV  ADASANS  ANITOCLI  OLNSQRY  DCIBIDX
  LNPCLGAM     XLASCHEM  SPIDPRC  TRKSPID  BILLSCRN  ANIFSPL  MAXCONNS  DISPSPID
-------------------------------------------------------------------------------
OCIPTOREMOTE N      N       NONE      NA        N         NONE        0
  N              N         N        N         N         N       60        N
OCIPTOHOST   N      N       NONE      NA        N         NONE        0
  N              N         N        N         N         N       60        N
POSIPVL      N      N       NONE      NA        N         NONE        0
  N              N         N        N         N         N       48        N
```

### OFCENG

Table OFCENG contains office-wide parameters. The following parameters are relevant to TOPS-IP applications:

- IPGW_PCM_SELECTION specifies the speech companding law and bit inversion pattern on the 7X07 Gateway's C-side links. In all standard office configurations, the value of this parameter should be set to AUTO (default). When set to AUTO, the correct speech processing information is automatically determined by the value of OFCENG parameter TYPE_OF_NETWORK when the Gateway is loaded.

  ***Note 1:*** Any change in the value of this parameter requires the Gateway to be reloaded

  ***Note 2:*** Depending upon voice quality, international TOPS offices may need to set the parameter to a value other than AUTO. The value must be determined on a per site basis depending upon the TYPE_OF_NETWORK value and the appropriate PCM bit inversions.

- NUMPERMEXT allocates data structures (permanent extension blocks) for calls. For most TOPS-IP voice applications, this value should be incremented by one for each dynamic trunk group member. Refer to the chapters on the individual applications for exceptions.

  ***Note 1:*** NUMPERMEXT does not appear in table OFCENG if it is autoprovisioned in table OFCAUT.

  ***Note 2:*** If the number of usable members in a dynamic trunk group has been limited in table TOPSTOPT (see page 67), no more than the MAXCONNS limit of portperm extension blocks will be used by the trunk group. However, it is safer to overprovision the portperm extension blocks, in case the MAXCONNS datafill is changed in the future.

The following example shows datafill for these OFCENG parameters.

**Figure 29 MAP display example for table OFCENG**

```
PARMNAME                    PARMVAL
------------------------------------------------------------
IPGW_PCM_SELECTION          AUTO
NUMPERMEXT                  244
```

***Note:*** Other engineering parameters are related to specific TOPS-IP applications Refer to the chapters on the individual applications for more information.

## PKTVPROF

Table PKTVPROF defines packetized voice profiles for use in TOPS-IP call processing. The profile index identifies a tuple and is referenced by application-specific tables. The other fields specify how codec selection should work.

The following example shows datafill for three packetized voice profiles. A brief description of each field follows the example. In the example,

- Profile 0 specifies that a G.711 codec (A-law or Mu-law) is always to be used.
- Profile 1 specifies that G.723 is always to be used.
- Profile 2 specifies that G.711 is the preferred codec, but G.723 may be used if (a) the application supports auto-compression and (b) the criteria for auto-compression are met. Refer to Chapter 4: "TOPS IP position application" for more information about auto-compression.

***Note:*** Table PKTVPROF was changed in TOPS19. The end of this section includes important information for customers who are using TOPS-IP in earlier releases.

**Figure 30 MAP display example for table PKTVPROF**

```
PROFNUM  CODEC  AUTOCOMP
-------------------------------------------------------------------
0        G711   N
1        G723   N
2        G711   Y G723
```

### PROFNUM field

PROFNUM identifies the tuple, so that it can be referenced by other tables.

### CODEC field

CODEC identifies the preferred codec to be used for voice encoding. The datafillable values are G711 (for uncompressed voice) and G723 (for compressed voice). Refer to "Voice encoding and packetization" on page 49 for more information about these codecs.

### AUTOCOMP field

AUTOCOMP includes a Y/N selector and possible refinements. The selector specifies whether auto-compression should be used for applications that support it. Datafilling N means the profile does not support auto-compression, and the codec in the CODEC field will always be used even if the application supports auto-compression. Datafilling Y means that the profile does support auto-compression for applications that also support it.

When Y is entered, the user must also datafill the codec to be used when auto-compression is in effect. The only entry allowed here is G723. For more information about auto-compression, refer to Chapter 7: "TOPS-IP engineering guidelines" of this book and to *TOPS IWS Base Platform User's Guide*.

## Table PKTVPROF prior to TOPS19

Table PKTVPROF was changed in TOPS19 to include the fields and values described above. In releases earlier than TOPS19, the table appears as in the following example. (See version 02.03 of this document for a complete description.)

**Figure 31 MAP display example for table PKTVPROF prior to TOPS19**

```
PROFNUM  PKTVFLDS
---------------------------------------------------------
0        G711
1        G729 NOSILSUP
2        G729 SILSUP
```

As the example shows, there was no selector for auto-compression, and it was possible to datafill the G.729 codec (no longer supported) with or without silence suppression. Patch CFX84 affects the interpretation of PKTVPROF datafill, in CM loads earlier than TOPS19, as shown in the following table. Refer to the patch documentation for more complete information.

**Table 1 Interpretation of table PKTVPROF in CM loads earlier than TOPS19/SN06**

| CFX84 status | PKTVPROF datafill, field PKTVFLDS | Codec used for VoIP between two Gateways | Codec used for VoIP between Gateway and IWS |
|---|---|---|---|
| not applied | G711 | G.711 | G.711 |
| | G729 NOSILSUP | G.729 w/o silence suppression | G.711 |
| | G729 SILSUP | G.729 with silence suppression | G.711 |
| applied but not activated | G711 | G.711 | G.711 |
| | G729 NOSILSUP | G.723 | G.723 |
| | G729 SILSUP | G.723 | G.723 |
| activated | G711 | G.711 | G.711 or G.723 depending on detected voice quality (auto-compression). |
| | G729 NOSILSUP | G.723 | G.723 |
| | G729 SILSUP | G.723 | G.723 |

# Chapter 3: TOPS OC-IP application

The TOPS-IP product implements Operator Centralization (OC) over an integrated IP infrastructure. This chapter describes the OC-IP application, focusing on the following areas:

- background on traditional OC connectivity, call flow, and capabilities
- introduction to OC-IP data and voice communication
- overview of datafill for OC-IP data links
- overview of datafill for OC-IP voice links
- OC-IP call processing and failure handling

***Note:*** The OC-IP application has interactions with the IP position application in networks that use both. Some of the interactions are discussed in this chapter, and some in Chapter 4: “TOPS IP position application.”

## OC background

In a TOPS OC network, a number of TOPS remote switches share the operator positions provided by a TOPS host switch. Calls originate in an OC remote switch, which is responsible for call control. The OC host switch provides the operator positions and is responsible for call and agent queue management, force management, and position maintenance. The OC host and OC remote communicate over data links and voice links to process a call.

### Traditional OC data and voice connectivity

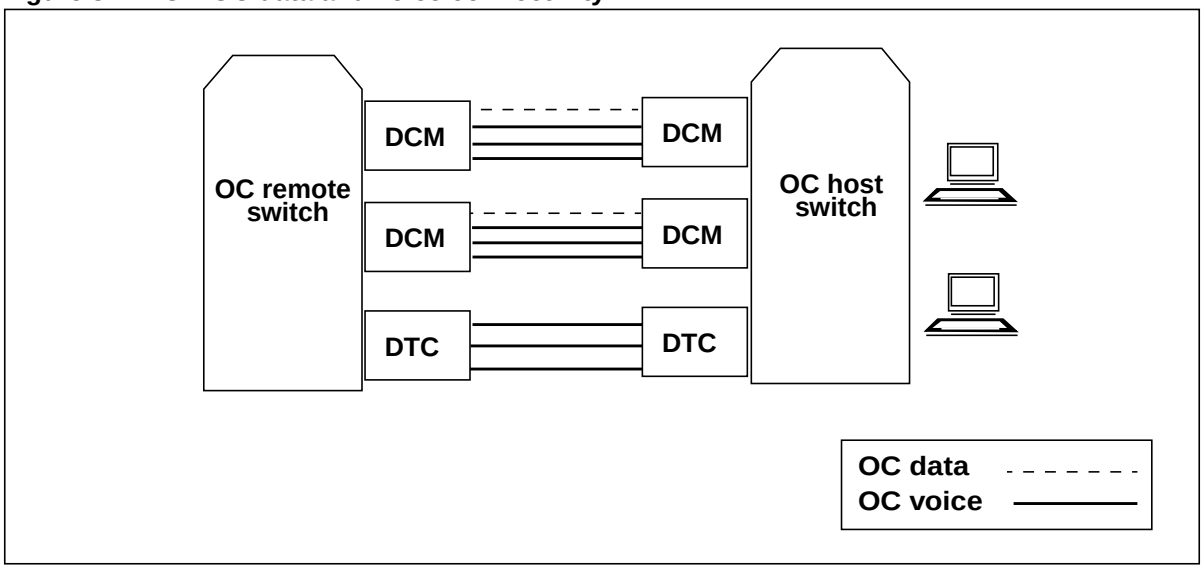
The OC data links are used for call control messages, key function messages, and screen update messages. One data link can be shared by many calls in progress. In a traditional OC configuration, the data links can be provisioned on either Digital Carrier Module (DCM) or Enhanced TOPS Message Switch (ETMS) peripherals. Data links are provisioned per remote in the host, and per host in the remote.

The OC voice links traditionally provide a speech path between the operator in the host and the calling and called parties in the remote. (The OC remote uses a conference three-port circuit to connect the voice link with the calling and called parties.) In a configuration that uses TDM-based trunking for voice facilities, the voice links are provisioned per remote in the host, and per host in the remote. Each call must have a *dedicated* voice link while the operator services the call.

## DCM OC connectivity

Figure 32 shows an example DCM OC configuration. Each DCM can support one OC data link, and the remaining DCM circuits can be used for OC voice links. In addition, OC voice links can be provisioned on any switch peripheral that supports appropriate analog or digital trunks.

**Figure 32 DCM OC data and voice connectivity**




***Note:*** DCMs are no longer manufactured or sold.

## ETMS OC connectivity

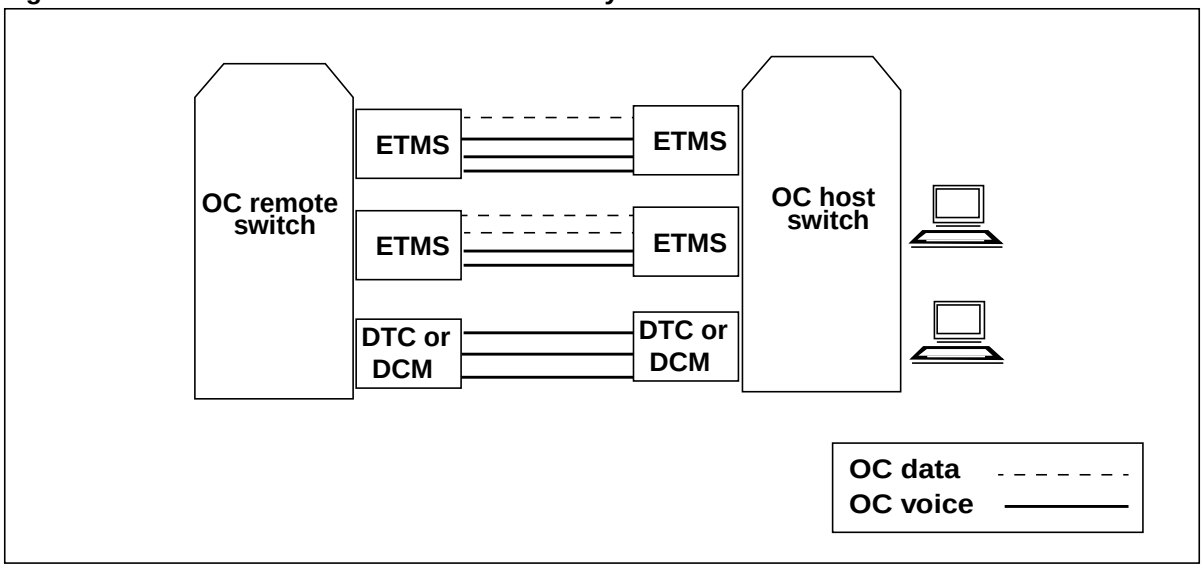
TOPS introduced ETMS OC to increase OC capacity in the following ways:

- Increased the number of OC nodes (switches) that a single switch can communicate with—from 15 to 31, or 15 to 30 if the Host Remote Networking by Queue Type capability is used.
- Removed the limitation that an OC host could provide a maximum of 150 positions for each remote.
- Removed the limitation that the data link technology could support a maximum distance of 1500 miles between an OC host and OC remote.

Figure 33 shows an example ETMS OC configuration. Each ETMS peripheral can support up to 31 OC data links, and the remaining ETMS circuits can be used for OC voice links. In addition, OC voice links can be provisioned on any switch peripheral that supports appropriate analog or digital trunks.

***Note***: TOPS OC via ETMS functionality is no longer available.

**Figure 33 ETMS OC data and voice connectivity**



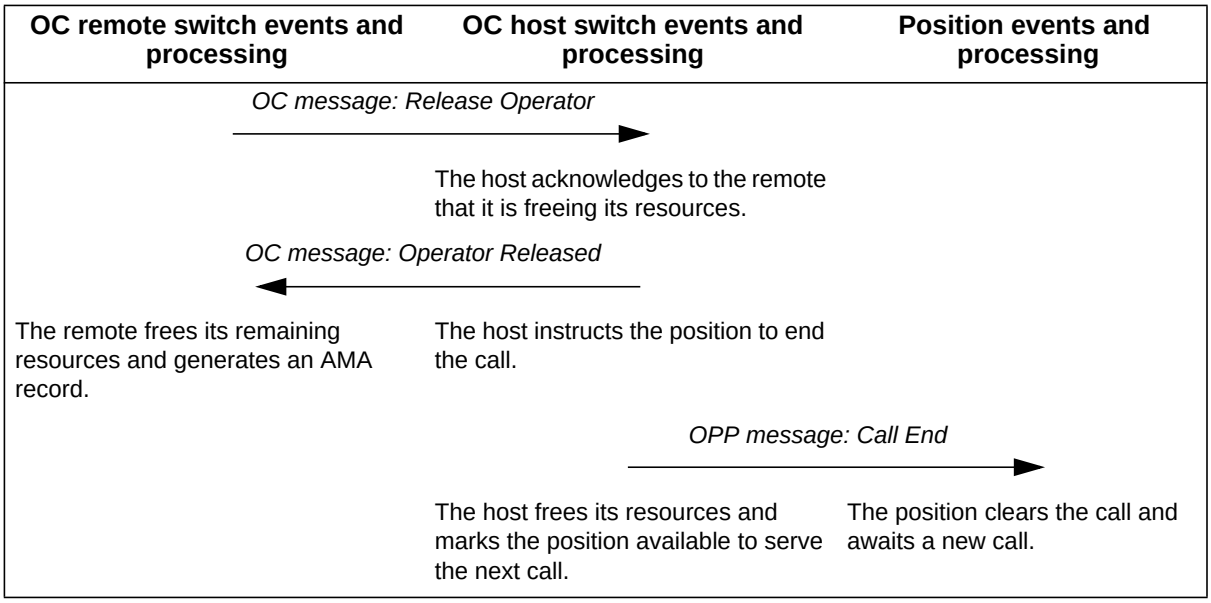

## Traditional OC call flow

Figure 34 shows an example traditional OC call flow that illustrates the use of voice and data links. Use of voice links is described in the text. The arrows represent data messages. The data messages include both OC data (between the host and remote) and OPP data (Open Position Protocol, between the host and position.) Note that some OC messages encapsulate OPP messages.

**Figure 34 Example of traditional OC call flow**

| OC remote switch events and processing | OC host switch events and processing | Position events and processing |
|---|---|---|
| A call that requires an operator arrives at a TOPS switch. QMS and OC translations determine that this is a TDM OC call. | | |
| The remote selects an OC data link and requests an operator from the host. | | |
| *OC message: Request Operator* → | | |
| | The host selects an operator at a TDM position. | |

| OC remote switch events and processing | OC host switch events and processing | Position events and processing |
|---|---|---|
| | The host selects an OC voice link and connects it to the position's nailed-up voice link.<br><br>The host informs the remote that a position has been allocated for the call. (This message identifies which OC voice link the host has selected.) | |
| *OC message: Got Operator* ← | | |
| The remote allocates a conference three-port circuit (CF3P) and uses it to connect the OC voice link to the caller's voice.<br><br>The remote sends call arrival data to the host, in a series of OPP messages encapsulated in a series of OC messages. | | |
| *OC message: OPP Call Begin* →<br>. . .<br>*OC message: OPP Call Updates* → | | |
| | The host extracts the OPP call arrival data from the OC messages, and forwards it to the position in a series of OPP messages. | |
| | *OPP message: Call Begin* →<br>. . .<br>*OPP message: Call Updates* → | |
| The remote generates call arrival tones for the operator over the OC voice link. (These tones are not heard by the caller.) | | The position displays the call arrival information for the operator. The operator hears the call arrival tones. |
| The call is established and data messages are processed. | The host forwards OPP key function and screen update messages between the remote and the position as needed to process the call. | The caller and the operator converse. The operator may key in call information. The position may exchange OPP messages with the host. The position may also communicate with various data bases. |
| When the call is complete, the remote breaks its voice connections, deallocates the CF3P, frees its end of the OC voice link, and instructs the host to release its resources. | | |




***Note:*** Refer to page 105 for an example OC-IP call that uses a TDM position. Refer to page 144 for an example OC-IP call that uses an IP position.

## OC capabilities

TOPS OC provides the following two optional capabilities:

- Host Remote Networking by Queue Type (HRNQT) allows calls in a single OC remote switch to obtain operators from different OC hosts based on the call queue assigned to the call. Also, some calls can be handled as standalone (non-OC) calls while others are handled as OC remote calls based on the call queue. With HRNQT, a TOPS switch is no longer a pure standalone, host, or remote switch. A single TOPS switch can function as all three.
- Alternate host processing (part of HRNQT) allows the operating company to datafill the following information for each call queue:
  - — a primary and an alternate host
  - — a list of reasons (such as deflection) why failure to get an operator from the primary host would cause the switch to attempt to get an operator from the alternate host

  If a call fails to get an operator from the primary host and is not eligible for alternate host processing, it is routed to treatment.

***Note:*** Operator Centralization Night Closedown (OCNC) was used with the TOPSACD queuing system to allow a TOPS switch to function as a remote during certain times of the day and as a standalone (non-OC) for the rest of the day. TOPS Queue Management System (QMS), which has replaced TOPSACD, provides a more powerful way to handle calls differently depending on time of day.

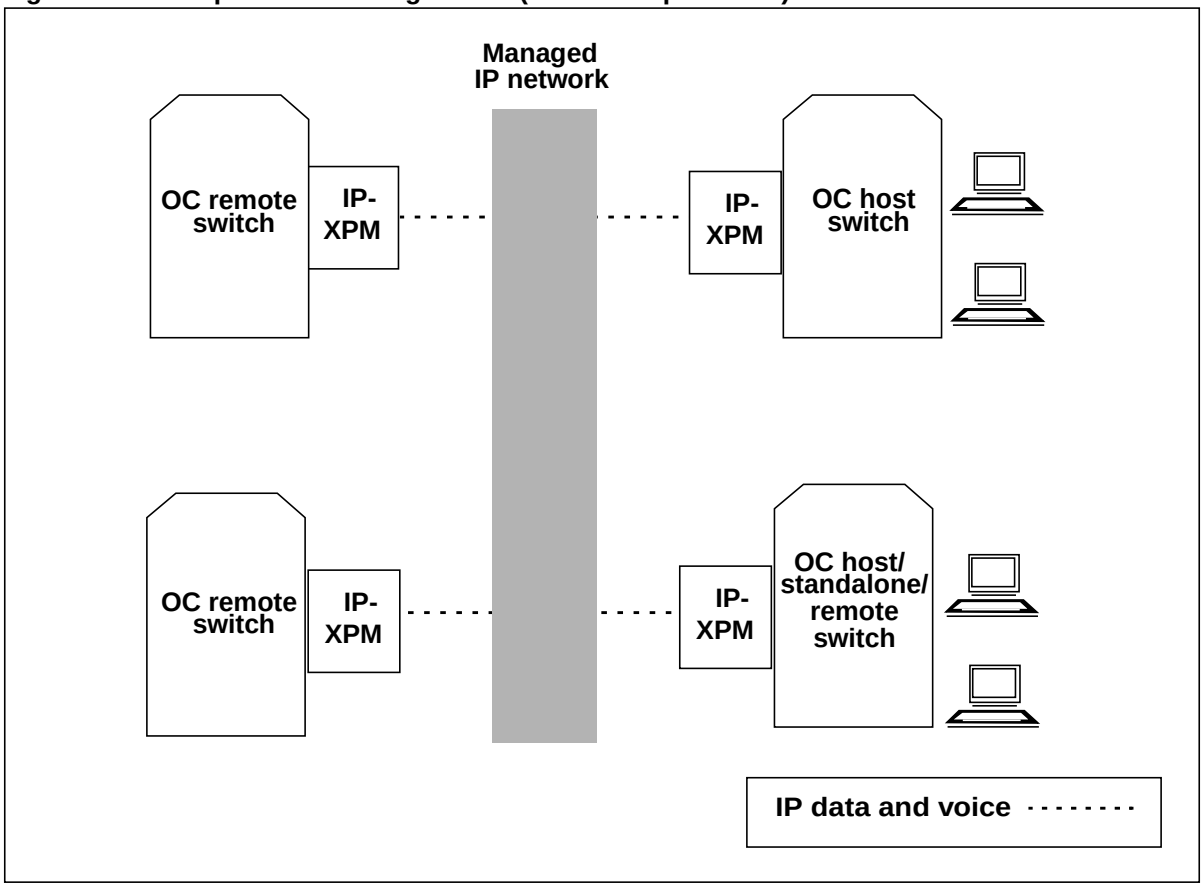
## OC-IP introduction

In an OC-IP configuration, a common IP infrastructure replaces the separate, point-to-point provisioning of data and voice between the OC switches. Through the IP-XPM, TOPS-IP handles all the OC data and voice traffic across the managed IP network.

General OC functionality remains unchanged in a TOPS-IP network. OC host and remote switches have the same fundamental roles as before, and the IP data and voice communication technology is transparent to operators. OC-IP interworks fully with HRNQT and Alternate Host Selection. The alternate host need not use OC-IP. OC-IP also interworks fully with both traditional TDM-based operator positions and IP positions.

Figure 35 shows an example OC-IP configuration with TDM-based positions.

**Figure 35 Example OC-IP configuration (without IP positions)**



## OC-IP data communication

This section discusses concepts and terms related to OC-IP data communication.

***Note:*** Much of this information is specific to the OC-IP application. For more basic information about the TOPS-IP infrastructure for data communication, refer to Chapter 2: "TOPS-IP data and voice communication."

### IP-XPM data interface

The SX05DA processor card in the IP-XPM provides the switch interface for OC-IP data communication between OC host and remote switches.

### OC-IP data links

OC-IP data links are used for call control, key function, and screen update messaging between an OC host switch and an OC remote switch. At the transport layer they use the UDP protocol

The OC-IP application does not have an explicit concept of data link *groups*. However, it is still possible to datafill multiple data links to be used for communication with a distant office. As with traditional OC, the reason for having multiple data links between a pair of offices is to provide redundancy or to increase throughput capacity (or both). With OC-IP, these objectives are achieved by provisioning data links to a distant office on more than one IP-XPM. (Datafilling more than one data link to a distant office on the same IP-XPM does not increase throughput capacity. And, depending on how the network is configured, it may provide only a small amount of redundancy.)

An OC data link represents a *logical* connection between two switches. Although it does not represent a physical path, the two endpoints of the data link are fixed. An OC switch must have datafill for both of the connection endpoints—the local end and the distant end—of each data link it uses.

### Related switch datafill

The local endpoint of an OC data link is represented in switch datafill by a COMID. Recall that a COMID specifies a particular SX05DA-equipped DTC and, indirectly through table IPSVCS, a port. Each OC-IP data link is associated with a unique COMID.

The switch datafill for the far endpoint of an OC-IP data link specifies the distant socket directly, as follows:

- It specifies the active IP address of the SX05DA XPM that provides LAN connectivity for the data link in the distant switch.
- It specifies the port number that is datafilled in the distant switch against its end of the data link.

***Note:*** The CM cannot learn the far-end IP address or port from the network.

### Parallel datafill requirements

Datafill for IP-XPM IP addresses and ports must be coordinated between switches in the OC network. Also, if the Dynamic Host Configuration Protocol (DHCP) is used to configure SX05DA IP addresses, the CM datafill at one end of a link must be consistent with the information provided by the DHCP server at the other end of the link. If the datafill between switches is inconsistent for a data link, it will not be possible to bring the data link into service.

***Note:*** For more discussion, refer to "Parallel datafill for OC-IP data links" on page 91.

### Encryption

A simple encryption algorithm is used on OC-IP data links to protect sensitive data such as passwords, PINs, and credit card numbers. The encryption algorithm is intended to protect data against casual observers of the IP network traffic. It may not be sophisticated enough to withstand serious efforts to decrypt the messages.

## OC-IP voice communication

This section discusses concepts and terms related to OC-IP voice communication.

***Note:*** This section assumes familiarity with TOPS-IP infrastructure for voice communication. Refer to Chapter 2: "TOPS-IP data and voice communication," for more information.

### IP-XPM voice interface

The 7X07AA Gateway card in the IP-XPM provides OC-IP voice communication. The 7X07 converts between circuit-switched voice and packet-switched voice in an OC call.

### Dynamic voice trunks

OC-IP voice links use dynamic trunks to send voice traffic over a data packet protocol. With dynamic trunking, there is no fixed connection to the far end. One implication is that an OC remote switch, for example, can use the same dynamic trunk group to connect to different OC hosts.

### ISUP call processing

From the CM perspective, dynamic voice trunks appear as ISUP trunks that use the Q.764 protocol. However, ISUP is only used between the CM and the IP-XPM. The CM includes proprietary information, such as terminal identifiers (TID), in the ISUP IAM message used to establish a VoIP connection. The SX05DA card in the IP-XPM routes ISUP messages to the 7X07 Gateway card, which converts between ISUP signaling on its C-side and a VoIP signaling protocol on the LAN side.

***Note:*** The SS7 network and associated datafill are *not used* in OC-IP.

### Interactions with IP positions

When a call in an OC remote switch is assigned a traditional TDM-based position in the host switch, the VoIP connection is between 7X07 Gateways in the host and the remote. However, when a call in an OC remote switch is assigned an IP position in the host, the VoIP connection is directly between the position and a 7X07 Gateway in the remote. This is referred to as a *host voice bypass* call, and it uses no voice resources in the host—neither for call signaling nor for bearer.

Host voice bypass improves VoIP quality at the IP position in two ways:

- Reduces the VoIP packet latency (delay) and jitter (variability in the delay) between the OC remote and the position, by eliminating the need to have the host receive and forward each packet. This can reduce one-way latency by 50 to 70 ms.
- Reduces transcoding. Each time speech data undergoes decoding and encoding from one representation to another, some degradation of the signal occurs. This is especially important for calls (such as calls that come to TOPS from the wireless network) that may have already undergone compression and decompression before they reach the OC remote switch.

***Note:*** Refer to Chapter 7: “TOPS-IP engineering guidelines” for information about the impact of host voice bypass on provisioning in an OC host.

The same IP-XPM can support both OC-IP and IP positions.

### Dynamic trunk groups

A 7X07 Gateway card supports 48 dynamic trunk members. All 48 members must be in the same trunk group. An OC host switch can use the same trunk group for connections to all of the OC remotes it serves, if the capacity of a trunk group is sufficient. Similarly, an OC remote can use a single trunk group to connect to all of its OC hosts. However, a combination host/remote switch must use different trunk groups (and thus different Gateways) for its connections to hosts and its connections to remotes.

In an OC remote switch, the same dynamic OC trunk group can be used both for connections with host switches and for connections with positions, in host bypass calls. However, an OC host must use different trunk groups (and thus different Gateways) for its connections to remotes and its connections to the IP positions that it hosts.

### VoIP signaling

To control voice connections across the managed IP network, the Gateways use the SIP protocol in 7X07 software release 4.0 and higher. (Earlier 7X07 software releases used the proprietary IGIP protocol for call signaling.) A streamlined subset of SIP is used when Gateways in an OC host and an OC remote communicate with each other. When a Gateway in an OC remote is communicating directly with an IP position, it uses industry-standard SIP.

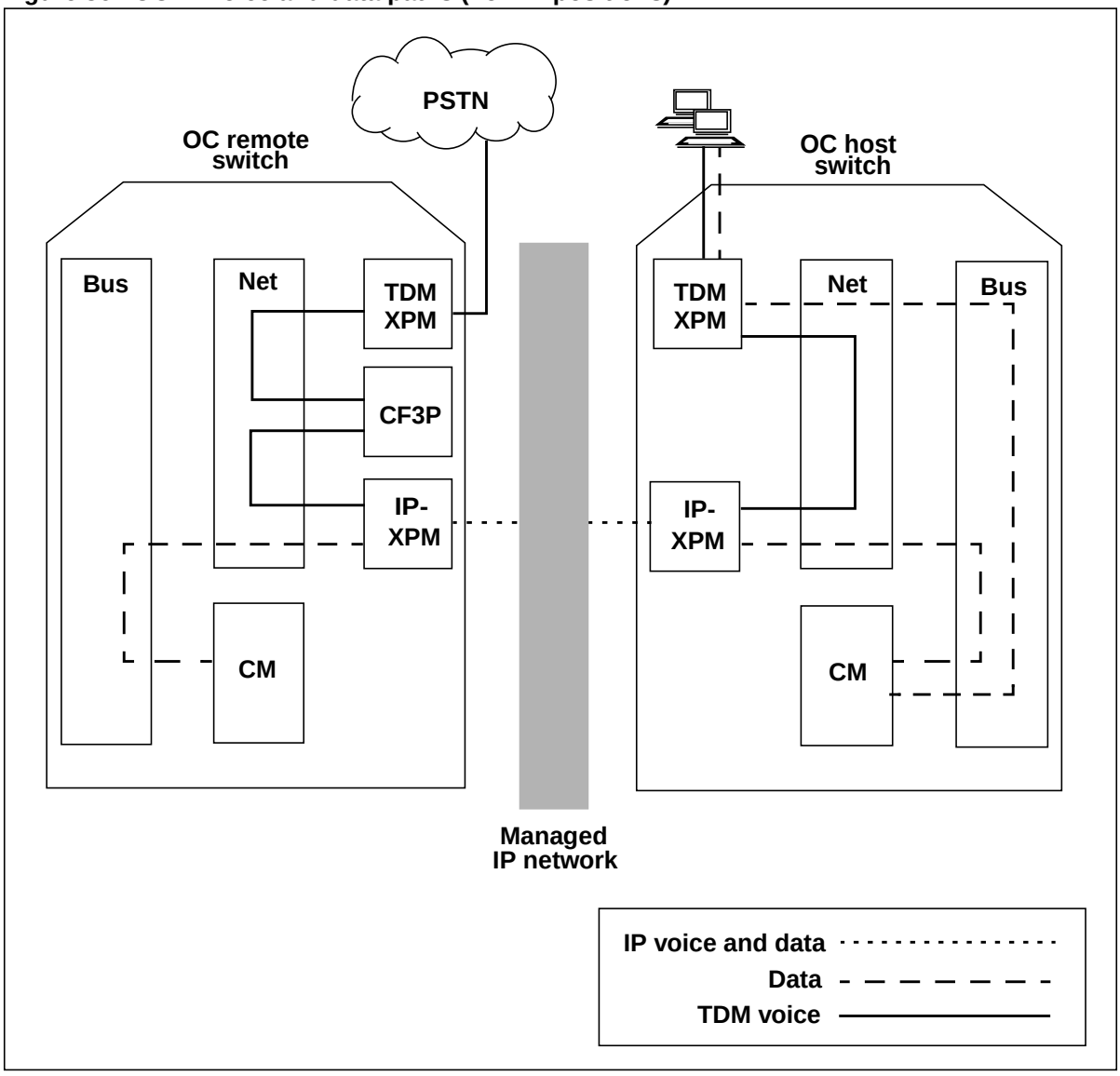
### Voice encoding

The OC-IP application can use two codecs, G.711 and G.723, depending on the packetized voice profile that is datafilled against the call queue. Auto-compression is not supported when the IP voice connection is between the OC remote and OC host (that is, when a traditional TDM position is serving the call). However, auto-compression is supported in host voice bypass calls, where the IP voice connection is between the OC remote and an IP position. Refer to Chapter 4: “TOPS IP position application” for more information about auto-compression.

## OC-IP voice and data paths

Figure 36 illustrates the voice and data paths for an OC-IP call that uses a traditional TDM-based position in the OC host. A description follows the figure.

**Figure 36 OC-IP voice and data paths (non-IP positions)**




***Note:*** Refer to page 121 for a similar figure that includes an IP position and host voice bypass.

In the figure, the subscriber voice path originates at the OC remote switch from a TDM trunk in the public switched telephone network (PSTN), and is connected to a conference circuit (CF3P) through the DMS network. The OC-IP voice link connects to the same CF3P and terminates to the C-side of a 7X07 Gateway card in the remote's IP-XPM. The Gateway converts TDM voice to packetized voice and presents the voice stream to the managed IP network. In the host, a second 7X07 Gateway converts the packetized voice stream back to TDM voice. The TDM voice path in the host is from the C-side of the host's Gateway, through the DMS network to a TDM peripheral and then toward the position.

The CM in the remote switch can originate data messages for the host (OC protocol) and for the position via the host (OPP protocol encapsulated in OC protocol). These messages travel via the remote's DMS Bus (message switch) and network to an SX05DA card in the remote's IP-XPM. The SX05DA packetizes the data and presents it to the managed IP network. The SX05DA in the host's IP-XPM receives the data from the IP network. The data path from there is across the host IP-XPM's C-side links through the DMS network and message switch to the host's CM. Between the host and the position, the data path is the same as it would be without OC-IP.

## Mixing OC-IP and traditional OC

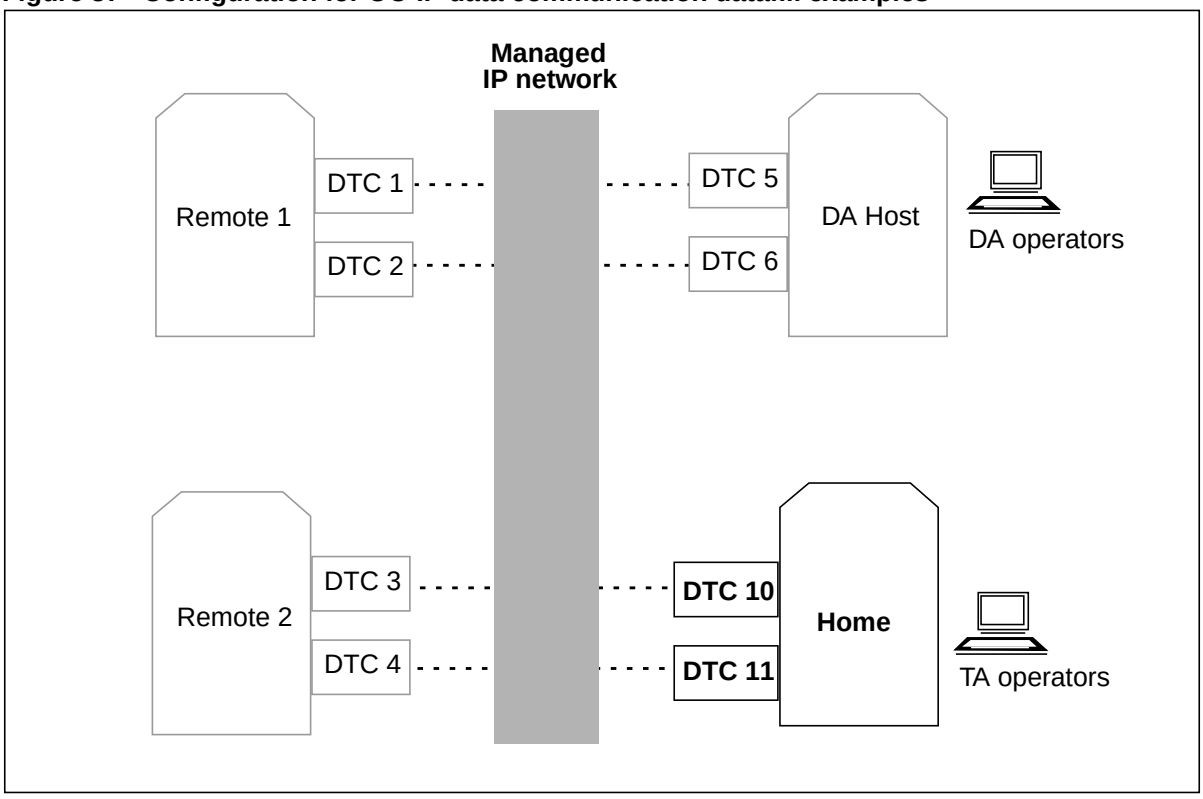
OC-IP and traditional DCM or ETMS OC can no longer coexist in the same switch. TDM-OC links must be replaced by OC-IP links prior to an upgrade to SN08 or higher. Any OCHOST or OCHOSTQ tuple which references a TDM-OC link will cause a TABXFR to halt if not replaced prior to such an upgrade.

Once the host is upgraded to SN08 or higher, a position using an ETMS for data connectivity to a host will not be able to RTS or login. Similarly, after upgrading to SN08, a remote using an ETMS for data connectivity to a host will not be able to send calls to that host. A host using an ETMS for data connectivity to a remote will stop receiving calls from that remote once the remote is upgraded to SN08 or higher.

## Overview of datafill for OC-IP data links

This section introduces the datafill required for OC-IP data links. Throughout this discussion the example datafill is shown for the OC switch labeled "Home" in Figure 37.

**Figure 37 Configuration for OC-IP data communication datafill examples**




The Home switch uses the HRNQT capability, and functions in the following three ways:

- as an OC host for TA calls from switches "Remote 1" and "Remote 2"
- as a standalone switch for TA calls that are routed directly to it from end offices or tandems
- as a remote for DA calls that are routed directly to it from end offices or tandems; its DA operators are provided by the switch "DA Host"

In the example configuration, the Home switch needs OC communication with three distant OC offices. For each distant switch, Home provisions four OC-IP data links—two on each IP-XPM (DTC 10 and DTC 11)—for a total of 12 data links.

This section discusses the data-related tables that are specific to OC-IP and the data-related tables that are part of the base IP infrastructure. For the infrastructure tables, it includes OC-IP application-specific considerations. Each table description includes an example of the datafill for OC-IP data links at the Home switch. The tables are described in the following order:

- LTCINV (Line Trunk Controller Inventory)
- XPMIPGWY (XPM IP Gateway)
- XPMIPMAP (XPM IP Mapping)
- IPSVCS (IP Services)
- IPCOMID (IP Communication Identifier)
- OCOFC (OC Office)
- OCGRP (OC Group)
- OCIPDL (OC-IP Data Link)
- TOPSPARM (TOPS Parameters)

***Note 1:*** Datafill for OC-IP data links is unaffected by whether the calls that use these data links use IP positions or traditional TDM-based positions. All of the examples and discussion in this section apply for both situations. Refer to Chapter 4: “TOPS IP position application” for information about IP position datafill.

***Note 2:*** Refer to Chapter 8: “TOPS-IP data schema” for details on the range of valid datafill for every table affected by TOPS-IP.

## LTCINV

Table LTCINV specifies hardware inventory information for each IP-XPM (excluding the P-side link assignments). TOPS-IP infrastructure considerations for table LTCINV are discussed beginning on page 52. OC-IP data links introduce no application-specific considerations.

In the following example, the Home switch datafills DTC 10 and DTC 11 with the most recent QTP and firmware load names and the circuits that are needed for TOPS-IP data links.

**Figure 38 MAP display example for table LTCINV**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
-------------------------------------------------------------------------------
DTC 10   1001   LTE    0    51    0     C   0    6X02AF  QTP22xx (ABTRK DTCEX)$
   (0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5)
(0 11 0 6) (0 11 0 7) (0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11)
(0 11 0 12) (0 11 0 13) (0 11 0 14) (0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0     6X02AF   QTP22xx (ABTRK DTCEX)$
   (0 11 1 0) (0 11 1 1) (0 11 1 2) (0 11 1 3) (0 11 1 4) (0 11 1 5)
(0 11 1 6) (0 11 1 7) (0 11 1 8) (0 11 1 9) (0 11 1 10) (0 11 1 11)
(0 11 1 12) (0 11 1 13) (0 11 1 14) (0 11 1 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
```

## XPMIPGWY

Table XPMIPGWY specifies gateway router information for SX05DA cards. A gateway router is a component of the managed IP network and is used to forward IP packets to other networks. TOPS-IP infrastructure considerations for table XPMIPGWY are discussed beginning on page 55. OC-IP data links introduce no application-specific considerations.

In the following example, the Home switch datafills two default routers.

**Figure 39 MAP display example for table XPMIPGWY**

```
GWINDEX   DESTADDR       RTEMASK           GWIPADDR       METRIC
-------------------------------------------------------------------
0         0 0 0 0        0 0 0 0           47 192 3 1     0
1         0 0 0 0        0 0 0 0           47 192 3 2     0
```

***Note:*** Home will not actually use this datafill, since it uses the DHCP (network) method for configuring its IP-XPMs. Home did not need to datafill anything in table XPMIPGWY.

### XPMIPMAP

Table XPMIPMAP specifies various IP information for the SX05DA, including the configuration method used when the IP-XPM is brought into service. TOPS-IP infrastructure considerations for table XPMIPMAP are discussed beginning on page 57. OC-IP data links introduce no application-specific considerations.

In the following example, the Home switch datafills the DHCP method for DTC 10 and DTC 11, along with the Ethernet speed specification and subnet mask.

**Figure 40 MAP display example for table XPMIPMAP**

```
XPMNAME  AUTONEG  SUBNMASK       IPCONFIG    ACTADDR       INADDR
      UNIT0         UNIT1              GWINDEX         DNSINFO
-------------------------------------------------------------------------------------
DTC 10   AUTO     255 255 255 0  DHCP
DTC 11   AUTO     255 255 255 0  DHCP
```

***Note 1:*** When the DHCP method is datafilled, the IP-XPM is configured by the DHCP network server, so router datafill in table XPMIPGWY is never used.

***Note 2:*** When the CM method is datafilled, the GWINDEX refinement specifies a list of indexes into table XPMIPGWY. After changing the datafill for GWINDEX, users should update the static data for the SX05DA. For details, refer to “Updating static data” on page 299.

### IPSVCS

Table IPSVCS defines IP transport services for the SX05DA. Each service name represents a software port and transport protocol. The service name is referenced by table IPCOMID. TOPS-IP infrastructure considerations for table IPSVCS are discussed beginning on page 59.

The OC-IP application requires that the protocol be datafilled as UDP. Also, the application does not allow the port to be changed unless all data links that use the IP service are off-line.

Each OC-IP data link associated with a particular IP-XPM must use a different IPSVCS tuple. However, two OC-IP data links associated with different IP-XPMs may use the same IPSVCS tuple.

In the following example, the Home switch defines eight IP transport services for OC-IP data links.

**Figure 41 MAP display example for table IPSVCS**

```
SERVICE              PORT       PROTOCOL
-----------------------------------------------------------------------
REM1_OCIPSVC1        8600       UDP
REM1_OCIPSVC2        8601       UDP
REM1_OCIPSVC5        8604       UDP
REM1_OCIPSVC6        8605       UDP
REM2_OCIPSVC1        8608       UDP
REM2_OCIPSVC2        8609       UDP
DAHOST_OCIPSVC1      8612       UDP
DAHOST_OCIPSVC2      8613       UDP
```

The example illustrates two different strategies for defining IP transport services. Keep in mind that the Home office will have four OC-IP data links—two on each IP-XPM—to each of three offices.

- The first strategy, shown for the data links to Remote 1, is to datafill a unique IP transport service for each OC-IP data link. This is the most straightforward strategy.
- The second strategy, shown for the data links to Remote 2, involves reusing the same set of IP transport services on each IP-XPM. Thus it is necessary to datafill only two services for Remote 2. (The second strategy is also used for DA Host.) This strategy requires a little less datafill. It also uses fewer port numbers, which could be useful if it is difficult for network planners to identify a sufficiently large range of ports for use by OC-IP data links. (See Note 1.)

There is no performance reason for selecting either strategy. The decision depends only on which one the operating company finds easier to manage.

***Note 1:*** The managed IP network can be configured to use port assignments for different applications to manage quality of service, including minimizing loss of OC data link messages. Refer to Chapter 7: “TOPS-IP engineering guidelines,” for the recommended port range and other related information.

***Note 2:*** Each OC switch must know, for each of its data links, which port the distant switch has datafilled for its end of the data link. For more discussion, refer to “Parallel datafill for OC-IP data links” on page 91.

## IPCOMID

Table IPCOMID defines COMIDs. A COMID represents *local* connectivity information for a data link. TOPS-IP infrastructure considerations for table IPCOMID are discussed beginning on page 60.

A separate COMID must be datafilled for each OC-IP data link. The COMID is referenced by table OCIPDL, which associates a data link with it.

The Home switch distributes its OC-IP data connectivity across two IP-XPMs, and each XPM has two data links to each of the three distant offices. In the following example, the Home switch defines the 12 COMIDs needed for its OC-IP data links. Notice that all the COMIDs that are datafilled to use the same IP-XPM have different IP transport services, but the same service can be used for COMIDs on different IP-XPMs.

**Figure 42 MAP display example for table IPCOMID**

```
COMID    SERVICE            XPMNAME
-------------------------------------------------------
4        REM1_OCIPSVC1      DTC 10
5        REM1_OCIPSVC2      DTC 10
8        REM2_OCIPSVC1      DTC 10
9        REM2_OCIPSVC2      DTC 10
12       DAHOST_OCIPSVC1    DTC 10
13       DAHOST_OCIPSVC2    DTC 10
16       REM1_OCIPSVC5      DTC 11
17       REM1_OCIPSVC6      DTC 11
20       REM2_OCIPSVC1      DTC 11
21       REM2_OCIPSVC2      DTC 11
24       DAHOST_OCIPSVC1    DTC 11
25       DAHOST_OCIPSVC2    DTC 11
```

***Note:*** The COMID associated with a data link only specifies information about the local end of the data link. The COMID does not specify anything about the far end of the data link (at the distant switch); this information is defined in table OCIPDL (page 89). For more discussion, refer to “Parallel datafill for OC-IP data links” on page 91.

## OCOFC

Table OCOFC defines the names of offices in the OC network. This table is also used by traditional OC, and the OC-IP application does not change the way it is used. Since Home uses HRNQT and handles some calls as a standalone switch, the Home office is datafilled along with the three distant offices.

***Note:*** OC-IP may use office numbers in the range 1 to 31.

**Figure 43 MAP display example for table OCOFC**

```
VALUE   SYMBOL
-----------------------------------------
1       HOME
2       REMOTE1
3       REMOTE2
5       DAHOST
```

## OCGRP

Table OCGRP provides information about each distant office datafilled in table OCOFC. It identifies each office as a host or a remote, specifies the BCS level of that office, and provides information about the voice and data connectivity to that office. Table OCGRP allows the voice and data paths to be provisioned as either TDM or IP.

***Note:*** IP data connectivity can be used only when IP voice connectivity is used, and vice versa.

The DLOVRLAY field consolidates the data refinements, and the VLGRP field specifies the voice circuit (described on page 103). For OC-IP, the data link selector is IP and there are no further refinements or subfields.

In the following example, the Home switch datafills the three offices with which it has IP data and voice connectivity.

**Figure 44 MAP display example for table OCGRP**

```
OFFICE    OFCTYPE   VLGRP          DLOVRLAY  BCSLEVEL
-------------------------------------------------------------------
REMOTE1   REMOTE    OCIPTOREMOTE   IP        50
REMOTE2   REMOTE    OCIPTOREMOTE   IP        52
DAHOST    HOST      OCIPTOHOST     IP        52
```

***Note 1:*** When the network uses HRNQT, a distant switch may function as both a host and a remote for some other office. In this case, the distant switch must have two different entries in both table OCOFC and table OCGRP. One OCGRP entry identifies it as a host and the other entry identifies it as a remote. Also, a distant switch needs two entries in OCOFC if some of the OC traffic uses OC-IP and some of it uses traditional OC.

***Note 2:*** Although table control allows IP voice and data entries for offices datafilled with BCS 48 or higher, the OC-IP application is not supported unless both the host and the remote are at BCS 50 (TOPS15) or higher.

## OCIPDL

Table OCIPDL defines the OC-IP data links that are used to communicate with each distant office. It also provides local and distant endpoint information about each link.

The two-part key consists of a distant office name and a data link number (0 to 7). Up to eight data links can be datafilled against each distant office. The distant office name must already be defined in table OCGRP with an IP data selector. The COMID identifies a tuple in table IPCOMID, which indirectly specifies the port, protocol, and IP-XPM used for the *local* end of the data link.

The IP address and port number fields directly specify the socket that the *distant* office uses for its end of the data link. This IP address is the active side IP address of the SX05DA that supports the distant office's end of the data link. For more discussion, refer to "Parallel datafill for OC-IP data links" on page 91.

In the following example, the Home switch datafills four data links for each distant office, for a total of 12.

**Figure 45 MAP display example for table OCIPDL**

```
OCDLKEY      COMID   IPADDR              PORT
-------------------------------------------------------
REMOTE1 0    4       47 192 201 112      8600
REMOTE1 1    5       47 192 201 112      8601
REMOTE1 4    16      47 192 201 212      8604
REMOTE1 5    17      47 192 201 212      8605
REMOTE2 0    8       47 192 218 140      8644
REMOTE2 1    9       47 192 218 140      8654
REMOTE2 4    20      47 192 218 240      8684
REMOTE2 5    21      47 192 218 240      8694
DAHOST 0     12      47 192 63 100       8606
DAHOST 1     13      47 192 63 100       8607
DAHOST 4     24      47 192 63 200       8610
DAHOST 5     25      47 192 63 200       8611
```

## TOPSPARM

Table TOPSPARM contains TOPS-specific office parameters. The OCIPDL_AUDIT_THRESHOLD parameter specifies how many consecutive audit failures are allowed before the state of an OC-IP data link is changed from INSV to SYSB. Audits are performed every 5 seconds. The range of values is 2 to 10 failures and the default is 3.

***Note:*** For more information on OC-IP data link maintenance, refer to Chapter 10: "TOPS-IP maintenance activities."

In the following example, the Home switch sets the audit threshold to 3 failures.

**Figure 46 MAP display example for table TOPSPARM**

```
PARMNAME                 PARMVAL
-------------------------------------------------------------
OCIPDL_AUDIT_THRESHOLD   3
```

## Parallel datafill for OC-IP data links

Datafill for the local and far-end OC-IP data link connectivity must be parallel between nodes on the network. This ensures that data messages can be routed to the correct IP-XPM and to the correct application software. A data link cannot be brought into service unless the datafill is consistent.

This section discusses the parallel datafill requirements for the IP configuration methods (identified in the IPCONFIG field in table XPMIPMAP), as follows:

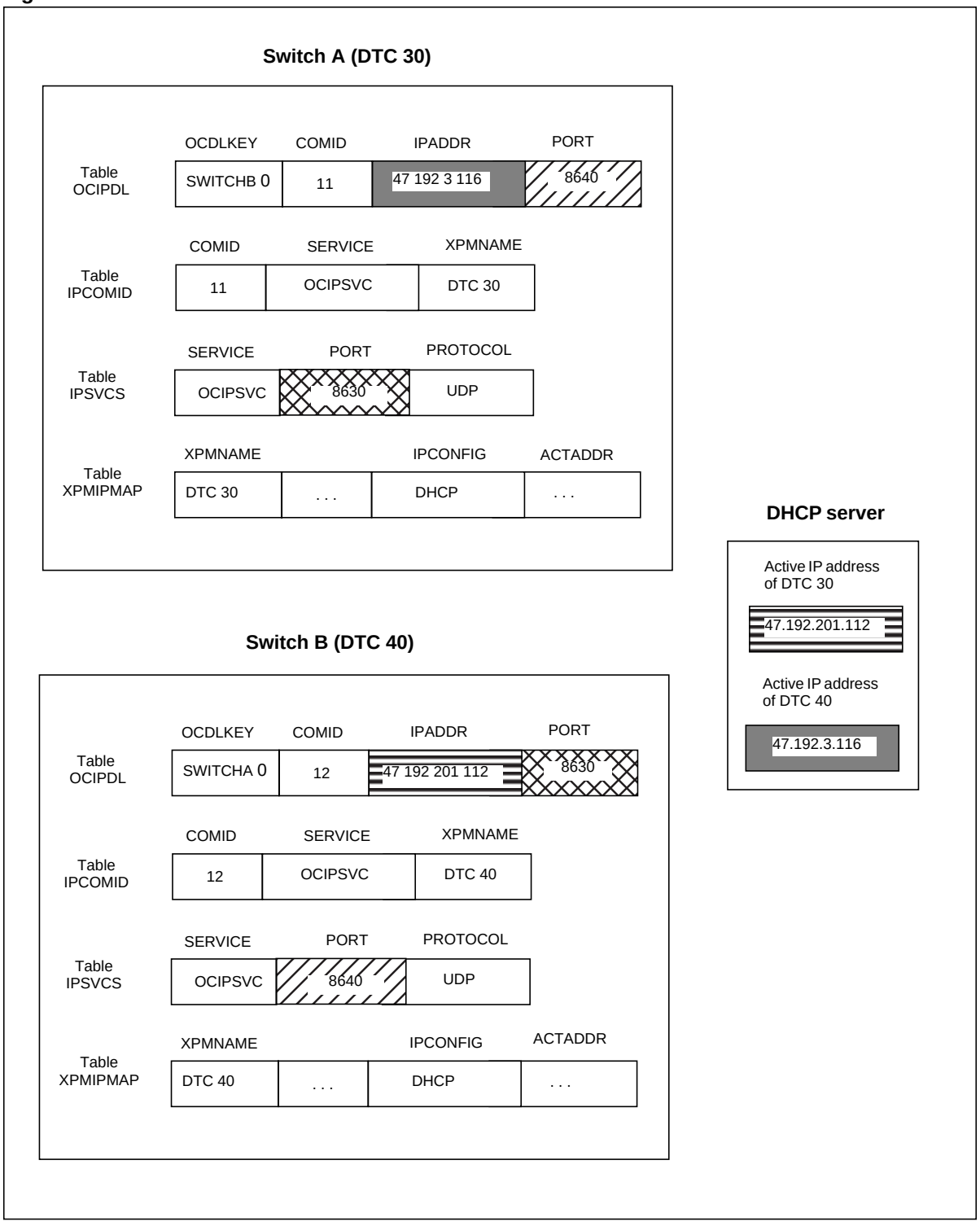
- network method (DHCP)
- CM method

### Network method

When using the DHCP method, the IP-XPM receives its active IP address from a DHCP server in the network. Figure 47 illustrates the parallel datafill required between OC switches and the DHCP server. Fields showing the same background pattern must have the same datafill.

As shown in the figure, the IP address provided to Switch A by the network must match the IPADDR value in table OCIPDL at Switch B, and vice versa. Also, the PORT value in table IPSVCS at Switch A must be the same one as the PORT value in OCIPDL at Switch B.

**Figure 47 Parallel datafill for OC-IP data links—network method**

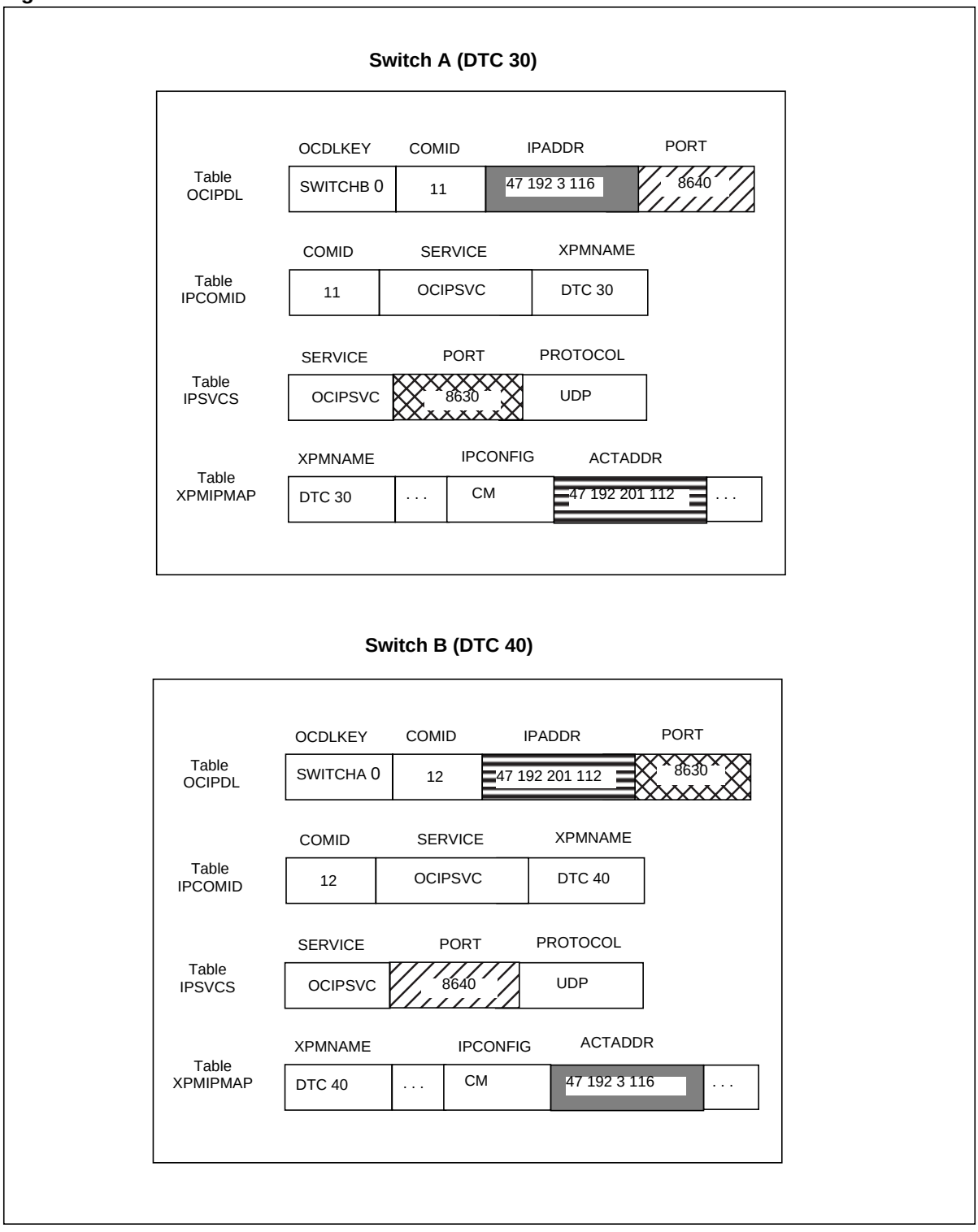


### CM method

When using the CM method, the IP-XPM obtains its IP information from CM datafill. At either switch, the local data link connectivity information is contained in table XPMIPMAP in the ACTADDR field, and in table IPSVCS in the PORT field. The distant data link connectivity information is contained in table OCIPDL in fields IPADDR and PORT. Figure 48 illustrates the parallel datafill required between two OC switches. Fields showing the same background pattern must have the same datafill.

As shown in the figure, for a given data link to have parallel datafill between Switch A and Switch B, the ACTADDR value in XPMIPMAP at Switch A (local) must match the IPADDR value in OCIPDL at Switch B (distant). And the PORT value in IPSVCS at Switch A (local) must match the PORT value in OCIPDL at Switch B (distant).

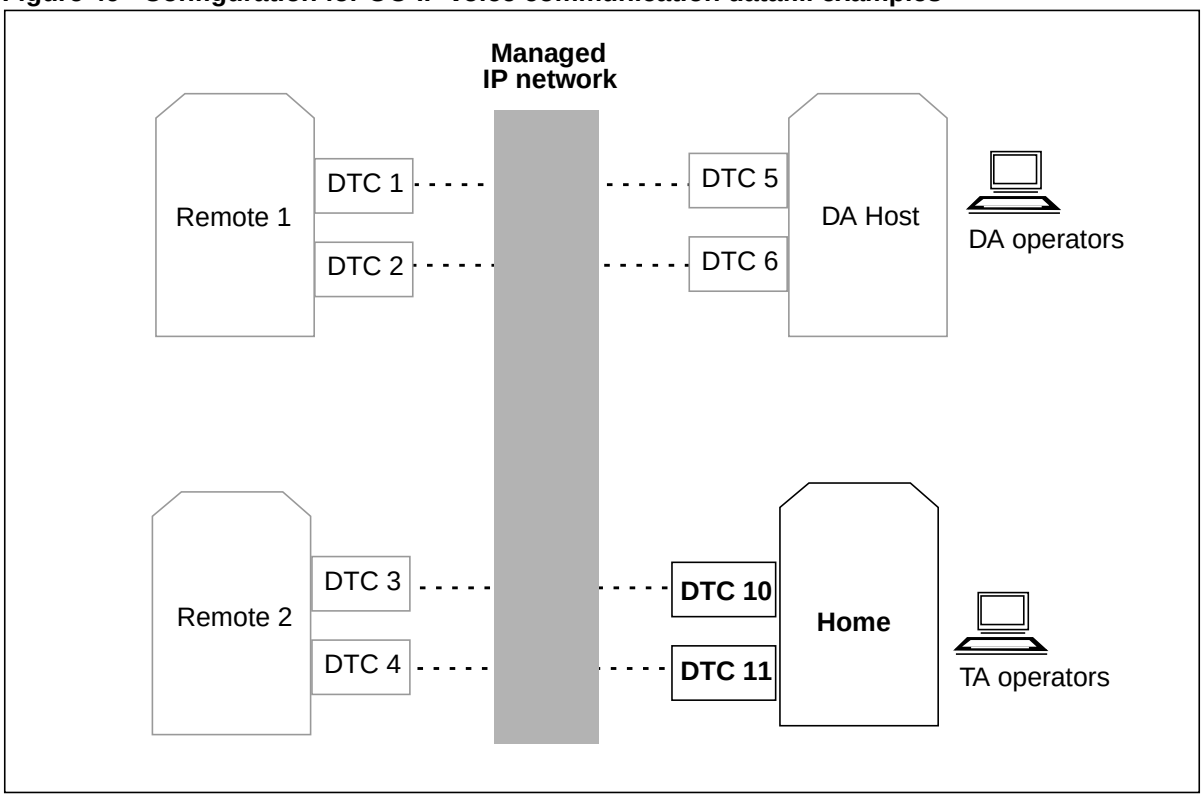
**Figure 48 Parallel datafill for OC-IP data links—CM method**



## Overview of datafill for OC-IP voice links

This section introduces the datafill required for OC-IP voice links. Again, throughout this discussion the example datafill is shown for the OC switch labeled “Home” in Figure 49.

**Figure 49 Configuration for OC-IP voice communication datafill examples**




This section discusses the voice-related tables that are specific to OC-IP and the voice-related tables that are part of the base IP infrastructure. For the infrastructure tables, it includes OC-IP application-specific considerations. Each table description includes an example of the datafill for OC-IP voice links at the Home switch. The tables are described in the following order:

- LTCINV (LTC Inventory)
- CARRMTC (Carrier Maintenance)
- LTCPSINV (LTC P-side Inventory)
- CLLI (Common Language Location Identifier)
- TRKGRP (Trunk Group)
- TRKSGRP (Trunk Subgroup)
- TRKOPTS (Trunk Options)
- SITE (Site)
- IPINV (IP Inventory)
- TRKMEM (Trunk Members)

- TOPSTOPT (TOPS Trunk Options)
- OFCENG (Office Engineering)
- PKTVPROF (Packetized Voice Profile)
- TQCQINFO (TOPS QMS Call Queue Information)
- OCGRP (Operator Centralization Group)

***Note 1:*** Datafill for OC-IP voice links is essentially the same regardless of whether the OC-IP calls are expected to be served by operators at IP positions or operators at traditional TDM-based positions. This section notes where there are differences.

One difference not fully discussed in this section, however, is the effect of host voice bypass on engineering rules for 7X07 Gateway cards. Refer to Chapter 7: "TOPS-IP engineering guidelines" for more information.

***Note 2:*** Refer to Chapter 8: "TOPS-IP data schema" for details on the range of valid datafill for every table affected by TOPS-IP.

## LTCINV

Table LTCINV contains the inventory datafill (excluding the P-side link assignments) for IP-XPMs. TOPS-IP infrastructure considerations for table LTCINV are discussed beginning on page 52. OC-IP voice links introduce no application-specific considerations.

In the following example, the Home switch datafills DTC 10 and DTC 11 with the North American toneset, which is required to satisfy table control and diagnostics, and with the other information that is required for TOPS-IP.

**Figure 50 MAP display example for table LTCINV**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
-------------------------------------------------------------------------------
DTC 10   1001   LTE    0    51    0     C   0    6X02AF  QTP22xx (ABTRK DTCEX)$
   (0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5) (0 11 0 6)
(0 11 0 7) (0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11) (0 11 0 12) (0 11 0 13)
(0 11 0 14) (0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0    6X02AF   QTP22xx (ABTRK DTCEX)$
   (0 11 1 0) (0 11 1 1) (0 11 1 2) (0 11 1 3) (0 11 1 4) (0 11 1 5) (0 11 1 6)
(0 11 1 7) (0 11 1 8) (0 11 1 9) (0 11 1 10) (0 11 1 11) (0 11 1 12) (0 11 1 13)
(0 11 1 14) (0 11 1 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02     (CCS7) $
       6X40FC    N
```

## CARRMTC

Table CARRMTC specifies maintenance control information for the IP-XPM. TOPS-IP infrastructure considerations for table CARRMTC are discussed beginning on page 53. OC-IP voice links introduce no application-specific considerations.

In the following example, the Home switch datafills carrier maintenance information for the type of IP-XPM (DTC) used for OC-IP voice.

**Figure 51 MAP display example for table CARRMTC**

```
CSPMTYPE TMPLTNM  RTSML  RTSOL  ATTR
-------------------------------------------------------------------------------
DTC      TGWY     255    255    DS1 NT7X07AA  MU_LAW SF ZCS BPV NILDL N 250 1000
50 50 150 1000 3 6 864 100 17 511 4 255
```

## LTCPSINV

Table LTCPSINV contains the IP-XPM's P-side link assignments for the 7X07 Gateway cards. TOPS-IP infrastructure considerations for table LTCPSINV are discussed beginning on page 54. OC-IP voice links introduce no application-specific considerations.

In the following example, the Home switch datafills P-side links 6 through 11 for DTC 10 and DTC 11. These links will support three Gateways on each IP-XPM. The even-numbered links will be datafilled as the port numbers in table IPINV (page 100).

**Figure 52 MAP display example for table LTCPSINV**

```
LTCNAME   PSLINKTAB
-------------------------------------------------------------------------------
DTC 10    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE)(4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N) (8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $

DTC 11    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE)(4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N) (8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $
```

## CLLI

Table CLLI specifies trunk group names and the maximum number of members in each trunk group. TOPS-IP infrastructure considerations for table CLLI are discussed beginning on page 61.

Unlike traditional OC, in which a different trunk group is required for connecting to each distant office, OC-IP allows a pure host or a pure remote to use a single trunk group for connecting to all distant offices. A hybrid host/remote will need one trunk group for all connections to hosts and another trunk group for all connections to remotes.

Although it is *allowed* for a pure host or a pure remote to datafill multiple dynamic OC trunk groups, it is not recommended (unless needed for capacity reasons) because of its impact on sparing. As described in Chapter 7: "TOPS-IP engineering guidelines," N+1 redundancy of 7X07 Gateway cards is needed for each trunk group.

An OC remote can use the same trunk group for all of its OC-IP calls, regardless of whether the host provides a traditional TDM-based position or an IP position. In an OC host, however, different trunk groups are needed for connecting to remotes and for connecting to hosted positions.

In the following example, the Home switch datafills two trunk groups, one for all of its connections to hosts (including hosts that have IP positions), and one for all of its connections to remotes. Since Home does not host any IP positions, it does not need a third trunk group.

**Figure 53 MAP display example for table CLLI**

```
CLLI            ADNUM      TRKGRSIZ     ADMININF
-----------------------------------------------------------------
OCIPTOREMOTE    356        2016         OCIP_TOREMOTE_VOICE_LINK
OCIPTOHOST      367        2016         OCIP_TOHOST_VOICE_LINK
```

## TRKGRP

Table TRKGRP specifies the trunk group type, direction, and other information for each trunk group. TOPS-IP infrastructure considerations for table TRKGRP are discussed beginning on page 61.

The OC-IP application has these requirements for trunk group direction:

- If the trunk group will be datafilled against host office(s) in table OCGRP, its direction must outgoing (OG).
- If the trunk group will be datafilled against remote office(s) in table OCGRP, its direction must be two-way (2W).

Table OCGRP, where voice trunks are associated with offices, enforces this restriction. An OG dynamic trunk group in the remote can be used for calls that get TDM positions in the host, and also for calls that get IP positions in the host (and therefore use host voice bypass).

In the following example, the Home switch datafills the two trunk groups it defined in table CLLI.

**Figure 54 MAP display example for table TRKGRP**

```
GRPKEY          GRPINFO
-----------------------------------------------------------------
OCIPTOREMOTE    IT 0 NPDGP NCRT 2W OA MIDL 000 NPRT NSCR 619 000 N N $
OCIPTOHOST      IT 0 NPDGP NCRT OG OA MIDL 000 NPRT NSCR 619 000 N N $
```

### TRKSGRP

Table TRKSGRP defines additional trunk group information such as signaling. TOPS-IP infrastructure considerations for table TRKSGRP are discussed beginning on page 62. OC-IP voice links introduce no application-specific considerations.

In the following example, the Home switch datafills OCIPTOREMOTE and OCIPTOHOST with ISUP signaling information.

**Figure 55 MAP display example for table TRKSGRP**

```
SGRPKEY    CARDCODE SGRPVAR  SGRPVAR
-------------------------------------------------------------------------------
OCIPTOREMOTE 0 DS1SIG C7UP   2W N N UNEQ NONE Q764 THRL 0 NIL $ NIL CIC
OCIPTOHOST 0  DS1SIG  C7UP   OG N N UNEQ NONE Q764 THRL 0 NIL $ NIL
```

***Note:*** The SS7 network and associated datafill are *not used* in OC-IP.

### TRKOPTS

Table TRKOPTS specifies additional trunk group options, including the dynamic option required by TOPS-IP voice trunks. TOPS-IP infrastructure considerations for table TRKOPTS are discussed beginning on page 62.

For OC-IP voice trunks, the application field in table TRKOPTS must be set to OC.

In the following example, the Home switch datafills OCIPTOREMOTE and OCIPTOHOST as dynamic IP trunk groups used for the OC application.

**Figure 56 MAP display example for table TRKOPTS**

```
OPTKEY                OPTINFO
-------------------------------------------------------------
OCIPTOREMOTE DYNAMIC  DYNAMIC ISUP IP IP OC
OCIPTOHOST DYNAMIC    DYNAMIC ISUP IP IP OC
```

***Note:*** A dynamic OC trunk group in an OC remote can be used to connect to a 7X07 Gateway card in a host (when the host provides a traditional TDM-based position), and it can be used to connect directly to an IP position provided by an OC host. It cannot be datafilled in table TOPSPOS or used to connection to an IP position on a standalone call.

### SITE

Table SITE identifies a site name associated with the 7X07 Gateway cards datafilled at the switch. TOPS-IP infrastructure considerations for table SITE are discussed beginning on page 63. OC-IP voice links introduce no application-specific considerations.

In the following example, the Home switch datafills the site name TGWY.

**Figure 57 MAP display example for table SITE**

```
NAME   LTDSN  MODCOUNT OPVRCLLI ALMDATA
-------------------------------------------------------
TGWY   0      0        VER90    $
```

***Note:*** As Gateways are added to and removed from table IPINV, the system automatically updates the MODCOUNT field to reflect the number of Gateways on the site.

### IPINV

Table IPINV defines the individual 7X07AA Gateway cards (nodes) at the switch. For Gateways used for TOPS-IP applications, IPINV datafill includes the name of a dynamic trunk group from which the switch *automatically* datafills a block of 48 members in table TRKMEM, when the tuple is added to table IPINV.

TOPS-IP infrastructure considerations for table IPINV are discussed beginning on page 63. OC-IP voice links introduce no application-specific considerations.

In the following example, the Home switch datafills six TGWY cards across DTC 10 and DTC 11. Associated with the Gateway cards are the OCIPTOREMOTE and OCIPTOHOST trunk groups, each of which supports 144 members.

**Figure 58 MAP display example for table IPINV**

```
IPNO       PMTYPE PMNO IPPEC  LOAD PORT  IPZONE              GWTYPE
-------------------------------------------------------------------------------
TGWY 10 3  DTC    10   7X07AA  $    6    47 174 68 7 0 0 0 0  TOPS OCIPTOREMOTE 0
TGWY 10 4  DTC    10   7X07AA  $    8    47 174 68 8 0 0 0 0  TOPS OCIPTOHOST 0
TGWY 10 5  DTC    10   7X07AA  $    10   47 174 68 9 0 0 0 0  TOPS OCIPTOREMOTE 48
TGWY 11 3  DTC    11   7X07AA  $    6    47 174 69 7 0 0 0 0  TOPS OCIPTOHOST 48
TGWY 11 4  DTC    11   7X07AA  $    8    47 174 69 8 0 0 0 0  TOPS OCIPTOREMOTE 96
TGWY 11 5  DTC    11   7X07AA  $    10   47 174 69 9 0 0 0 0  TOPS OCIPTOHOST 96
```

***Note 1:*** The DTC P-side links must first be assigned in table LTCPSINV (page 97). The PORT entry in table IPINV is the lower of the two P-side link numbers for that Gateway. For more detailed information on port mapping, see “LTCPSINV-to-IPINV port mapping” on page 249.

***Note 2:*** The example datafill shown in Figure 58 causes automatic datafill of the following trunk members in table TRKMEM:

- OCIPTOREMOTE 0 to 47, 48 to 95, and 96 to 143
- OCIPTOHOST 0 to 47, 48 to 95, and 96 to 143

***Note 3:*** Refer to table TOPSTOPT (page 101) for datafill that limits the number of trunks that may be used by call processing.

## TRKMEM

Table TRKMEM defines the individual trunk members associated with a trunk group. In the case of trunks defined as DYNAMIC OC in table TRKOPTS, no manual datafill in TRKMEM is allowed because tuples are automatically datafilled by table IPINV.

TOPS-IP infrastructure considerations for table TRKMEM are discussed beginning on page 66. OC-IP voice links introduce no application-specific considerations.

The following example shows part of the datafill that would be automatically added to table TRKMEM in the Home switch.

**Figure 59 MAP display example for table TRKMEM**

```
CLLI          EXTRKNM SGRP MEMVAR
-------------------------------------------------
OCIPTOREMOTE 0        0    DTC 10 6 1
OCIPTOREMOTE 1        0    DTC 10 6 2
OCIPTOREMOTE 2        0    DTC 10 6 3
 . . . . . .
OCIPTOREMOTE 143      0    DTC 11 9 24
OCIPTOHOST 0          0    DTC 10 8 1
OCIPTOHOST 1          0    DTC 10 8 2
OCIPTOHOST 2          0    DTC 10 8 3
 . . . . . .
OCIPTOHOST 143        0    DTC 11 11 24
```

## TOPSTOPT

Table TOPSTOPT specifies options for TOPS trunk groups. For dynamic trunks, the MAXCONNS field controls the maximum number of trunks that may be used by call processing. TOPS-IP infrastructure considerations for table TOPSTOPT are discussed beginning on page 67. OC-IP voice links introduce no application-specific considerations.

In the following example the Home switch datafills MAXCONNS, limiting to 60 the number of trunks that can be used for call processing in each of its dynamic OC trunk groups.

**Figure 60 MAP display example for table TOPSTOPT**

```
GRPKEY    ORGAREA  DISPCLG  ADASERV  ADASANS  ANITOCLI  OLNSQRY  DCIBIDX
  LNPCLGAM     XLASCHEM  SPIDPRC  TRKSPID  BILLSCRN  ANIFSPL  MAXCONNS  DISPSPID
-------------------------------------------------------------------------------
OCIPTOREMOTE N      N       NONE      NA        N         NONE        0
  N              N         N         N         N         N       60        N
OCIPTOHOST   N      N       NONE      NA        N         NONE        0
  N              N         N         N         N         N       60        N
```

## OFCENG

Table OFCENG contains office-wide parameters. TOPS-IP infrastructure considerations for table OFCENG are discussed beginning on page 68.

For the OC-IP application, NUMPERMEXT does *not* need to be incremented for members of trunk groups that connect to OC remotes (datafilled in table TRKGRP with direction 2W). It only needs to be incremented for trunk groups that connect to OC hosts (or IP positions).

In the following example, the Home switch leaves IPGW_PCM_SELECTION at its default value and increases the existing value of NUMPERMEXT from 100 to 244 to account for the 144 members in the OCIPTOHOST trunk group.

**Figure 61 MAP display example for table OFCENG**

```
PARMNAME                    PARMVAL
-------------------------------------------------------------
IPGW_PCM_SELECTION          AUTO
NUMPERMEXT                  244
TOPS_NUM_OC_EXT             1000
TOPS_OC_ENVIRONMENT         HOST
```

The example also shows parameters TOPS_NUM_OC_EXT and TOPS_OC_ENVIRONMENT, which are unchanged for TOPS-IP but are related to OC in general.

- TOPS_NUM_OC_EXT specifies the number of OC extension blocks allocated for traffic in the OC host. One OC extension block is needed for each call in the OC host that is either at position or queued for an operator. None are needed in a pure OC remote or standalone TOPS switch.
- TOPS_OC_ENVIRONMENT specifies whether the switch is an OC host or an OC remote. It is not typically consulted when Host Remote Networking by Queue Type (HRNQT) is used.

## PKTVPROF

Table PKTVPROF defines profiles used for packetized voice. TOPS-IP infrastructure considerations for table PKTVPROF are discussed beginning on page 69.

For OC-IP, table PKTVPROF is referenced by table TQCQINFO. If the IP voice connection for an OC-IP call is between 7X07 Gateways in the OC remote and host switches (that is, if the call gets a traditional TDM-based position in the host), only the CODEC field of the PKTVPROF tuple is consulted. Even if auto-compression is datafilled, it is not used in Gateway-to-Gateway connections. If the OC-IP voice connection is with an IP position, however, both the CODEC and the AUTOCOMP fields are consulted. OC-IP supports auto-compression on host voice bypass calls, where the far end of the VoIP connection is an IP position.

***Note:*** Refer to Chapter 4: "TOPS IP position application" for more information about auto-compression.

In the following example, the Home switch datafills three packetized voice profiles.

**Figure 62 MAP display example for table PKTVPROF**

```
PROFNUM  CODEC  AUTOCOMP
-------------------------------------------------------------------------
0        G711   N
1        G723   N
2        G711   Y G723
```

***Note:*** As explained on page 70, table PKTVPROF was significantly changed in TOPS19, and patch CFX84 modifies the interpretation of PKTVPROF datafill in loads earlier than TOPS19.

### TQCQINFO

Table TQCQINFO provides information about TOPS call queues, including a packetized voice profile index that applies to the call queue. In the following example, the Home switch specifies packetized voice profile index 0, for G.711 voice encoding, against several call queues.

**Figure 63 MAP display example for table TQCQINFO**

```
QTYPE  QMSSERV  CWOFF  CWON   TREAT  ALTAREA  PKTVPROF
-----------------------------------------------------------
CQ131  TOPS_TA  500    1000   VACT    N         0
CQ132  TOPS_TA  500    1000   VACT    N         0
CQ133  TOPS_TA  500    1000   VACT    N         0
```

***Note:*** If Home expected IP positions at DAHOST to serve its OC remote calls, and if the OSC for DAHOST were provisioned to require auto-compression, then Home would have datafilled 2 in the PKTVPROF field for all call queues.

### OCGRP

Table OCGRP identifies each distant office referenced in table OCOFC (page 88) as a host or remote. Datafill associates an OC-IP voice trunk group with a particular office.

In the following example, the Home switch associates OCIPTOREMOTE with both OC remote switches, REMOTE1 and REMOTE2. It associates OCIPTOHOST with the OC host switch, DAHOST.

**Figure 64 MAP display example for table OCGRP**

```
OFFICE    OFCTYPE   VLGRP           DLOVRLAY  BCSLEVEL
-------------------------------------------------------------------
REMOTE1   REMOTE    OCIPTOREMOTE    IP        52
REMOTE2   REMOTE    OCIPTOREMOTE    IP        54
DAHOST    HOST      OCIPTOHOST      IP        54
```

# OC-IP call processing

This section shows a successful OC-IP call flow and discusses various failure scenarios.

## Successful OC-IP call flow

Figure 65 describes an example OC-IP call that uses a traditional TDM position. The example illustrates the use of voice and data links. The arrows represent both data link messages (OC and position) and voice-related call control messages (SIP).

***Note:*** Refer to page 144 for a call flow in which the OC-IP call uses an IP position.

**Figure 65 Example OC-IP call flow with traditional position**

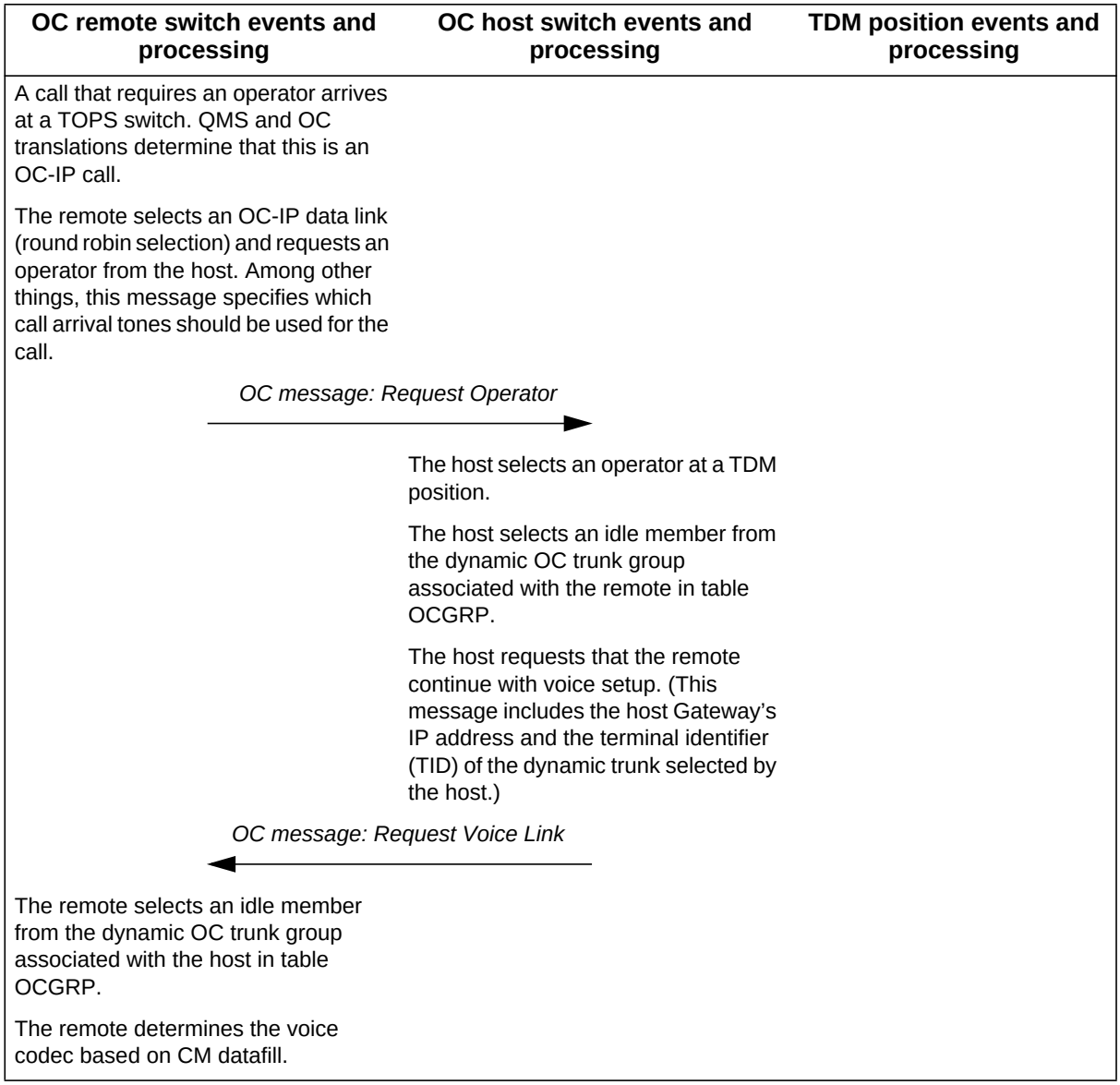


**Figure 65 Example OC-IP call flow with traditional position**

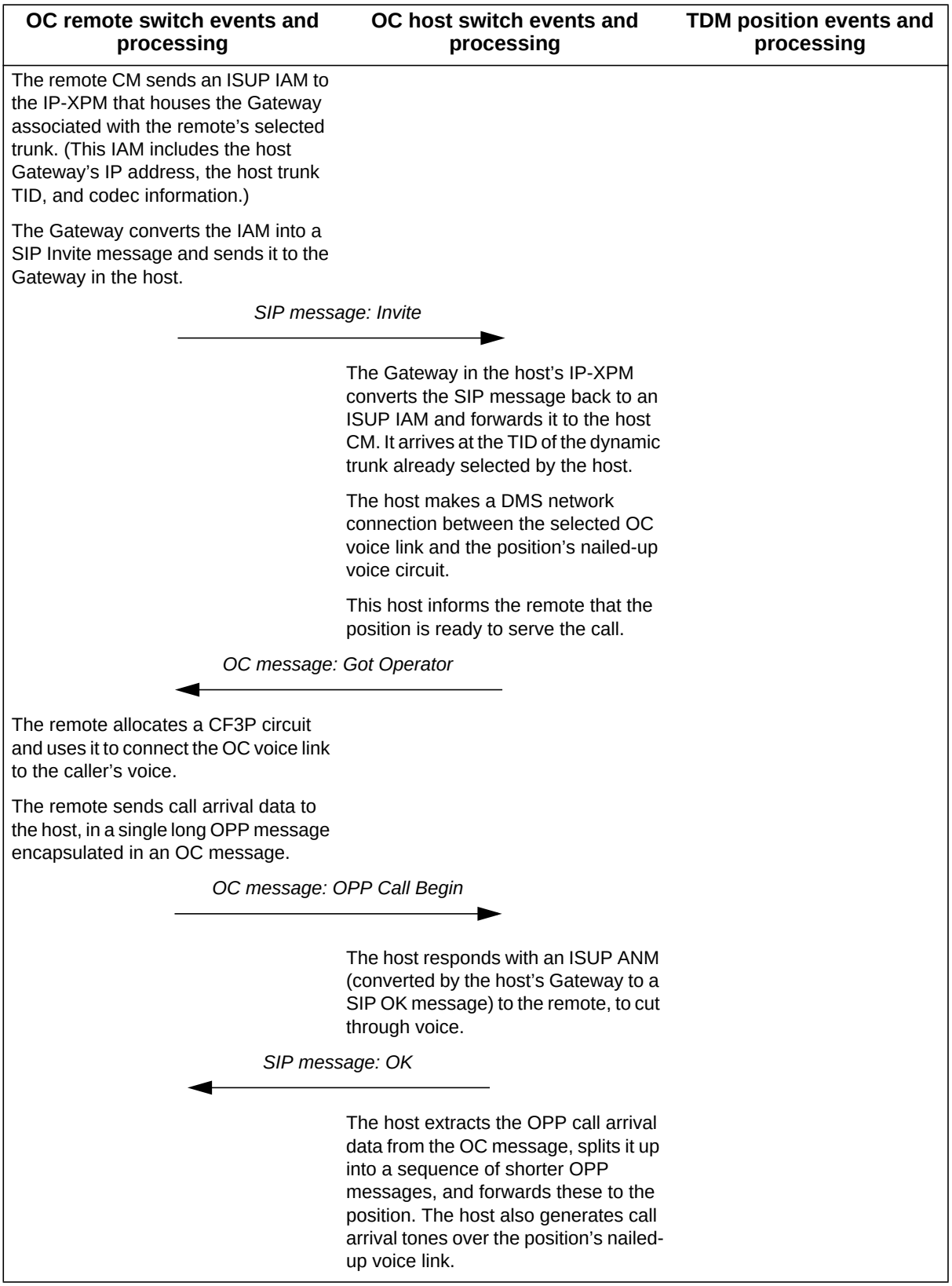
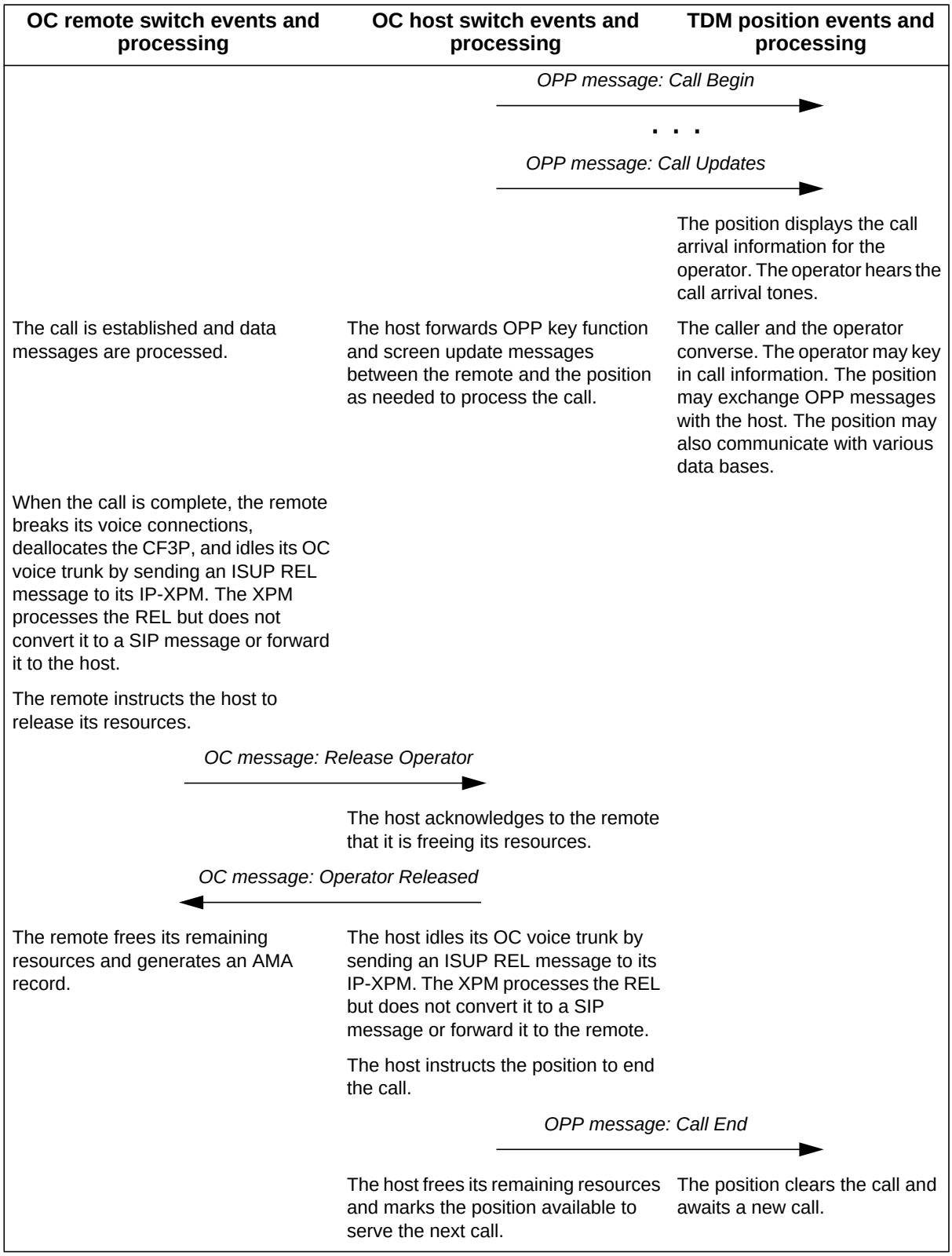


**Figure 65 Example OC-IP call flow with traditional position**



## Failure handling

During OC-IP call processing, various failures are possible in resource allocation, messaging, and DMS switch network connections. Call processing handles OC-IP failures in much the same way as it handles traditional OC failures.

The general failure-handling strategy is to requeue or reroute a call when possible. Requeuing or rerouting is normally possible for failures that occur during call setup. It is not normally possible to recover from failures that are detected after the call has been successfully presented to an operator; these failures usually cause the call to be ended. When a failure occurs, the switch generates appropriate log reports.

***Note:*** For details on logs, refer to Chapter 12: "TOPS-IP logs."

Following are descriptions of the requeuing and rerouting failure-handling strategies:

- **Requeuing** places the call back into the same queue at the same host, with the expectation that the failure was transient and will probably not reoccur the next time an operator is selected.

  When a call is requeued because of a resource shortage, the position that was originally selected for the call is placed in the "make busy" state. Positions in this state do not receive new calls, and they display as CRES at the MAP (see "IP position maintenance" beginning on page 340 for more information). Force management systems are informed of the state change. The switch sends the position a message informing it of its new state, and (assuming the IWS receives the message) the IWS drops to the assigned activities screen. The operator can key Start to re-enter the call processing screen and receive new calls.

- **Rerouting** causes the call to be routed to a different destination following the failure—either to an alternate host or to treatment. Datafill in table OCHOSTQ determines whether the call is rerouted to an alternate host or to treatment. An alternate host is tried if one is datafilled in table OCHOSTQ for the call's reroute reason. If an alternate host is not datafilled, the call is routed to treatment. In that case, the treatment datafilled in table TQCQINFO is used if deflection is permitted for the call, and otherwise CQOV (CAMA queue overflow) treatment is used.

The requeuing strategy is generally employed when there is a presumably-temporary shortage of a necessary resource, such as CF3P circuits or recording units, in the OC remote or host switch. The rerouting strategy is used for certain resource shortages, as explained later in this section, and also when the OC remote switch detects a problem in communicating with the host switch during call setup. The alternate host for an OC-IP call can be another OC-IP host or even the switch at which the processing is occurring (changes the call from OC to standalone). Unless otherwise noted in this section, the OCHOSTQ reroute reason used for OC-IP call setup failure is DEFLECT.

### Resource failures

The following resource failures may affect OC-IP processing:

- *No available virtual circuits (for data)*. If the remote already has 2048 calls queued or at position in the host, it will be unable to get a virtual circuit to the host. The call is then rerouted as described previously.
- *No available voice circuits*. If either the host or the remote cannot obtain a voice link for the call, the call is rerouted.
- *No available RU or CF3P*. If the remote cannot allocate an RU or a CF3P for the call, the call is requeued.
- *One data link to an office goes out of service*. New calls will not select an out-of-service data link. If a data link that has been assigned to a call goes out of service while the call is in progress, the call detects this on the next message it tries to send, and switches to an in-service data link to the same office.

  ***Note:*** It takes a certain amount of time for the switch to detect a fault, depending on the type of fault. After a data link has become unusable and before the system has removed it from service, calls may be adversely affected.
- *All data links to an office go out of service*. If a call in the remote initially attempts to select a data link to request an operator but finds no in-service links to the host, the call is rerouted according to OCHOSTQ datafill with reason DLFAIL.

  If a call has successfully allocated an in-service data link but that link goes out of service while the call is in progress, and if there is no other in-service link that the call can switch to, the call is terminated in the switch that detected the failure.

  Since there is no connectivity between the host and the remote, the switch that detected the failure cannot notify the other switch to terminate its half of the call. The problem may be detected by a connectivity audit time-out at the other end, or it may be detected when the subscriber goes on-hook in the remote (if the problem was first detected in the host) or when the operator keys on the call (if the problem was first detected in the remote). When the other end detects the problem, it terminates its part of the call and frees its resources.

## Messaging and connection problems

OC-IP SIP and data link messages use the UDP protocol over the managed IP network. The advantages of UDP are in simplicity and low real-time and bandwidth consumption. However, these advantages can potentially affect reliability in an improperly engineered network. UDP does not employ end-to-end acknowledgments or retransmission, nor does it guarantee that messages are delivered in the same sequence in which they are sent. With a properly engineered network, it should be rare for these UDP messages to be significantly delayed, lost, or delivered out of sequence.

Depending on where in the call flow a messaging problem occurs, the impact can range from slow response at the operator position to call take-down. The DMS switch does attempt to recover from problems when possible, using strategies similar to those used with TDM-based OC. However, recovery is not always possible, and it is the responsibility of the operating company to engineer the DMS switch and the managed IP network so that these problems are very rare.

***Note:*** For more information on engineering considerations for TOPS-IP, refer to Chapter 7: "TOPS-IP engineering guidelines."

The following messaging or connectivity problems may affect OC-IP processing:

- *Acknowledgement timeouts in the remote*. In setting up an OC-IP call at an operator position, several call control messages are exchanged (as shown in the call flow on page 105). Most of the messages used during setup have acknowledgement timers that are started after the message is sent. If an acknowledgement timer expires, the call is typically deflected. (For CSE acknowledgement timeouts, the CSE is typically released and the call remains active at the main operator.) When a timeout occurs, a TOPS133 log is generated and a Release Call message is sent to the host. The host will take down its end of the call and generate a TOPS102 log.
- *Acknowledgement timeouts in the host.* If the host times out while waiting for acknowledgement of a setup message, the host takes down its end of the call, since it assumes that connectivity has been lost with the remote. The host then sends a Release Call message back to the remote (if possible), which will also end the call in the remote.
- *Voice link signaling errors.* If a voice link signaling error is detected during setup (such as receiving an ISUP REL before receiving the ISUP ANM), the voice link is released and the call is rerouted. However, if a voice link signaling error is detected after setup (ISUP REL after ISUP ANM), the call is taken down.
- *Unexpected messages.* Unexpected messages will take a call down.

# Chapter 4: TOPS IP position application

The TOPS-IP product implements operator position connectivity over an integrated IP infrastructure. This chapter describes the IP position application, focusing on the following areas:

- background on traditional position connectivity and call flows
- introduction to IP position data and voice communication
- overview of datafill for IP position data links
- overview of datafill for IP position voice links
- overview of datafill for reporting IP position trouble
- successful IP position call flows
- IP position call processing interactions and failure handling

***Note:*** The IP position application interacts with the OC-IP application in networks that use both. Some of the interactions are discussed in this chapter, and some in Chapter 3: "TOPS OC-IP application."

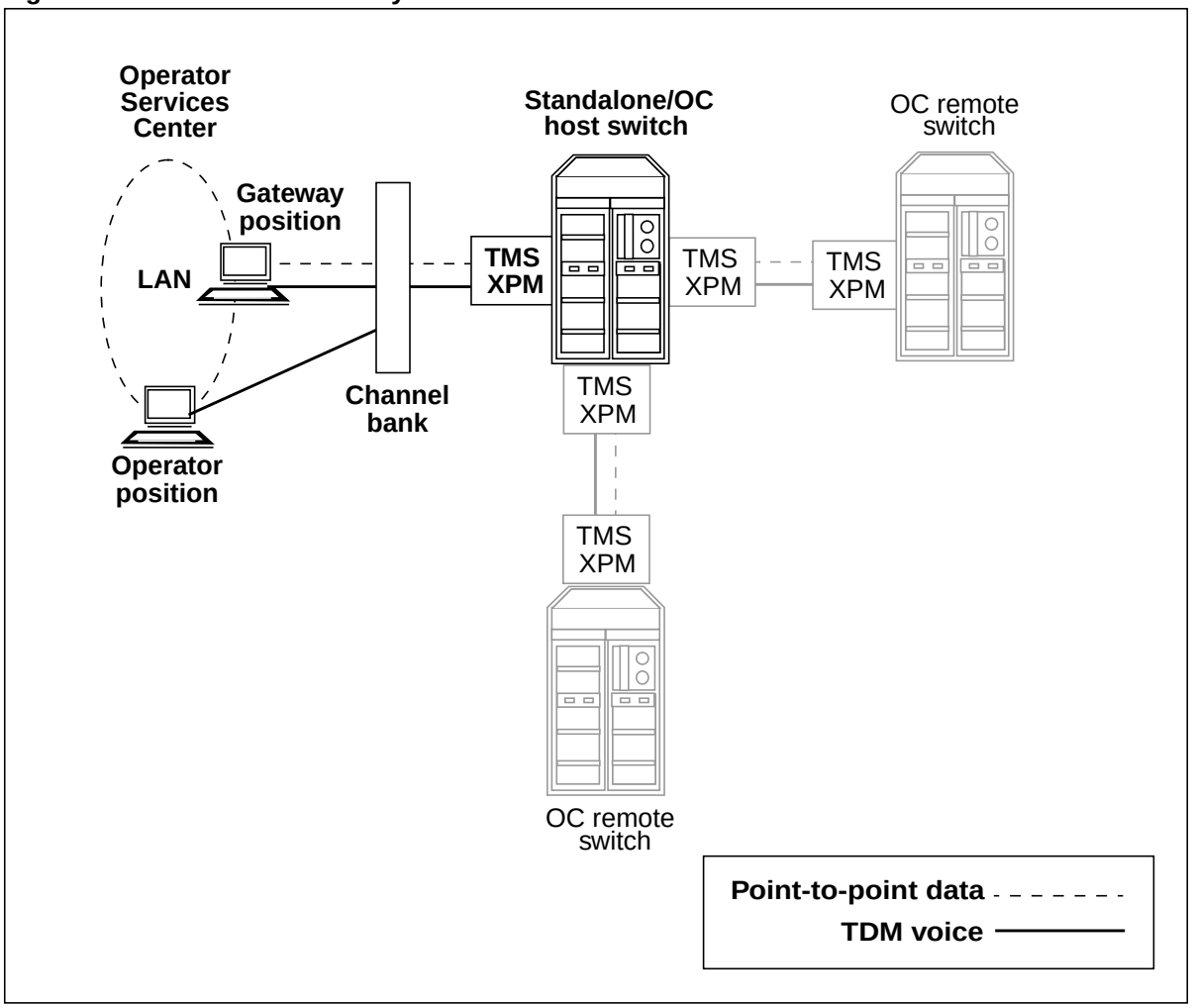
## Operator position background

In a TOPS network, teams of TOPS operators service a variety of calls from the public switched telephone network (PSTN). Operator positions located at Operator Services Centers (OSC) communicate voice and data with TOPS switches. The switches are responsible for call control, call and agent queue management, force management, and operator position maintenance.

### Traditional position connectivity

Figure 66 shows an example of a traditional, simple TDM-based network of operator positions and TOPS switches. In the figure, the "Standalone/OC host switch" could be a pure standalone TOPS switch in a non-Operator Centralization (OC) environment, or it could be a pure OC host switch, or a combination.

**Figure 66 Position connectivity without TOPS-IP**



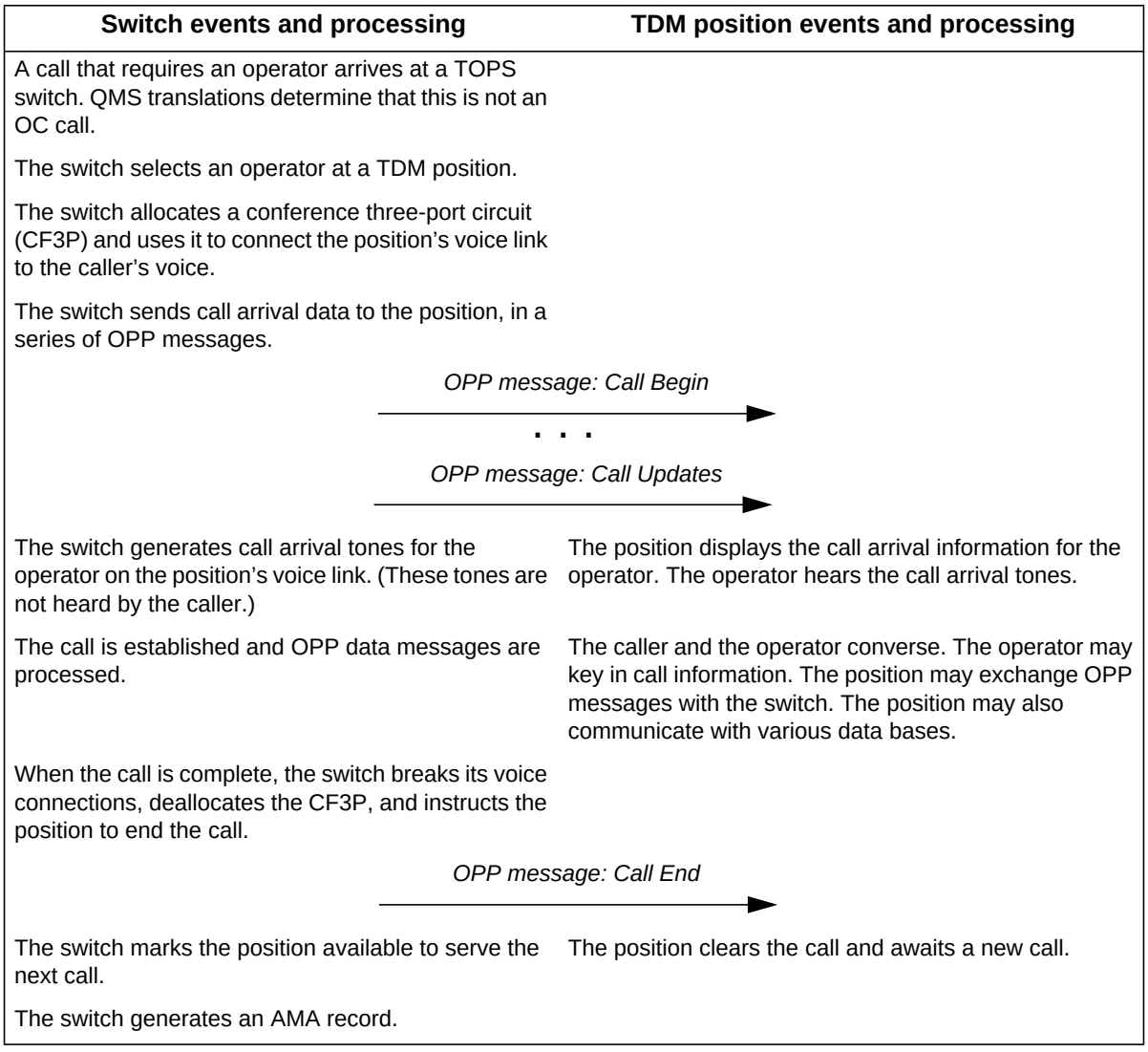

In a traditional network, voice and data connectivity are provisioned point to point between the standalone/OC host switch and each position. The dedicated TDM voice path to the position is through a TOPS Message Switch (TMS) XPM peripheral and a channel bank. The data path is also through a TMS and a channel bank, but it must pass through a gateway position, which transmits data to and from the other positions on the LAN. The gateway position is also responsible for maintenance of the positions in its cluster.

Although not shown in the figure, the three TOPS switches are also connected to the PSTN in the traditional way.

## Traditional standalone call flow

Figure 67 shows an example standalone TOPS call flow that uses a traditional TDM position. The example illustrates the use of position voice and data links. The arrows represent Open Position Protocol (OPP) data messages that are sent and received on the position data link. Use of the position voice link is described in the text.

**Figure 67 Example of traditional standalone call flow**




***Note:*** An example call flow for a traditional OC call begins on page 73. Example call flows using IP positions begin on page 139.

## IP position introduction

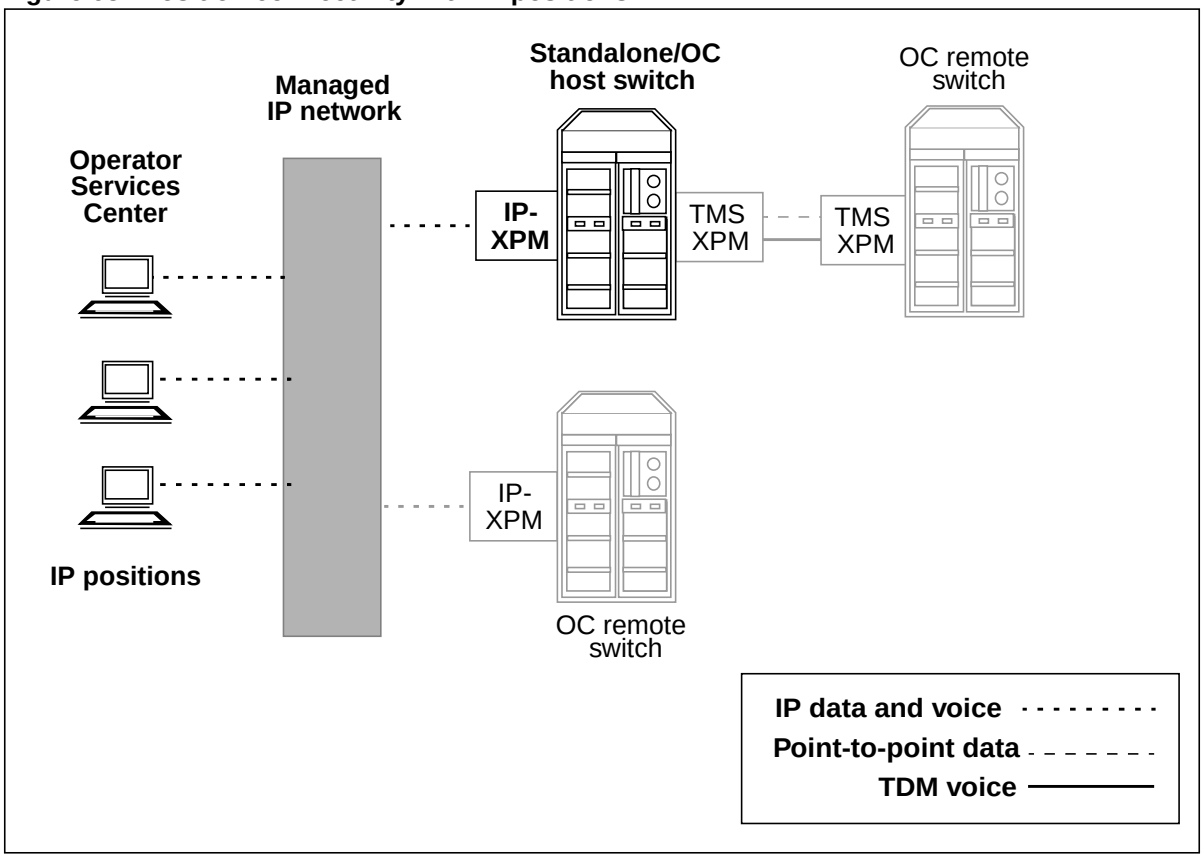
With the IP position application, the common IP infrastructure replaces the point-to-point provisioning of data and voice links between a TOPS switch and operator positions. Through the IP-XPM, a TOPS switch uses the managed IP network for data and voice communication with operator positions. No TMS peripheral is used for position connectivity, and there is no channel bank, nor gateway position with maintenance and data messaging responsibility for other positions.

In this document, positions that communicate with TOPS-IP switches over the managed IP network are referred to as *IP positions*. The use of IP data and voice communication technology is transparent to operators.

IP positions can be used for standalone TOPS calls, OC calls that use traditional TDM-based OC, and OC-IP calls. Figure 68 shows an example of a simple configuration of IP positions and TOPS switches. The IP positions at the OSC are still part of an Ethernet (not token ring) LAN, but the LAN is considered part of the managed IP network.

***Note:*** TDM OC links must be replaced by OC-IP links.

**Figure 68 Position connectivity with IP positions**



In the figure, the “Standalone/OC host switch” could be a pure standalone TOPS switch in a non-OC environment, or it could be a pure OC host switch, or it could be a combination standalone/host. As an OC host switch, it could provide IP positions for both of the OC remotes shown in the figure. One of these remotes uses the common IP infrastructure for its OC connectivity, and the other uses traditional TDM OC. Regardless of whether an OC remote uses OC-IP, it must be at TOPS15 or higher to successfully process a call for which the host selects an IP position.

***Note:*** TDM OC links must be replaced with OC-IP links.

## IP position data communication

This section discusses concepts and terms related to IP position data communication.

***Note:*** Most of this information is specific to the IP position application. For more basic information about the TOPS-IP infrastructure for data communication, refer to Chapter 2: “TOPS-IP data and voice communication.”

### IP-XPM data interface

The SX05DA processor card in the IP-XPM provides the switch interface for IP position data communication between a TOPS standalone or OC host switch and an IP position.

### IP position data links

An IP position data link is a logical data connection between an IP position and a TOPS standalone or OC host switch. IP position data links are used for OPP (key function and screen update) messages and maintenance messages. In OC calls, OPP messages between the OC remote switch and position always pass through the OC host switch. (This is also true with traditional TDM positions.) At the transport layer, IP position data links use the UDP protocol.

TOPS switch datafill for IP position data links specifies local connectivity information, including which IP-XPM provides the position’s data interface and which software port number on the IP-XPM is to be used for messaging with that position. This information is specified by datafilling a COMID against the position number in table TOPSPOS. Recall that a COMID specifies a particular SX05DA-equipped DTC and, indirectly through table IPSVCS, a port. A single COMID may be datafilled against many IP positions.

TOPS datafill does *not* include the position's IP address or port. The TOPS switch does not know how to address a message to an IP position until after the position has sent the first message to the switch, requesting to come in-service and providing the necessary addressing information. A position's IP address can be changed without a change in DMS datafill. Also, a position can be datafilled at more than one TOPS switch. The position can then request to come in-service at any switch on which it is datafilled. (Of course the request will be denied if the position is OFFL or MANB at that switch.)

A position can only be in-service at one switch at a time. This is enforced by the position. TOPS standalone and OC host switches do not communicate with each other about which positions are in-service at which switches.

***Note:*** It is not recommended that positions frequently come into and go out of service at different switches. This capability is intended primarily for disaster recovery in case of problems with the usual OC host. Refer to "Recovery issues for positions that initiate state changes" on page 347 for more information.

### Encryption

A simple encryption algorithm is used on IP position data links to protect sensitive data such as PINs, credit card numbers, and operator passwords. The encryption algorithm is intended to protect data against casual observers of the IP network traffic. It may not be sophisticated enough to withstand serious efforts to decrypt the messages.

### Related position datafill

For any DMS switch at which an IP position can come in-service, datafill in the position must specify the DMS IP address (active unit address of the IP-XPM) and port to which the position should send its in-service request message. The IWS position also has other datafill related to the IP position application. For more information on this datafill, refer to *TOPS IWS Base Platform User's Guide*.

## IP position voice communication

This section discusses concepts and terms related to IP position voice communication.

***Note:*** Most of this information is specific to the IP position application. For more basic information about the TOPS-IP infrastructure for voice communication, refer to Chapter 2: "TOPS-IP data and voice communication."

### IP-XPM voice interface

The 7X07AA Gateway card in the IP-XPM provides DMS voice communication with IP positions. The 7X07 converts between circuit-switched voice on the DMS network side and packet-switched voice on the IP network side.

### Dynamic voice trunks

IP position voice links use dynamic trunks in the DMS to send voice traffic over a data packet protocol. With dynamic trunking, there is no fixed connection to the far end. An IP position does not have a voice link allocated at any TOPS switch when it is not actively processing a call. A new IP voice connection is established between the switch and the position for each call.

### ISUP call processing

From the CM perspective, dynamic voice trunks appear as ISUP trunks that use the Q.764 protocol. However, ISUP is only used between the CM and the IP-XPM. The CM includes proprietary information, such as the IP address of a monitoring position, in the ISUP IAM message used to establish a VoIP connection. The SX05DA card in the IP-XPM routes ISUP messages to the 7X07 Gateway card, which converts between ISUP signaling on its C-side and a VoIP signaling protocol on the LAN side.

***Note:*** The SS7 network and associated datafill are *not used* for IP position voice links.

### Voice interactions with OC

When an OC host selects an IP position for an OC-IP call, the VoIP connection is directly between the position and the OC remote switch. The call does not use any voice resources in the OC host, either for signaling or for the media stream. This is referred to as a *host voice bypass* call.

### Voice signaling

The industry-standard SIP protocol is used between 7X07 Gateway cards and IP positions to control voice connections across the managed IP network.

### Voice encoding and auto-compression

Datafill in the CM can specify that VoIP connections with IP positions be made in any of three modes:

- Always use G.711.
- Always use G.723.
- Use auto-compression (patent pending). The following paragraphs describe the motivation for and operation of auto-compression.

Auto-compression is a solution that can help protect against degraded IP position performance under network fault conditions, without having to double the bandwidth engineered for traffic to IP positions.

TDM positions have nailed-up voice facilities between the position and its host switch (DS0 hard-wired to the position, connected via channel bank to a dedicated DS0 in a T1, T3, etc.). If a transport facility such as a T1 fails, the specific positions that use the facility go out of service until the facility is restored. No other positions are affected.

Since all the IP positions at an OSC share the available bandwidth (and facilities), all positions are potentially affected by a facility failure. If a failure causes the available network bandwidth to drop below the level required for all IP position voice and data packets, the network will begin to drop packets. Lost packets can result in symptoms ranging from voice drop-out to lost calls to "hung" positions. (The actual impact will depend on whether the various packet types have been properly prioritized in the network.) The important point is that all IP positions at the OSC are potentially affected.

One solution is to provide fully redundant facilities and diverse routing, with double the bandwidth that is needed when no fault is present. If G.711 is used, however, this solution significantly increases transport costs to the OSC. It could require up to four times the facilities needed for TDM positions.

A second solution is to use G.723 all the time. Since calls with G.723 need only about 1/3 the bandwidth of calls with G.711, this significantly decreases the cost of providing full redundancy. If the service provider is satisfied with the voice quality of G.723, this is a suitable alternative for minimizing transport costs.

Auto-compression is a third alternative, appropriate for service providers who prefer G.711 but need to economize on facilities to the OSC. When auto-compression is datafilled in the switch that initiates the VoIP connection to an IP position, the 7X07 Gateway at the switch offers to use either G.711 or G.723, leaving the selection up to the position. IP positions typically select G.711 as long as voice quality (latency, jitter, packet loss) is acceptable. When facilities are lost or data network equipment fails, and the available bandwidth is less than that required for IP positions, network performance degrades (that is, packet loss and jitter increase). IP positions detect the network quality degradation and will select G.723 on the next call.

Once a sufficient number of positions have switched to G.723, the network bandwidth will once again meet the bandwidth requirements, and network quality will rise. Some calls may be dropped and/or positions dropped from service during the brief period while auto-compression is activated.

IP positions automatically switch back from G.723 to G.711 in approximately four hours. (Field data indicates that most T1 outages are resolved within four hours.) If the facilities have not been recovered when positions begin to switch back, auto-compression will be re-activated. It is also possible to manually change an IP position back to G.711, if facilities are restored before four hours. See *TOPS IWS Base Platform User's Guide* for more information.

If auto-compression is datafilled at all DMS switches that use IP positions at an OSC (OC-IP remotes as well as the host switch), only the amount of bandwidth required for all IP positions to use G.711 need be provisioned.

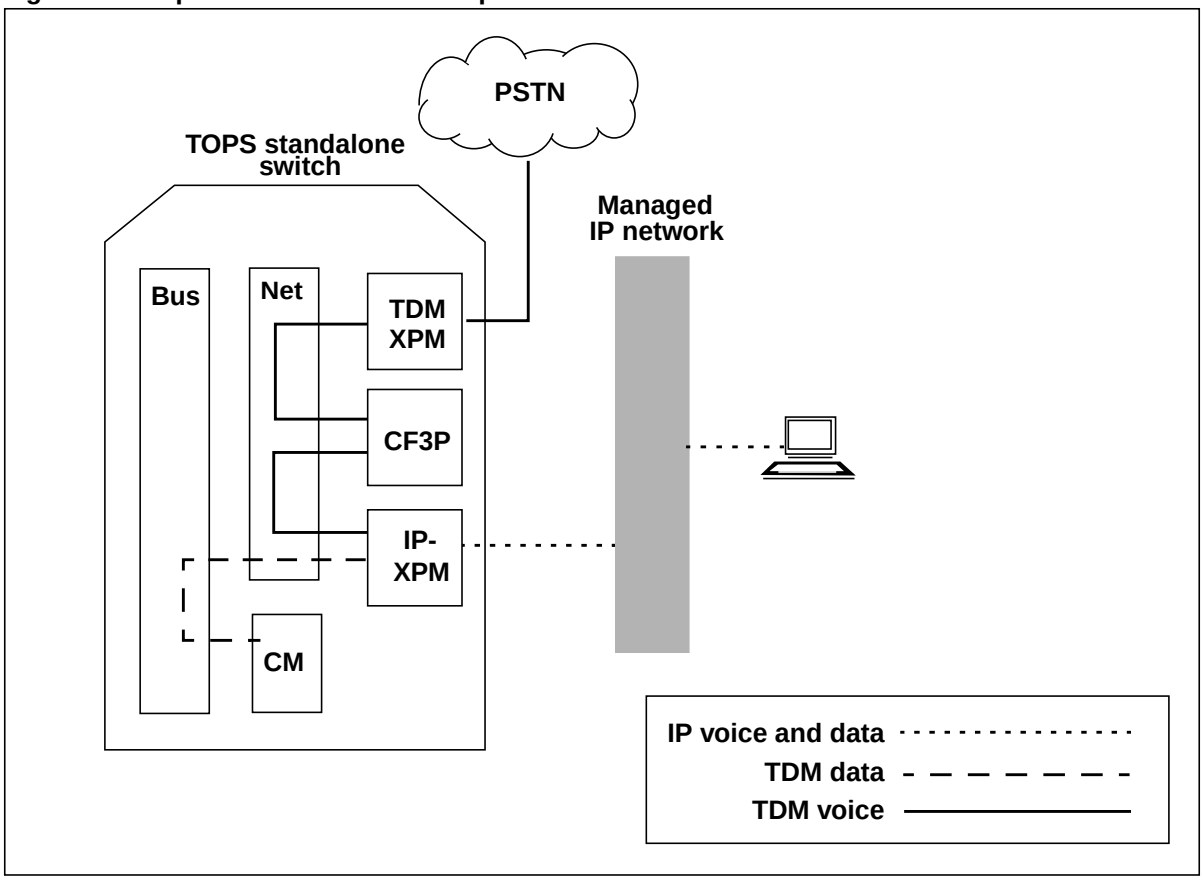
***Note:*** Auto-compression is datafilled in switch tables PKTVPROF and TQCQINFO, described later in this section.

## Voice and data paths for IP positions

This section illustrates and describes the voice and data paths for IP position standalone calls, IP position calls that use traditional TDM OC, and IP position calls that use OC-IP.

Figure 69 illustrates the paths for voice and data for a TOPS standalone call. A description follows the figure.

**Figure 69 IP position voice and data paths - standalone call**




The subscriber voice path originates at the standalone TOPS switch from a TDM trunk in the public switched telephone network (PSTN), and is connected to a conference circuit (CF3P) through the DMS network. The position voice link connects to the same CF3P and terminates to the C-side of a 7X07 Gateway card in the IP-XPM. The Gateway converts between TDM voice and packetized voice, and presents the voice stream to the managed IP network for the position.

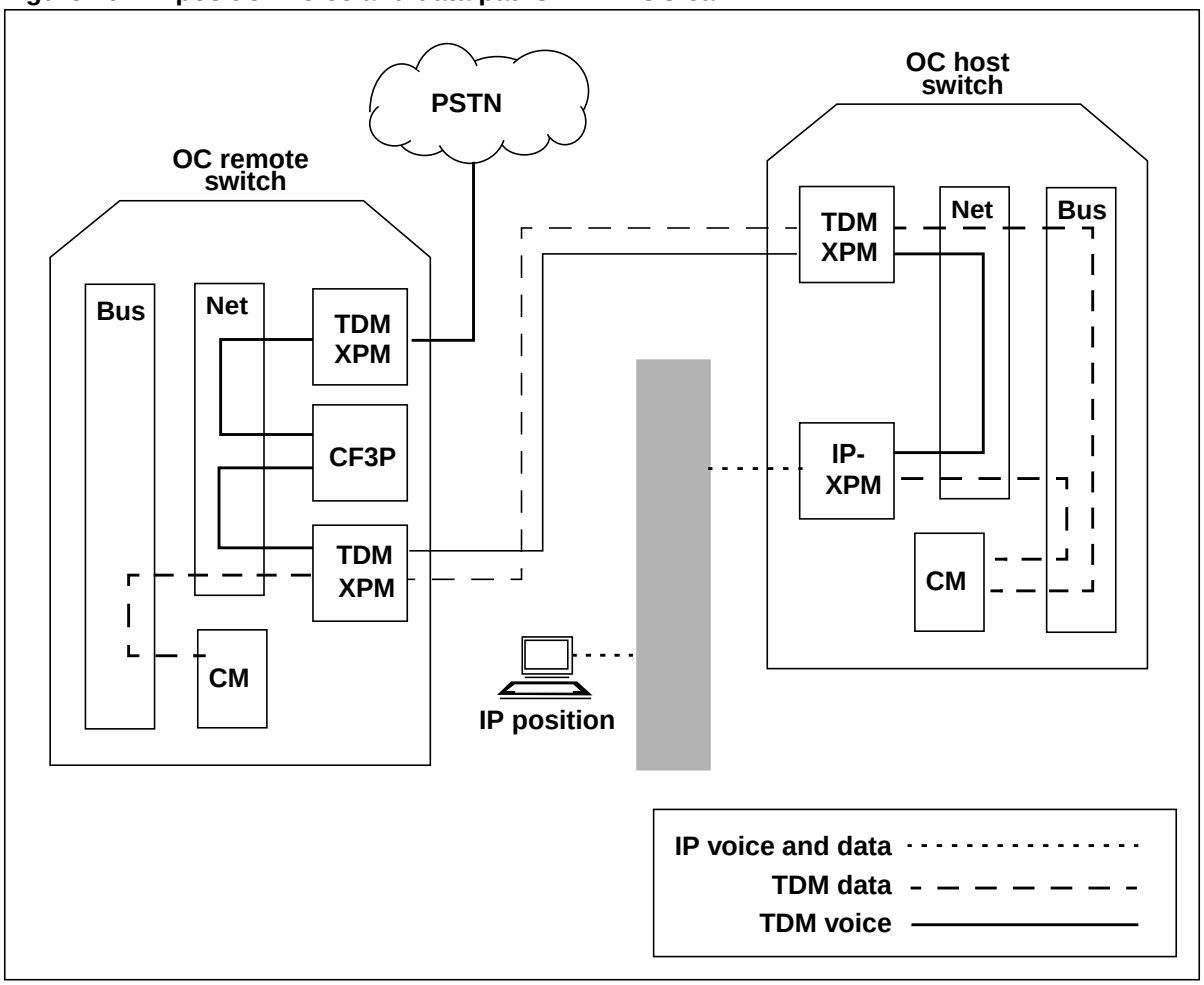
The CM in the switch can originate data messages for the position. These messages travel via the switch's DMS Bus (message switch) and network to an SX05DA card in the IP-XPM. The SX05DA packetizes the data and presents it to the managed IP network for the position.

Figure 70 illustrates the paths for voice and data for an IP position call that uses traditional TDM OC.

***Note:*** TDM OC links must be replaced by OC-IP links.

A description follows the figure.

**Figure 70 IP position voice and data paths - TDM OC call**

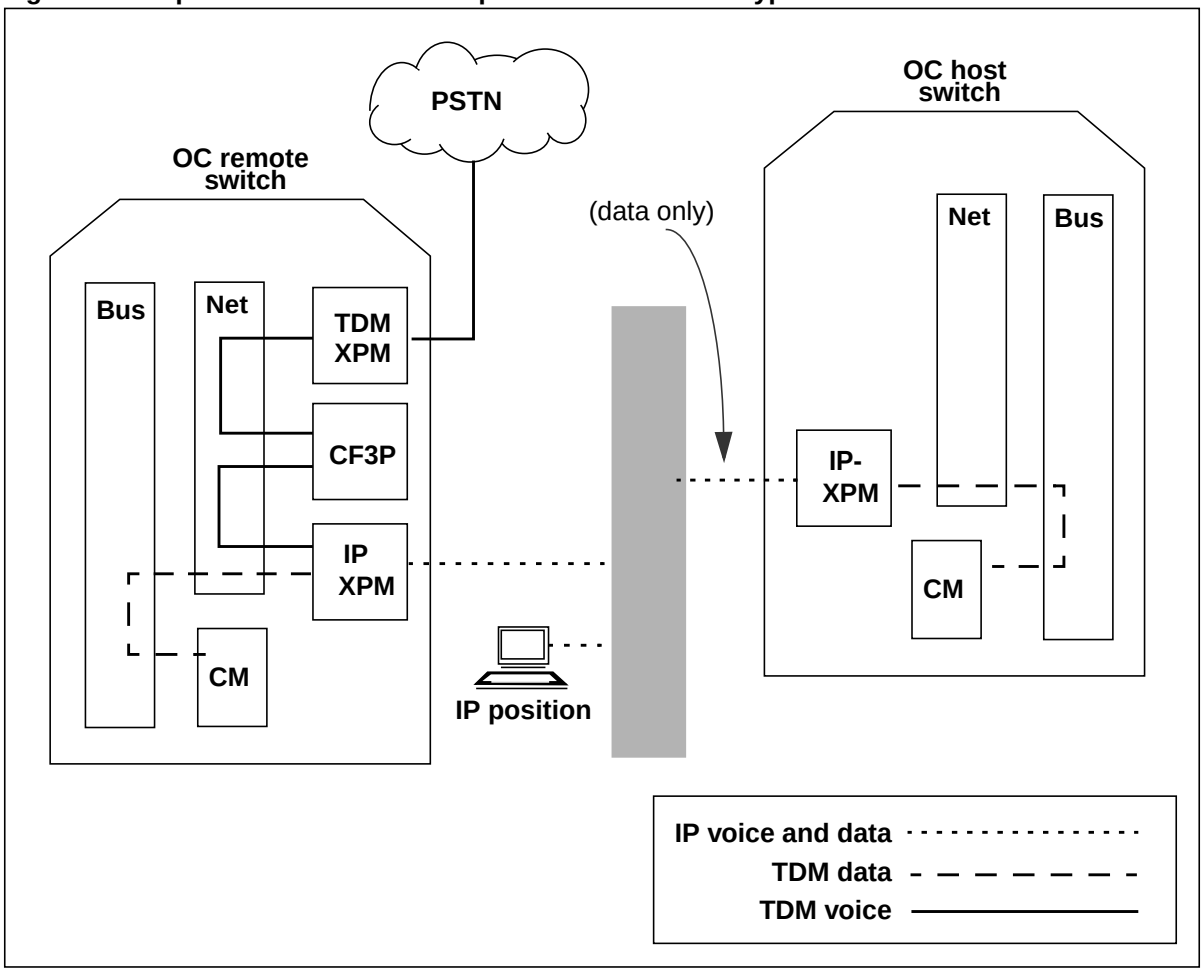



The subscriber voice path originates at the OC remote switch from a TDM trunk in the PSTN, and is connected to a CF3P through the DMS network. The OC-IP voice link connects to the same CF3P and to a TDM peripheral. A dedicated voice trunk connects this TDM peripheral to a similar one at the OC host. There the TDM voice terminates to the C-side of a 7X07 Gateway card in the host's IP-XPM. The Gateway converts TDM voice to packetized voice and presents the voice stream to the managed IP network for the position.

The data path from the remote CM to the position goes first to a TDM peripheral via the DMS Bus (message switch) and DMS network. From there the data travels via X.25 to a TDM peripheral at the host, and to the host CM via the DMS network and message switch. The host CM sends the data to the SX05DA card in the IP-XPM via the message switch and DMS network. The SX05DA packetizes the data and presents it to the managed IP network for the position.

Figure 71 illustrates the paths for voice and data in the unified topology, for a call that uses both OC-IP and an IP position. A description follows the figure.

**Figure 71 IP position voice and data paths for host voice bypass call**




The subscriber voice path originates at the OC remote switch from a TDM trunk in the PSTN, and is connected through the DMS network using a CF3P circuit to the remote's IP-XPM. It terminates at the C-side of a 7X07 Gateway card in the IP-XPM. The Gateway converts between TDM voice and packetized voice, and presents the voice stream to the managed IP network for the IP position.

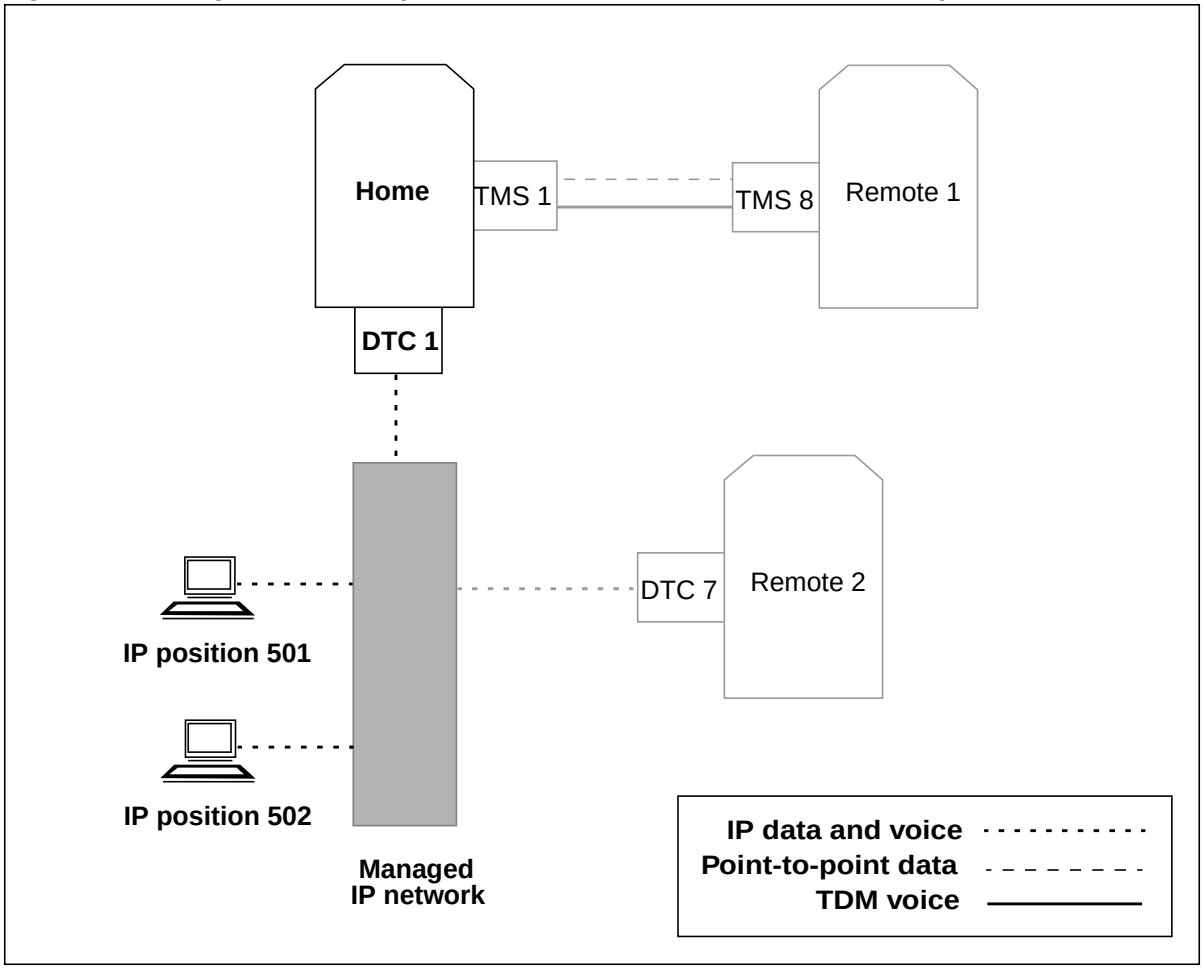
The data path from the remote CM to the position goes via the DMS Bus (message switch) and DMS network to the SX05DA card in the remote's IP-XPM. The SX05DA packetizes the data and presents it to the managed IP network for the SX05DA in the host's IP-XPM. The host's SX05DA sends the data to the host's CM via the DMS network and DMS bus, and the CM sends data for the position back over the same path. The SX05DA again packetizes the data and presents it to the managed IP network for the position.

## Overview of datafill for IP position data links

This section introduces the switch datafill required for IP positions data links. Figure 72 shows a simple network which is used in the datafill examples. All datafill examples are for the switch labeled "Home" in the figure.

***Note:*** This is not the same Home switch that was used in the examples in Chapter 3: "TOPS OC-IP application."

**Figure 72 Configuration for IP position data communication datafill examples**



Home functions as a standalone/OC host switch, and it hosts IP positions 501 and 502. These positions serve standalone calls that are routed directly to Home from end offices or tandems. They also serve OC calls from Remote 1, which has traditional TDM OC connectivity with Home, and from Remote 2, which has OC-IP connectivity with Home. (Both DTCs in the figure are IP-XPMs.)

***Note:*** TDM OC links must be replaced by OC-IP links.

This section discusses the data-related tables that are specific to IP positions and the data-related tables that are part of the base IP infrastructure. For the infrastructure tables, it includes IP position application-specific considerations. Each table description includes an example of the datafill that supports IP position data links at the Home switch. The tables are described in the following order:

- LTCINV (Line Trunk Controller Inventory)
- XPMIPGWY (XPM IP Gateway)
- XPMIPMAP (XPM IP Mapping)
- IPSVCS (IP Services)
- IPCOMID (IP Communication Identifier)
- TOPSPOS (TOPS Position)
- TOPSPARM (TOPS Parameter)

***Note 1:*** The discussion and examples in this section pertain only to Home's IP position data links. They do not include Home's OC datafill. Datafill for IP position data links is not affected by whether the position is used for standalone or OC host calls. Refer to Chapter 3: "TOPS OC-IP application" for information about OC-IP datafill.

***Note 2:*** Refer to Chapter 8: "TOPS-IP data schema" for details on the range of valid datafill for every table affected by TOPS-IP.

## LTCINV

Table LTCINV specifies hardware inventory information for each IP-XPM (excluding the P-side link assignments). TOPS-IP infrastructure considerations for table LTCINV are discussed beginning on page 52. IP position data links introduce no application-specific considerations.

In the following example, the Home switch datafills DTC 1 with the most recent QTP and firmware load names and the circuits that are needed for TOPS-IP data links.

**Figure 73 MAP display example for table LTCINV**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD     EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC              EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
--------------------------------------------------------------------------------
DTC 1    1001   LTE    0    51    0     C   0    6X02AF  QTP22xx (ABTRK DTCEX)$
(0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5)
(0 11 0 6) (0 11 0 7) (0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11)
(0 11 0 12) (0 11 0 13) (0 11 0 14) (0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     0         SXFWAJ02    $
       6X40FC    N
```

## XPMIPGWY

Table XPMIPGWY specifies gateway router information for SX05DA cards. A gateway router is a component of the managed IP network and is used to forward IP packets to other networks. TOPS-IP infrastructure considerations for table XPMIPGWY are discussed beginning on page 55. IP position data links introduce no application-specific considerations.

In the following example, the Home switch leaves table XPMIPGWY empty, since Home uses the DHCP (network) method for configuring its IP-XPM.

**Figure 74 MAP display example for table XPMIPGWY**

```
GWINDEX   DESTADDR       RTEMASK            GWIPADDR       METRIC
--------------------------------------------------------------------
```

## XPMIPMAP

Table XPMIPMAP specifies various IP information for the SX05DA, including the configuration method used when the IP-XPM is brought into service. TOPS-IP infrastructure considerations for table XPMIPMAP are discussed beginning on page 57. IP position data links introduce no application-specific considerations.

In the following example, the Home switch datafills the DHCP method for DTC 1, along with the Ethernet speed specification and subnet mask.

**Figure 75 MAP display example for table XPMIPMAP**

```
XPMNAME  AUTONEG  SUBNMASK       IPCONFIG  ACTADDR       INADDR
      UNIT0         UNIT1              GWINDEX         DNSINFO
-----------------------------------------------------------------
DTC 1    AUTO     255 255 255 0  DHCP
```

***Note 1:*** When the DHCP method is datafilled, the IP-XPM is configured by the DHCP network server, so router datafill in table XPMIPGWY is never used.

***Note 2:*** When the CM method is datafilled, the GWINDEX refinement specifies a list of indexes into table XPMIPGWY. After changing the datafill for GWINDEX, users should update the static data for the SX05DA. For details, refer to "Updating static data" on page 299.

### IPSVCS

Table IPSVCS defines IP transport services for the SX05DA. Each service name represents a software port and transport protocol. The service name is referenced by table IPCOMID. TOPS-IP infrastructure considerations for table IPSVCS are discussed beginning on page 59.

The IP position application requires that the protocol be datafilled as UDP. Also, the application does not allow the port to be changed unless all positions that use the IP service are off-line.

If the operating company decides to datafill only a single COMID for all the positions that use the same IP-XPM, then one IPSVCS tuple is sufficient for the entire IP position application. Otherwise a separate IPSVCS tuple must be datafilled for each COMID that shares an IP-XPM.

In the following example, the Home switch defines one IP transport service, POSIPSVC, for IP position data links.

**Figure 76 MAP display example for table IPSVCS**

```
SERVICE             PORT       PROTOCOL
-------------------------------------------------------------------
POSIPSVC            8700       UDP
```

***Note 1:*** The managed IP network can be configured to use port assignments for different applications to manage quality of service, including minimizing loss of IP position data link messages. Refer to Chapter 7: "TOPS-IP engineering guidelines," for the recommended port range and other related information.

***Note 2:*** An IWS position must know what port number is datafilled for it in the switch, and it must know the active IP address of the IP-XPM that is datafilled for it in the switch. The DMS IP address and port are datafilled in the IWS. The IWS needs this information so it can send an in-service request message to the switch.

### IPCOMID

Table IPCOMID defines COMIDs. A COMID represents *local* connectivity information for each data link. TOPS-IP infrastructure considerations for table IPCOMID are discussed beginning on page 60.

COMIDs are associated with IP position data links in table TOPSPOS (page 126). Many IP positions can share the same COMID. Positions with the same COMID use the same UDP socket on the same IP-XPM.

In the following example, the Home switch defines a COMID for IP data communication with the IP positions it hosts.

**Figure 77 MAP display example for table IPCOMID**

```
COMID    SERVICE            XPMNAME
-------------------------------------------------------
19       POSIPSVC           DTC 1
```

***Note 1:*** A COMID only specifies information about the switch end of the position data link. The TOPS switch does not know the position's IP address or port until the position sends an in-service request message.

***Note 2:*** Parallel datafill is required in the IWS position for (a) the active unit IP address of the IP-XPM associated with the COMID datafilled in the switch for that position, and (b) the port datafilled in the IPSVCS tuple referenced by that COMID. Appendix D: "IWS IP datafill quick reference" is a quick but incomplete reference to the required IWS datafill. Refer to *TOPS IWS Base Platform User's Guide* for more information.

## TOPSPOS

Table TOPSPOS contains provisioning datafill for operator positions supported by the TOPS switch. This table is used only in TOPS standalone and OC host switches. Each tuple defines the voice and data link information for a single position. Table TOPSPOS allows each position's voice and data paths to be provisioned as either TDM or IP.

***Note:*** IP data connectivity can be used only when IP voice connectivity is used, and vice versa.

The DATAPATH field consolidates the data refinements, and the VLPATH field consolidates the voice refinements (described on page 136). The POSAREA field contains no information specific to IP positions.

In the following example, the Home switch datafills two IP positions, both of which use COMID 19 for data connectivity at DTC 1. A description of the DATAPATH refinements for IP positions follows the example.

**Figure 78 MAP display example for table TOPSPOS**

```
POSNO    VLPATH            DATAPATH      POSAREA
-------------------------------------------------------------------
501      PKTV POSIPVL      IP 19 N       OPR 6 20
502      PKTV POSIPVL      IP 19 N       OPR 6 20
```

For IP position data communication, the DATAPATH field consists of the following three subfields and refinements:

- DATATYPE defines IP as the type of data connectivity with the standalone/OC host switch.

- IPCOMID defines the COMID used for data communication. It references a COMID from table IPCOMID. The IP service referenced by the IPCOMID tuple must use the UDP protocol.

  For each IP-XPM that is used for IP positions, up to eight different COMIDs may be datafilled in table TOPSPOS. Each COMID corresponds to a different UDP socket in the XPM. For any particular IP-XPM, there is no capacity advantage in using more than one COMID for IP positions. However, there may be administrative reasons for doing so, since positions can be posted and maintained by COMID at the MAP.

- URESOK ('N' in the example) defines the disposition of the position when it is in the unconnected restricted idle (URES) maintenance state. The URES state indicates that the switch has a socket open and ready for the position, and is waiting for the position to send an in-service request message.

  It is expected that most IP positions will be datafilled with URESOK=N. When the URESOK field is set to N, the position transitions to the SYSB state if the switch does not receive an in-service message from the position within a fixed time interval. When URESOK is set to Y, the switch allows the position to remain in the URES state indefinitely until a maintenance action (such as an in-service request from the position, or manual action at the MAP) forces a transition.

  ***Note:*** For more information about the URES state, refer to Chapter 10: "TOPS-IP maintenance activities."

### TOPSPARM

Table TOPSPARM contains TOPS-specific office parameters. Two parameters, IPPOS_AUDIT_INTERVAL and IPPOS_AUDIT_THRESHOLD, were created for the IP position application. However, neither of these parameters is used. They may be left at their default values.

In the following example, the Home switch leaves the two unused IP position parameters at their default values.

**Figure 79 MAP display example for table TOPSPARM**

```
PARMNAME                PARMVAL
-------------------------------------------------------------
IPPOS_AUDIT_INTERVAL    5
IPPOS_AUDIT_THRESHOLD   3
```

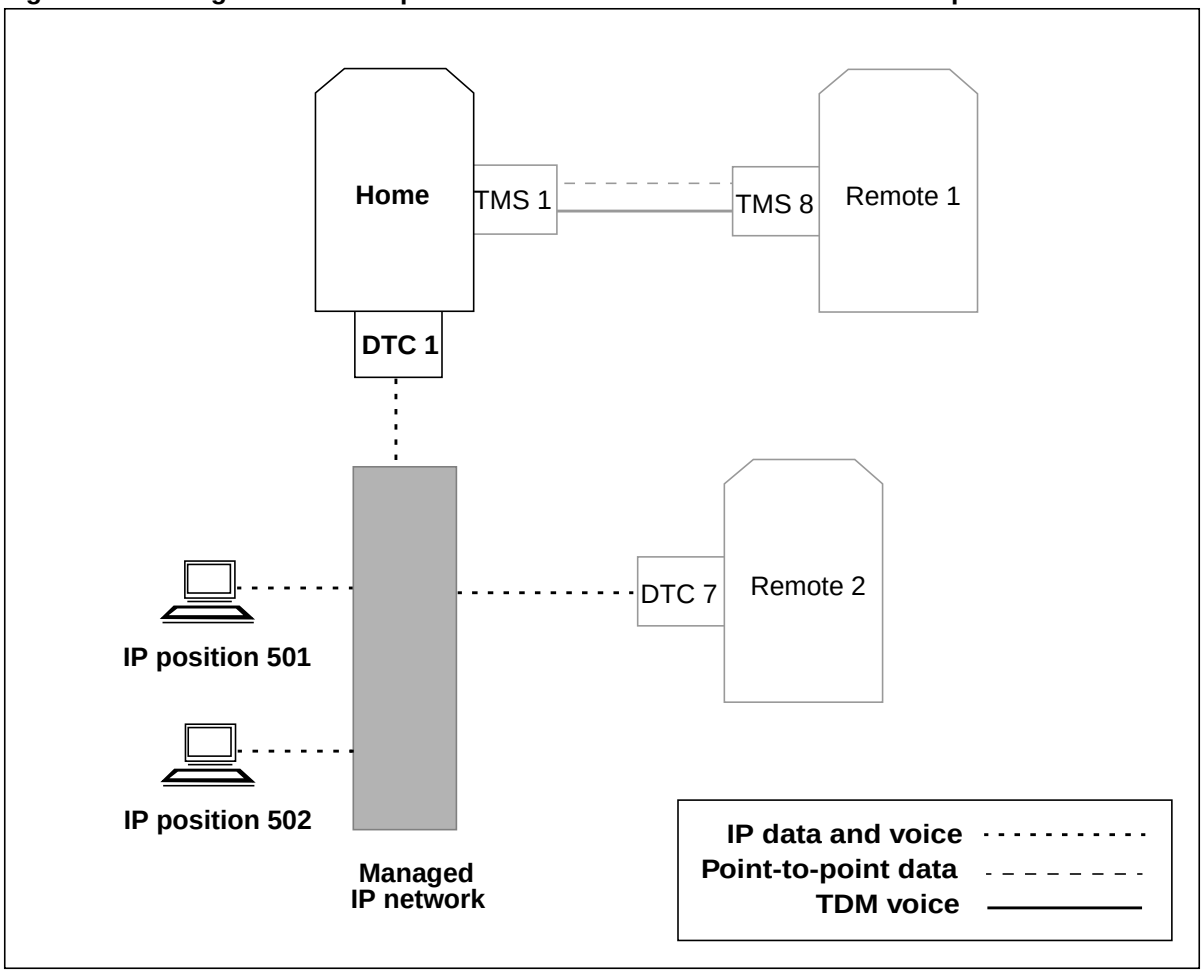
## Overview of datafill for IP position voice links

This section introduces the datafill required for IP position voice links. The discussion in this section uses the same example "Home" switch that was introduced on page 122. For convenience, Home's network configuration is shown again in Figure 80. Home supports three IP position configurations or call flows:

- IP position handling standalone TOPS call
- IP position handling OC-IP call (OC host voice bypass)
- IP position handling traditional TDM-based OC call

***Note:*** TDM OC links must be replaced by OC-IP links.

**Figure 80 Configuration for IP position voice communication datafill examples**




This section discusses the voice-related tables that are specific to IP positions and the voice-related tables that are part of the base IP infrastructure. For the infrastructure tables, it includes application-specific considerations for IP positions. Each table description includes an example of the datafill for IP position voice links at the Home switch. The tables are described in the following order:

- LTCINV (Line Trunk Controller Inventory)
- CARRMTC (Carrier Maintenance)
- LTCPSINV (LTC P-side Inventory)
- CLLI (Common Language Location Identifier)
- TRKGRP (Trunk Group)
- TRKSGRP (Trunk Subgroup)
- TRKOPTS (Trunk Options)
- SITE (Site)
- IPINV (IP Inventory)
- TRKMEM (Trunk Members)
- TOPSTOPT (TOPS Trunk Options)
- OFCENG (Office Engineering)
- PKTVPROF (Packetized Voice Profile)
- TQCQINFO (TOPS QMS Call Queue Information)
- TOPSPOS (TOPS Position)

***Note 1:*** The discussion and examples in this section pertain only to Home's IP position voice links. They do not include datafill for Home's OC voice links. Datafill for IP position voice links is essentially the same regardless of whether the positions are expected to serve standalone calls or OC-IP calls. This section notes where there are differences.

One difference not fully discussed in this section, however, is the effect of host voice bypass on engineering rules for 7X07 Gateway cards. Refer to Chapter 7: "TOPS-IP engineering guidelines" for more information.

***Note 2:*** Refer to Chapter 8: "TOPS-IP data schema" for details on the range of valid datafill for every table affected by TOPS-IP.

### LTCINV

Table LTCINV contains the inventory datafill (excluding the P-side link assignments) for IP-XPMs. TOPS-IP infrastructure considerations for table LTCINV are discussed beginning on page 52. IP position voice links introduce no application-specific considerations

In the following example, the Home switch datafills DTC 1 with the North American toneset, which is required to satisfy table control and diagnostics, and with the other information that is required for IP position voice links.

**Figure 81 MAP display example for table LTCINV**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
-------------------------------------------------------------------------
DTC 1    1001   LTE    0    51    0     C   0    6X02AF  QTP22xx (ABTRK DTCEX)$
   (0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5) (0 11 0 6)
(0 11 0 7) (0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11) (0 11 0 12) (0 11 0 13)
(0 11 0 14) (0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02    (CCS7) $
       6X40FC    N
```

### CARRMTC

Table CARRMTC specifies maintenance control information for the IP-XPM. TOPS-IP infrastructure considerations for table CARRMTC are discussed beginning on page 53. IP position voice links introduce no application-specific considerations.

In the following example, the Home switch datafills carrier maintenance information for the type of IP-XPM (DTC) used for IP position voice.

**Figure 82 MAP display example for table CARRMTC**

```
CSPMTYPE TMPLTNM  RTSML  RTSOL  ATTR
-------------------------------------------------------------------------------
DTC      TGWY     255    255    DS1 NT7X07AA  MU_LAW SF ZCS BPV NILDL N 250 1000
50 50 150 1000 3 6 864 100 17 511 4 255
```

### LTCPSINV

Table LTCPSINV contains the IP XPM's P-side link assignments for the 7X07 Gateway cards. TOPS-IP infrastructure considerations for table LTCPSINV are discussed beginning on page 54. IP position voice links introduce no application-specific considerations.

In the following example, the Home switch datafills P-side links 0 through 3 for DTC 1. Links 0 and 1 will support one 7X07 card, and links 2 and 3 will support a second 7X07 card. The even-numbered links will be datafilled as the port numbers in table IPINV (page 133).

**Figure 83 MAP display example for table LTCPSINV**

```
LTCNAME   PSLINKTAB
-------------------------------------------------------------------------------
DTC 1     N (0 DS1 TGWY N) (1 DS1 TGWY N) (2 DS1 TGWY N) (3 DS1 TGWY N)
(4 NILTYPE) (5 NILTYPE) (6 NILTYPE) (7 NILTYPE) (8 NILTYPE) (9 NILTYPE)
(10 NILTYPE) (11 NILTYPE) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE) (15 NILTYPE)
(16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $
```

***Note:*** Recall that in our example, the Home switch uses DTC 1 for OC-IP connectivity to switch Remote 2 as well as for connectivity to its IP positions. If this were a complete example of Home's datafill, additional P-side links assignments would be present for one or more 7X07 Gateways used for OC-IP voice connectivity with "Remote 2." The example shows only the assignments for the 7X07s that are used for the IP position application.

### CLLI

Table CLLI specifies the trunk group names and the maximum number of members in each trunk group. TOPS-IP infrastructure considerations for table CLLI are discussed beginning on page 61.

In the following example, the Home switch datafills the dynamic trunk group used for communication with the IP positions: POSIPVL. This CLLI and its associated trunk group are used when Home's IP positions handle standalone calls (including any call in which an operator keys to access an idle loop) and TDM-OC calls. When an IP position handles an OC-IP call, the IP voice connection bypasses the host and its 7X07 cards and associated trunk groups.

**Figure 84 MAP display example for table CLLI**

```
CLLI            ADNUM      TRKGRSIZ     ADMININF
-------------------------------------------------------------------
POSIPVL         484        2016         POSIP_VOICE_LINK
```

***Note:*** It is possible to datafill more than one dynamic POS trunk group for use with IP positions. However, this is not recommended because of its impact on sparing. As described in Chapter 7: "TOPS-IP engineering guidelines," N+1 redundancy of 7X07 Gateway cards is needed for each trunk group.

### TRKGRP

Table TRKGRP specifies the trunk group type, direction, and other information for each trunk group. TOPS-IP infrastructure considerations for table TRKGRP are discussed beginning on page 61.

Dynamic trunk groups used for voice connections with IP positions must have direction outgoing (OG). Table TOPSPOS, where voice trunks are associated with positions, enforces this restriction.

In the following example, the Home switch datafills the OG direction for the dynamic trunk group that will be datafilled against its IP positions.

**Figure 85 MAP display example for table TRKGRP**

```
GRPKEY   GRPINFO
-----------------------------------------------------------------
POSIPVL  IT 0 NPDGP NCRT OG NIL MIDL 000 NPRT NSCR 619 619 000 N N $
```

### TRKSGRP

Table TRKSGRP defines additional trunk group information such as signaling. TOPS-IP infrastructure considerations for table TRKSGRP are discussed beginning on page 62. IP position voice links introduce no application-specific considerations.

In the following example, the Home switch datafills the dynamic trunk group that will be used for IP positions with ISUP signaling information.

**Figure 86 MAP display example for table TRKSGRP**

```
SGRPKEY    CARDCODE SGRPVAR  SGRPVAR
-------------------------------------------------------------------------
POSIPVL 0  DS1SIG   C7UP     OG N N UNEQ NONE Q764 THRL 0 NIL $ NIL
```

***Note:*** The SS7 network and associated datafill are *not used* for IP position voice links.

### TRKOPTS

Table TRKOPTS specifies additional trunk group options, including the dynamic option required by TOPS-IP voice trunks. TOPS-IP infrastructure considerations for table TRKOPTS are discussed beginning on page 62.

For dynamic voice trunks that are datafilled against IP positions in table TOPSPOS, the application field in table TRKOPTS must be set to POS.

In the following example, the Home switch datafills POSIPVL as dynamic POS.

**Figure 87 MAP display example for table TRKOPTS**

```
OPTKEY                OPTINFO
-----------------------------------------------------------
POSIPVL DYNAMIC       DYNAMIC ISUP IP IP POS
```

***Note:*** A dynamic POS trunk group is used to connect to IP positions in a standalone or OC host switch. For OC-IP calls that are served by IP positions and thus use host voice bypass, the remote's trunk group is datafilled in table TRKOPTS as OC, not POS. Dynamic POS trunks are used only in the switch that is hosting an IP position.

### SITE

Table SITE identifies a site name associated with the 7X07 Gateway cards datafilled at the switch. TOPS-IP infrastructure considerations for table SITE are discussed beginning on page 63. IP position voice links introduce no application-specific considerations.

In the following example, the Home switch datafills the site name TGWY.

**Figure 88 MAP display example for table SITE**

```
NAME   LTDSN  MODCOUNT OPVRCLLI ALMDATA
-------------------------------------------------------
TGWY   0      0        VER90    $
```

***Note:*** As Gateways are added to and removed from table IPINV, the system automatically updates the MODCOUNT field to reflect the number of Gateways on the site.

### IPINV

Table IPINV defines the individual 7X07AA Gateway cards (nodes) at the switch. For Gateways used for TOPS-IP applications, IPINV datafill includes the name of a dynamic trunk group from which the switch *automatically* datafills a block of 48 members in table TRKMEM, when the tuple is added to table IPINV.

TOPS-IP infrastructure considerations for table IPINV are discussed beginning on page 63. IP position voice links introduce no application-specific considerations.

In the following example, the Home switch datafills two TGWY cards at DTC 1. Associated with the Gateway cards is the POSIPVL trunk group, which supports 96 members.

**Figure 89 MAP display example for table IPINV**

```
IPNO       PMTYPE PMNO IPPEC   LOAD  PORT  IPZONE                GWTYPE
-------------------------------------------------------------------------------
TGWY 01 0  DTC    1    7X07AA  $     0     47 174 68 15 0 0 0 0  TOPS POSIPVL 0
TGWY 01 1  DTC    1    7X07AA  $     2     47 174 68 29 0 0 0 0  TOPS POSIPVL 96
```

***Note 1:*** The DTC P-side links must first be assigned in table LTCPSINV (page 130). The PORT entry in table IPINV is the lower of the two P-side link numbers for that Gateway. For more detailed information on port mapping, see “LTCPSINV-to-IPINV port mapping” on page 249.

***Note 2:*** The example datafill shown in Figure 89 causes automatic datafill of POSIPVL members 0 to 47 and 96 to 147 in table TRKMEM:

***Note 3:*** Refer to table TOPSTOPT (page 134) for datafill that limits the number of trunks that may be used by call processing.

### TRKMEM

Table TRKMEM defines the individual trunk members associated with a trunk group. In the case of trunks defined as DYNAMIC POS in table TRKOPTS, no manual datafill in TRKMEM is allowed because tuples are automatically datafilled by table IPINV.

TOPS-IP infrastructure considerations for table TRKMEM are discussed beginning on page 66. IP position voice links introduce no application-specific considerations.

The following example shows part of the datafill that would be automatically added to table TRKMEM in the Home switch.

**Figure 90 MAP display example for table TRKMEM**

```
CLLI  EXTRKNM      SGRP  MEMVAR
-----------------------------------------------------
POSIPVL 0          0     DTC 1 0 1
POSIPVL 1          0     DTC 1 0 2
POSIPVL 2          0     DTC 1 0 3
 . . . . . .
POSIPVL 23         0     DTC 1 0 24
POSIPVL 24         0     DTC 1 1 1
POSIPVL 25         0     DTC 1 1 2
 . . . . . .
POSIPVL 47         0     DTC 1 1 24
POSIPVL 96         0     DTC 1 2 1
POSIPVL 97         0     DTC 1 2 2
 . . . . . .
POSIPVL 143        0     DTC 1 3 24
```

### TOPSTOPT

Table TOPSTOPT specifies options for TOPS trunk groups. For dynamic trunks, the MAXCONNS field controls the maximum number of trunks that may be used by call processing. TOPS-IP infrastructure considerations for table TOPSTOPT are discussed beginning on page 67. IP position voice links introduce no application-specific considerations.

In the following example the Home switch datafills MAXCONNS, limiting to 26 the number of trunks that can be used for call processing in dynamic POS trunk group POSIPVL.

**Figure 91 MAP display example for table TOPSTOPT**

```
GRPKEY    ORGAREA  DISPCLG  ADASERV  ADASANS  ANITOCLI  OLNSQRY
  DCIBIDX   LNPCLGAM  XLASCHEM  SPIDPRC  TRKSPID  BILLSCRN  ANIFSPL
MAXCONNS  DISPSPID
-------------------------------------------------------------
POSIPVL      N      N        NONE     NA       N          NONE
  0            N         N         N        N        N         N
26         N
```

### OFCENG

Table OFCENG contains office-wide parameters. TOPS-IP infrastructure considerations for table OFCENG are discussed beginning on page 68. In addition to the infrastructure considerations, parameters NUMCALLPROCESSES and NUMCPWAKE may need to be increased in offices with IP positions. OMs useful in determining whether these parameters need to be increased include:

- CP_CPSZ/CPSZ2 (seizures), and CP2_CPHI (high water mark), for NUMCALLPROCESSES, and
- CP_WAKESZ/WAKESZ2 (seizures), and CP2_WAKEHI (high water mark), for NUMCPWAKE.

In the following example, the Home switch leaves IPGW_PCM_SELECTION at its default value and increases the existing value of NUMPERMEXT from 244 to 340. This accounts for the 96 members in the POSIPVL dynamic POS trunk group. Home monitors OMs to determine values for NUMCALLPROCESSES and NUMCPWAKE.

**Figure 92 MAP display example for table OFCENG**

```
PARMNAME                    PARMVAL
-------------------------------------------------------------
IPGW_PCM_SELECTION          AUTO
NUMCALLPROCESSES            2000
NUMCPWAKE                   2800
NUMPERMEXT                  340
```

### PKTVPROF

Table PKTVPROF defines profiles used for packetized voice. TOPS-IP infrastructure considerations for table PKTVPROF are discussed beginning on page 69.

For IP positions, table PKTVPROF is referenced by table TQCQINFO. IP positions support auto-compression. Refer to “Voice encoding and auto-compression” on page 117 for information about auto-compression.

In the following example, the Home switch datafills three packetized voice profiles.

**Figure 93 MAP display example for table PKTVPROF**

```
PROFNUM  CODEC  AUTOCOMP
-----------------------------------------------------------------
0        G711   N
1        G723   N
2        G711   Y G723
```

***Note:*** As explained on page 70, table PKTVPROF was significantly changed in TOPS19, and patch CFX84 modifies the interpretation of PKTVPROF datafill in loads earlier than TOPS19.

## TQCQINFO

Table TQCQINFO provides information about TOPS call queues, including a packetized voice profile index that applies to the call queue. In the following example, the Home switch specifies packetized voice profile index 2 against several call queues. This enables auto-compression. The effect is that G.711 encoding will be used when adequate bandwidth is available, but G.723 encoding will be used when the IWS detects voice quality problems, most likely due to inadequate bandwidth.

**Figure 94 MAP display example for table TQCQINFO**

```
QTYPE   QMSSERV   CWOFF   CWON    TREAT   ALTAREA   PKTVPROF
-----------------------------------------------------------
CQ131   TOPS_TA   500     1000    VACT     N          2
CQ132   TOPS_TA   500     1000    VACT     N          2
CQ133   TOPS_TA   500     1000    VACT     N          2
```

## TOPSPOS

Table TOPSPOS contains provisioning datafill for operator positions supported by the TOPS switch. This table is used only in TOPS standalone and OC host switches. Each tuple defines the voice and data link information for a single position. Table TOPSPOS allows each position's voice and data paths to be provisioned as either TDM or IP.

***Note:*** IP voice connectivity can be used only when IP data connectivity is used, and vice versa.

The VLPATH field consolidates the voice refinements and the DATAPATH field consolidates the data refinements (described on page 126). The POSAREA field contains no information specific to IP positions.

In the following example, the Home switch datafills two IP positions, both of which use dynamic POS trunk group POSIPVL for voice connectivity at DTC 1. A description of the VLPATH refinements follows the example.

**Figure 95 MAP display example for table TOPSPOS**

```
POSNO    VLPATH              DATAPATH      POSAREA
-------------------------------------------------------------------
501      PKTV POSIPVL        IP 19 N       OPR 6 20
502      PKTV POSIPVL        IP 19 N       OPR 6 20
```

For IP position voice communication, the VLPATH field consists of the following subfields and refinements:

- VLTYPE defines PKTV (packetized voice) as the type of voice connectivity.
- VLCLLI specifies the voice link CLLI used for standalone calls with the IP position. This CLLI must be datafilled as a dynamic POS trunk group in table TRKOPTS (page 132).

***Note:*** This voice link CLLI is not used for host voice bypass calls. Table control allows the user to enter a CLLI that is datafilled only in table CLLI, and not in the trunk or inventory tables. This is referred to as a *placeholder CLLI*, and it may be appropriate in a pure OC host whose calls are all from OC-IP remotes. However, there are important limitations, discussed in "Operator-originated calls" on page 149, on the functionality that is available to positions datafilled with placeholder CLLIs. For that reason, table control displays a warning and requires the user to confirm before it allows a placeholder CLLI to be datafilled.

## Overview of datafill for reporting IP position trouble

This section introduces the datafill that allows service providers to associate text with error codes returned by IP positions. The text is used in log reports and in displays at the MAP.

The tables are described in the following order:

- MTCFAIL (Maintenance Failure Messages)
- MTCTEST (Maintenance Test Failure Messages)

***Note:*** These tables are not specific to TOPS-IP. However, IP positions may return different failure codes than TDM positions, so new datafill may be needed for IP positions.

### MTCFAIL

Table MTCFAIL associates text strings with numeric failure codes that may be sent from operator positions to the switch. If a failure code is datafilled in table MTCFAIL, the switch includes the associated text string when it reports the failure.

IP positions can notify the switch that they need to be removed from service. When an IP position does this, it indicates whether it is troubled. If it is troubled, the out of service notification message includes a failure code. If that failure code is datafilled in table MTCFAIL, the switch uses the associated text string in the position state change log report (see "TOPS502" on page 471).

The following example shows a text string datafilled against one of the failure codes that IP positions can send to the switch.

**Figure 96 MAP display example for table MTCFAIL**

```
ERRCODE                                                    ERRTEXT
-----------------------------------------------------------------
156                              POSITION_MAINTENANCE_IN_PROGRESS
```

***Note:*** Refer to *TOPS IWS Base Platform User's Guide* for information about the failure codes that an IP position can send to the switch.

## MTCTEST

Table MTCTEST associates text strings with numeric failure codes that may be sent from operator positions to the switch in response to a test command issued at the MAP. If the failure code is datafilled in table MTCTEST, the switch includes the associated text string when it reports the test failure.

For IP positions, the text string datafilled in table MTCTEST is displayed to the MAP user when the user issues the TST command and the position reports test failure.

The following example shows a text string datafilled against one of the test failure codes that IP positions can send to the switch.

**Figure 97 MAP display example for table MTCTEST**

```
ERRCODE                                                    ERRTEXT
-----------------------------------------------------------------
153                                  INITIALIZATION_IN_PROGRESS
```

***Note 1:*** Refer to *TOPS IWS Base Platform User's Guide* for information about the failure codes an IP position can send to the switch in response to a test command from the MAP.

***Note 2:*** Refer to page 352 for more information about the TST command for IP positions.

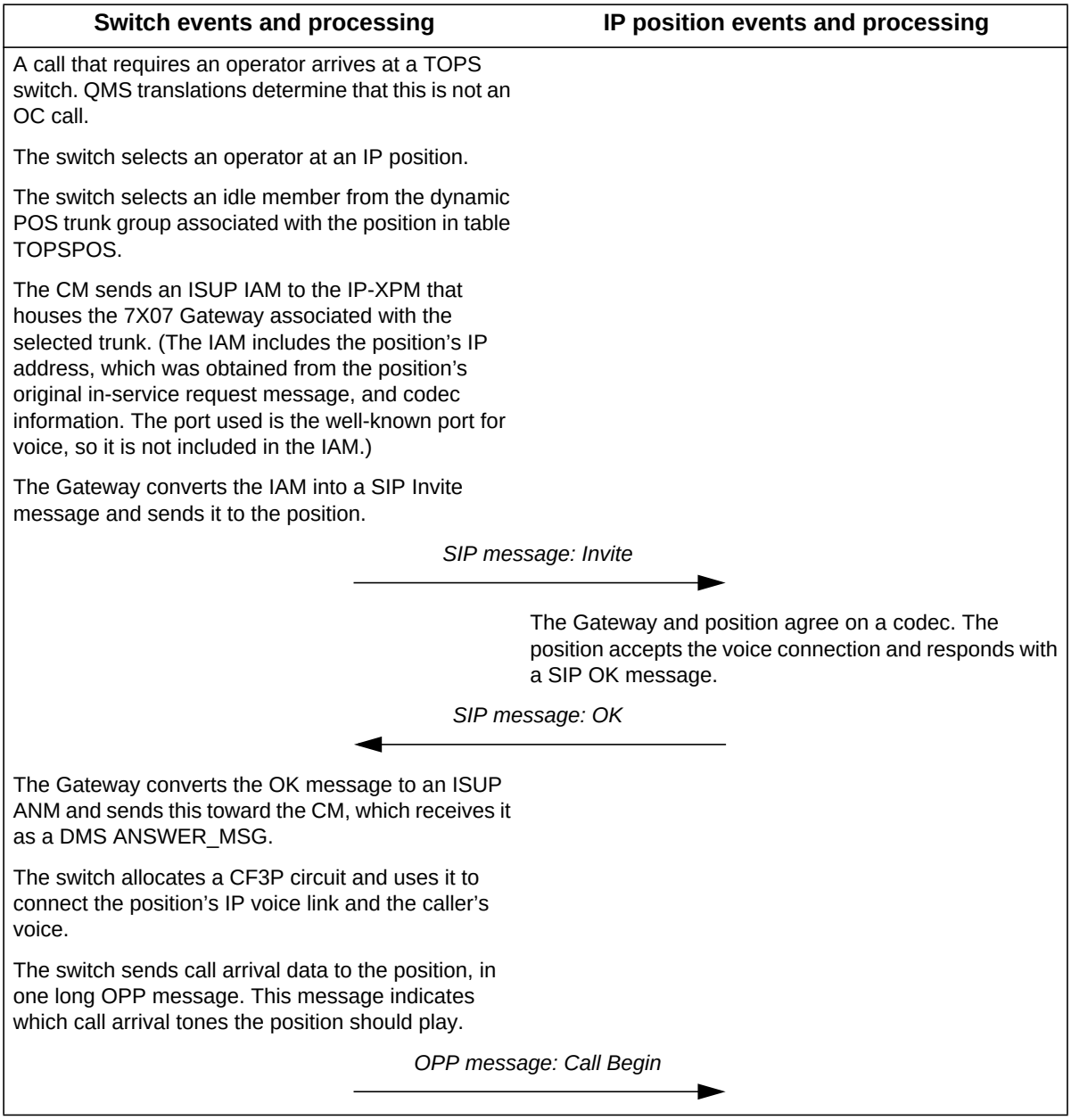
## Successful IP position call flows

This section shows successful IP position call flows for a TOPS standalone call, a call that uses traditional TDM-based OC, and an OC-IP call.

### Standalone call with IP position

Figure 98 shows an example standalone call flow that uses an IP position. The example illustrates the use of the position's voice and data links. The arrows represent both position data link messages (OPP) and voice-related call control messages (SIP).

**Figure 98 Example of IP position standalone call flow**



| Switch events and processing | IP position events and processing |
|---|---|
| | The position displays the call arrival information for the operator and generates the call arrival tones. |
| The call is established and data messages are processed. | The caller and the operator converse. The operator may key in call information. The position may exchange OPP messages with the switch. The position may also communicate with various data bases. |
| When the call is complete, the switch breaks its voice connections and deallocates the CF3P. It sends toward the position an ISUP REL message (converted by the 7X07 to a SIP Bye) to close the VoIP connection. It also sends an OPP message instructing the position to end the call. | |
| | *SIP message: Bye* → |
| | *OPP message: Call End* → |
| The switch generates an AMA record. | The position responds to the SIP Bye by sending a SIP OK and closing its end of the voice connection. |
| | *SIP message: OK* ← |
| The 7X07 converts the OK to an ISUP RLC and sends it to the XPM main processor, which processes it but does not forward anything to the CM. | The position responds to the OPP Call End message by clearing the call and letting the switch know it is ready for a new call. |
| | *OPP message: Call Cleared ACK* ← |
| The switch marks the position available to serve the next call. | |

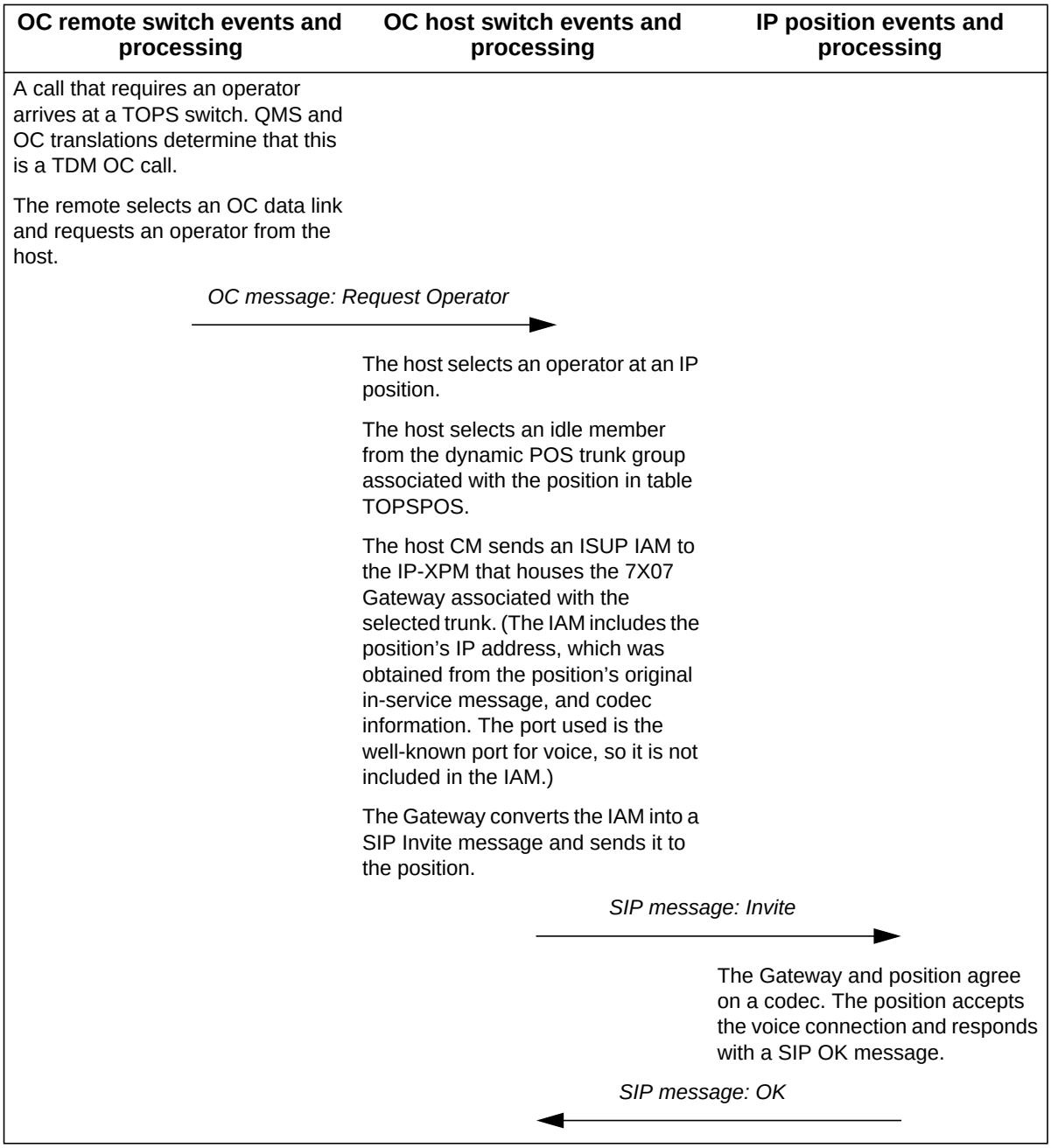
***Note:*** Voice setup between the Gateway and the position actually involves more messaging than the table shows. The table shows only the SIP messages that corresponds to ISUP messages exchanged between the Gateway and the SX05DA.

## Traditional OC call with IP position

Figure 99 shows an example IP position call flow that uses traditional OC. The example illustrates the use of voice and data links in this configuration. The arrows represent OC and position data link messages (OC and OPP protocols), and also voice-related call control messages (SIP) for the VoIP connection between the host and the position.

***Note:*** TDM OC links must be replaced by OC-IP links.

**Figure 99 Example of IP position call flow with traditional OC**



| OC remote switch events and processing | OC host switch events and processing | IP position events and processing |
|---|---|---|
| | At the host, the 7X07 converts the OK message to an ISUP ANM and sends this toward the CM, which receives it as a DMS ANSWER_MSG.<br><br>The host selects a TDM OC voice link and connects it to the IP position voice link.<br><br>The host informs the remote that a position has been allocated for the call. (This message includes an identification of the OC voice link selected by the host. It also indicates that an IP position was selected.) | |
| | *OC message: Got Operator* ← | |
| The remote allocates a CF3P circuit and uses it to connect the OC voice link and the caller's voice.<br><br>The remote sends call arrival data to the host, in a series of OPP messages encapsulated in a series of OC messages. (The encapsulated OPP messages include an indication of which call arrival tones to play.) | | |
| | *OC message: OPP Call Begin* → | |
| | . . . | |
| | *OC message: OPP Call Updates* → | |
| | The host extracts the individual OPP messages and builds them into a single long OPP message to send to the position. | |
| | | *OPP message: Call Begin* → |
| | | The position displays the call arrival information for the operator and generates the call arrival tones. |
| The call is established and data messages are processed. | The host forwards OPP key function and screen update messages between the remote and the position as needed to process the call. | The caller and the operator converse. The operator may key in call information. The position may exchange OPP messages with the switch. The position may also communicate with various data bases. |

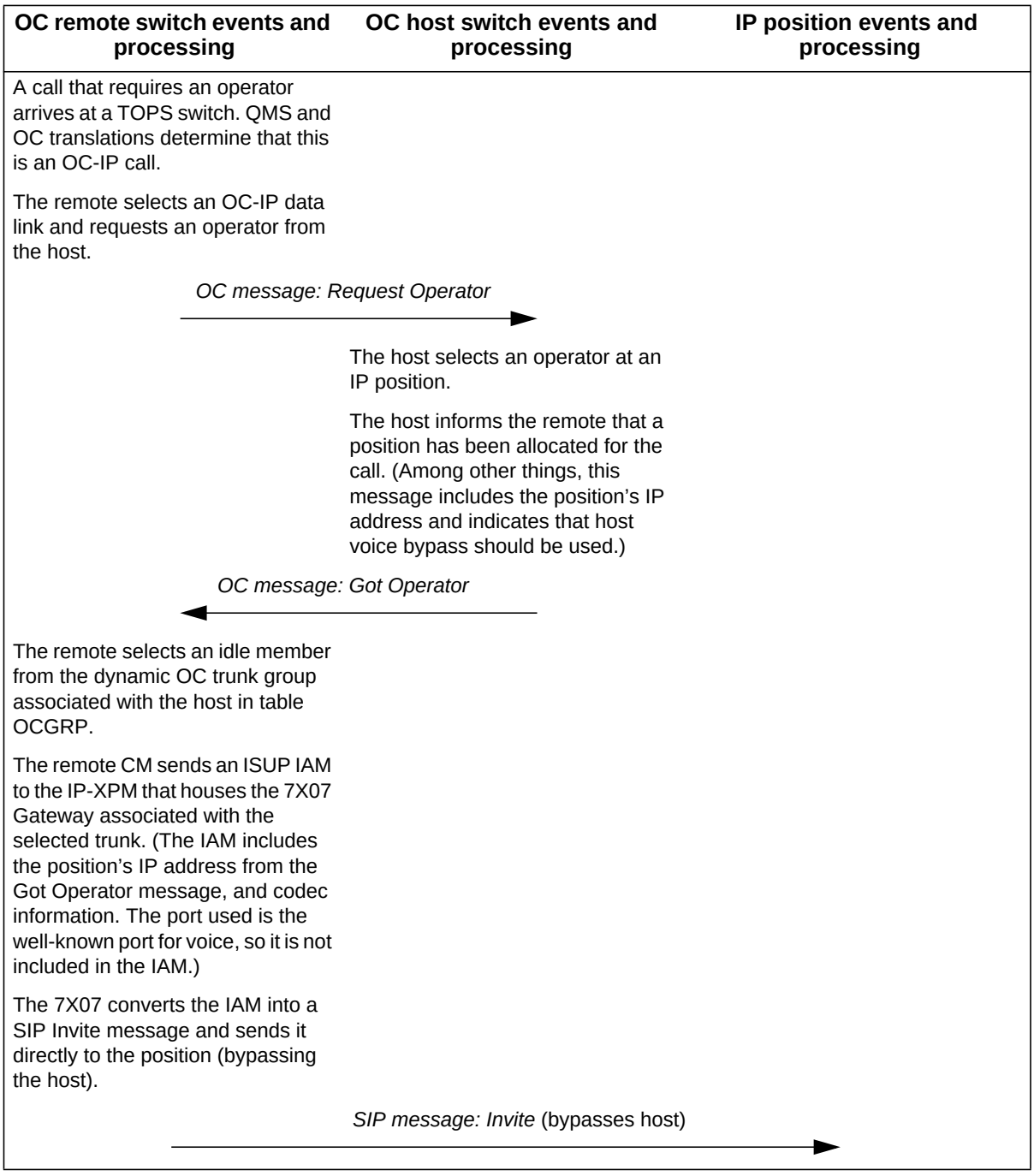
| OC remote switch events and processing | OC host switch events and processing | IP position events and processing |
|---|---|---|
| When the call is complete, the remote breaks its voice connections, deallocates the CF3P, frees its end of the OC voice link, and instructs the host to release its resources. | | |
| | *OC message: Release Operator* → | |
| | The host acknowledges to the remote that it is freeing its resources. | |
| | ← *OC message: Operator Released* | |
| The remote frees its remaining resources and generates an AMA record. | The host sends toward the position an ISUP REL message (converted by the 7X07 to a SIP Bye) to close the VoIP connection. It also sends an OPP message instructing the position to end the call. | |
| | *SIP message: Bye* → | |
| | *OPP message: Call End* → | |
| | | The position responds to the SIP Bye by sending a SIP OK and closing its end of the voice connection. |
| | ← *SIP message: OK* | |
| | The 7X07 converts the SIP OK to an ISUP RLC and sends it to the XPM main processor, which processes it but does not forward anything to the CM. | The position responds to the OPP Call End message by clearing the call and letting the host know it is ready for a new call. |
| | ← *OPP message: Call Cleared ACK* | |

***Note:*** Voice setup between the Gateway and the position actually involves more messaging than the table shows. The table shows only the SIP messages that corresponds to ISUP messages exchanged between the Gateway and the SX05DA.

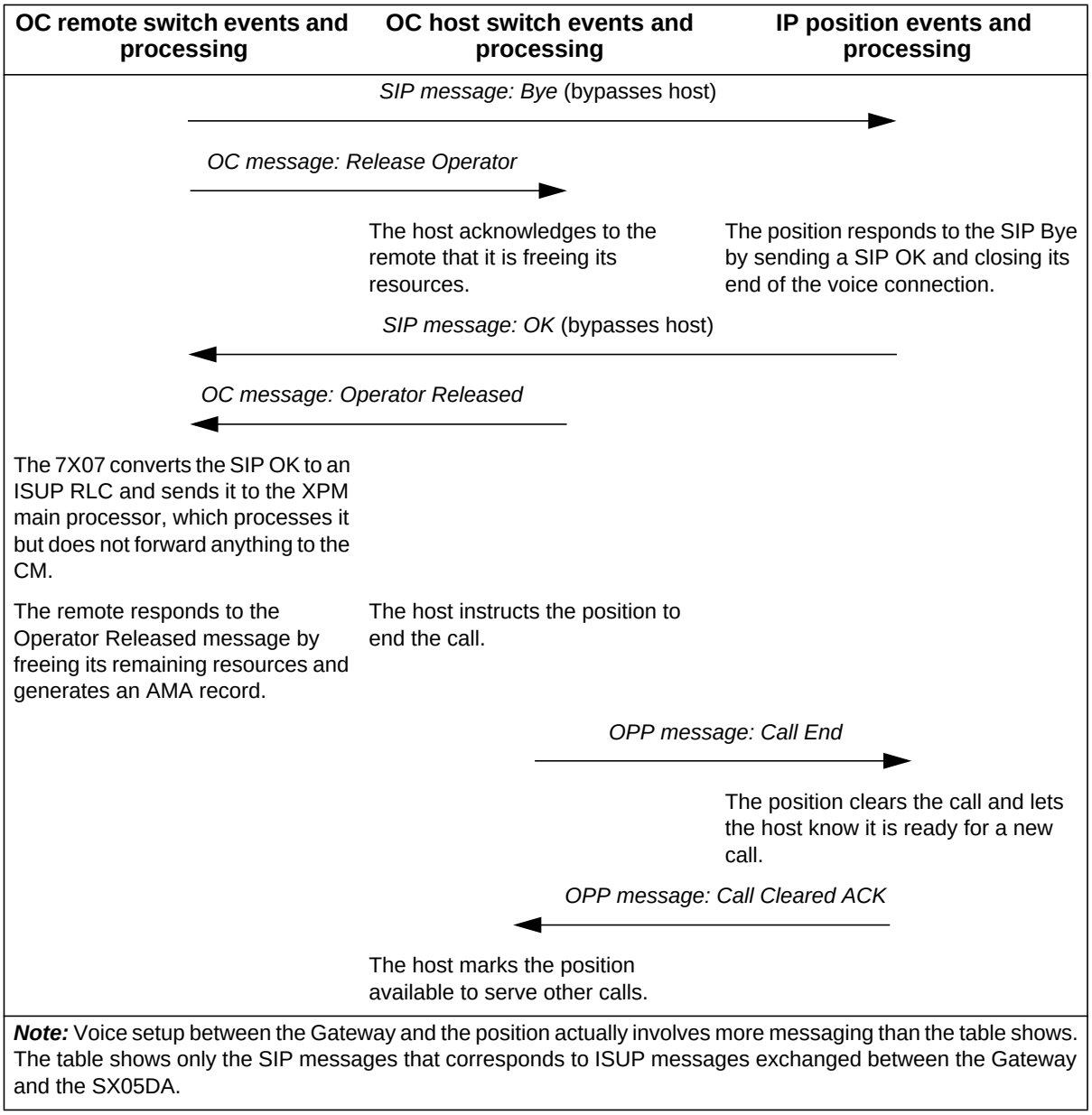
## OC-IP call with IP position

Figure 100 shows an example IP position call flow that uses OC-IP. This is a host voice bypass call. The example illustrates the use of voice and data links. The arrows represent messages sent and received on OC and position data links (OC and OPP protocols), and also voice-related call control messages (SIP) for the VoIP connection between the remote and the position.

**Figure 100 Example of IP position call flow with OC-IP call flow**



| OC remote switch events and processing | OC host switch events and processing | IP position events and processing |
|---|---|---|
| | | The Gateway and position agree on a codec. The position accepts the voice connection and responds with a SIP OK message. |
| | | *SIP message: OK* (bypasses host) ← |
| At the remote, the Gateway converts the OK message to an ISUP ANM and sends this toward the CM, which receives it as a DMS ANSWER_MSG. | | |
| The remote allocates a CF3P circuit and uses it to connect the IP voice link and the caller's voice. | | |
| The remote sends call arrival data to the host, in a single long OPP message encapsulated in an OC message. (The encapsulated OPP message include an indication of which call arrival tones to play.) | | |
| *OC message: OPP Call Begin* → | | |
| | The host extracts the OPP call arrival data and forwards it to the position in a single long OPP message. | |
| | | *OPP message: Call Begin* → |
| | | The position displays the call arrival information for the operator and generates the call arrival tones. |
| The call is established and data messages are processed. | The host forwards OPP key function and screen update messages between the remote and the position as needed to process the call. | The caller and the operator converse. The operator may key in call information. The position may exchange OPP messages with the host. The position may also communicate with various data bases. |
| When the call is complete, the remote breaks its voice connections and deallocates the CF3P. It sends toward the position an ISUP REL message (converted by the 7X07 to a SIP Bye) to close the VoIP connection. It also sends the host a message instructing it to release its resources. | | |




***Note:*** Voice setup between the Gateway and the position actually involves more messaging than the table shows. The table shows only the SIP messages that corresponds to ISUP messages exchanged between the Gateway and the SX05DA.

# IP position call processing interactions and failure handling

This section discusses the operation and interactions of the following call processing-related topics:

- call arrival tones
- assistance requests
- position monitoring
- operator-originated calls
- loop access and held calls
- force management statistics
- failure handling

## Call arrival tones

Traditionally the DMS switch has generated call arrival tones heard by TOPS operators. This is not true with IP positions. These positions generate their own call arrival tones for the operator. The data that the switch sends to an IP position at call presentation includes information about switch datafill for call arrival tones, so that the position can generate tones similar to the ones the switch would generate for a TDM position.

Generating the call arrival tones at the position allows the position to synchronize the tones with the screen updates for a call.

***Note:*** External interactive voice response systems, such as DA automation systems, may also generate call arrival tones. The IP position application does not change that.

## Assistance requests

When an operator requests assistance, table TQMSFCQA is referenced based on the CT4Q of the call. Table TQMSFCQA specifies whether the type of assistance for a CT4Q is SA (service assistance) or CSE (customer service expert).

### SA requests

SA assistance is not supported with IP positions. If an operator at an IP position requests assistance and the CT4Q of the call is datafilled for SA, the request is denied.

### CSE requests

IP positions fully support CSE assistance. There is no restriction on position type for either the operator requesting assistance or the CSE providing assistance. One, both, or neither can be at IP position.

## Position monitoring

TOPS has traditionally supported the capability of supervisory operators to monitor the calls that are processed at another position of the same type and protocol, and hosted by the same switch. Essentially the same functionality is supported with IP positions, but there are some differences.

The differences are transparent to the operator who is being monitored, but not to the operator doing the monitoring. The reasons for the differences are (a) a new voice connection is established each time a new call becomes active at an IP position, and (b) the voice connection bypasses the host, where monitoring connections have traditionally been made, when an OC-IP call is served by an IP position.

The following paragraphs describe the operation and limitations of IP position monitoring.

### Monitoring screen displays

Monitoring of screen displays works the same with IP positions as with TDM positions: all screen updates sent to the monitored position, from the switch or the DA system, are also sent to the monitoring position. Limitations are the same as with TDM positions:

- The monitoring and monitored positions must be the same type and use the same protocol. (This implies that monitoring between TDM and IP positions is not supported.)
- The monitoring and monitored positions must be hosted by the same switch.
- The monitor does not see keystrokes entered by the monitored operator.
- The monitor does not see local screen updates, such as context switches between the billing and search screens on DA calls.
- The monitor does not see screen updates that the monitored position makes as a result of interactions with external systems (other than the switch and the DA system) such as web servers.
- If a monitoring session begins while the monitored operator has a call, the monitor’s screen display will be incomplete until the next new call arrives.

### Monitoring voice

Voice connectivity for monitoring works very differently with IP positions.

- IP position monitoring does not employ an extra CF3P circuit in the switch, as TDM position monitoring does.
- Unlike TDM position monitoring, a new monitoring voice connection is made each time a new call becomes active at the monitored position.

One implication is that the monitoring position has no voice connection, and cannot hear the operator, when the operator has no call. Another implication is that if a monitoring session begins while the monitored operator has a call, the monitor will not hear anything until the next *new* call arrives at the position.

- Monitoring voice connections are made in the 7X07 Gateway card that connects to the monitored position for the call.

Each 7X07 Gateway has 60 DSP (digital signal processor) channels. However, limitations in the CM and XPM main processor prevent a Gateway from supporting more than 48 dynamic trunks. So each Gateway has 12 DSP channels that are available for any application that does not involve a trunk member from the CM and XPM perspective.

The IP position application takes advantage of this situation and makes the extra DSP channels available for monitoring. The CM sends monitoring information to the Gateway in the ISUP IAM message at the beginning of the call. After that, the CM has no further involvement until the beginning of the next call. The Gateway and the monitoring position handle all the monitoring connections and disconnections. The voice is bridged in the Gateway.

In the unlikely event that the Gateway is simultaneously using all 12 of its extra DSP channels for monitoring sessions, it will be unable to satisfy the next switch request for monitoring. In that case an IPGW600 log is generated with text “No monitoring ports available.” The monitored call proceeds normally, and the monitor sees the screen updates but hears no voice.

### Operator-originated calls

There are several scenarios in which an operator may access a loop to originate a call. This is significant because these call are *always* handled as standalone calls, and they require 7X07 Gateway resources even in an OC host whose subscriber calls are all OC-IP (bypassing the host in their voice connections.) In addition to operator-originated calls, booked call database calls are also always handled as standalone calls.

The following calltypes require voice resources even in an OC host whose subscriber-originated calls are all OC-IP (bypass) calls:

- Delay calls. An operator may access an idle loop and connect back to a subscriber who attempted a call earlier but the call could not be established at that time.
- Operator-originated calls to other internal or external numbers. For example, an operator might access an idle loop to call the business office or a poison control center.
- Directed assistance requests. To make a directed assistance request using QMS CASE, an operator withholds calls, accesses an idle loop, and keys to request a connection with a specified operator or position.
- Response to a page. This uses the same underlying implementation as directed assistance.

- Booked call database calls. A booked call database call initiates automatically when its time-of-day timer expires.

All of the above-listed calltypes will fail if a placeholder CLLI (see page 126) is datafilled in table TOPSPOS for the position.

### Loop access and held calls

An IP position can have only one voice connection at a time. When an operator at an IP position has a call on one loop and keys to access the other loop, or to explicitly place the call on hold, the existing IP voice connection is released. A new voice connection is establish when the operator keys to re-access the held call (or, in the case of calls on temporary hold, when the call is auto-accessed).

One implication is that if there is a problem with voice on a TA call, the operator may try placing the call on hold and re-accessing it. (This only works for TA calls, since DA calls cannot be placed on hold.)

Another implication is that it is possible for there to be trouble establishing a new voice connection when a held call is re-accessed. If that happens, the switch allows the held call to be accessed without voice. See “Failure handling” on page 151 for more information.

### Force management interactions

Force management (FM) statistics are affected by three characteristics of IP position call processing:

- It takes longer to set up an IP voice connection than to supervise a nailed-up TDM connection.
- IP position calls have an extra call cleared acknowledgment message at the end of each call.
- The call arrival data is sent to an IP position in one long message rather than in multiple shorter messages.

The first two characteristics result in an increase in the operator’s idle time (IDLT). Any derived statistics that are based on IDLT will also be affected. An example is percent occupancy (%OCC). Since %OCC is calculated by dividing the total work volume by the sum of total work volume and idle time, increased IDLT implies lower %OCC.

The third characteristic tends to decrease the time it takes to process a call, since the screen pop may be faster.

***Note:*** For more information on force management statistics, refer to *TOPS IWS Force Management Guide*.

## Failure handling

This section discusses IP position failure-handling strategies. Before continuing with this section, please review the overview description on page 108 of TOPS failure-handling strategies. Briefly, the main strategies are to requeue the call, to reroute the call either to an alternate host or to treatment, and to end the call. Normally it is possible to recover by requeuing or rerouting the call if the failure occurs during setup, before the call has been presented to the operator. Normally it is not possible to recover from failures that are detected after the call has been successfully presented to an operator; these failures usually cause the call to be ended.

### Resource failures

The following resource failures may affect IP position call processing:

- *No available voice circuits*. If a voice link (dynamic trunk member) cannot be obtained for establishing a VoIP connection to an IP position, the requeuing strategy is used. This occurs regardless of whether the failure was in a standalone switch, an OC host (with TDM-OC), or an OC remote (with OC-IP).

  There are exceptions to this rule. For example:

  — If a voice link cannot be obtained to connect a CSE to a call that is still at the requesting operator's position, the CSE is released and the call remains active at the requesting operator's position.

  — If a voice link cannot be obtained to access a loop that has a held call, the switch allows the loop to be accessed without voice. The operator will realize there is a problem, and can do one of two things: (a) cancel and release the call, or (b) key to hold and re-access the call. The latter will work if the failure was transient and a voice circuit is available on the re-try.

- *No available RU or CF3P*. If a standalone, remote, or host switch fails to allocate a needed recording unit or CF3P circuit for a call involving an IP position, the requeuing strategy is used.

### Messaging problems

As explained elsewhere in this book (page 43, page 110), the OPP and SIP messages used to set up a call at an IP position use the UDP protocol, and while UDP has certain advantages, it is susceptible to lost messages in an improperly engineered network.

***Note:*** For more information on network engineering for TOPS-IP, refer to Chapter 7: "TOPS-IP engineering guidelines."

Other messaging problems can also occur. Depending on where in the call flow a messaging problem occurs, the impact can range from no response at the operator position (the operator will retry) to call take-down.

The following messaging problems can affect IP position call processing:

- *Acknowledgement time-out in call setup*. Successful call setup at an IP position involves an exchange of SIP messages. (If it is an OC call, OC messages are also exchanged during setup. For details, see the call flows that begin on page 139.) The switch sets a timer whenever it is expecting a call setup message, and if one of these timers expires, the switch reroutes the call. The reroute reason for table OCHOSTQ is DEFLECT.

  There are exceptions to this rule. For example, if the switch times out attempting to connect a CSE to a call that is still at the requesting operator's position, the CSE is released and the call remains active at the requesting operator's position.

- *Voice link signaling errors.* If a voice link signaling error is detected during setup (such as receiving an ISUP REL before receiving the ISUP ANM), the voice link to the position is released and the call is rerouted with reason DEFLECT. However, if a voice link signaling error is detected after setup, the call is ended.

- *Acknowledgement time-out in call take-down*. When a call leaves an IP position, the position sends the switch a message indicating it is ready to receive a new call. The switch does not select the position for a new call until it has received this message. If the switch times out waiting (lost message or problem with the position itself), it places the position in a make busy state. This is similar to the requeuing strategy described on page 108, except it only affects the position, since there is no call to requeue.

  ***Note:*** This would happen if data connectivity to the position were unexpectedly lost.

- *Lost Call Begin message*. As with TDM positions, operators at IP positions may occasionally receive a voice call with no screen update, and if this happens, the operator can recover by keying to request call details.

- *Unexpected messages.* As is done with TDM positions, unexpected messages will take a call down.

### OSSAIN calls with operators

An OSSAIN call can attach an operator while the service node (SN) is still connected to and controlling the call. In this scenario, most failures cause the switch to inform the SN of the problem, leaving the decision about how to handle the failure up to the SN.

### IWS failure handling

So far this section has addressed only the switch actions to handle failures. The IWS position also has failure-handling strategies. Some of the more important ones are:

- If the IWS is in-service but has not received any messages from the switch for a certain length of time, it audits the switch. In case there is no response to a series of these audits, the position removes itself from service, indicates to the operator that there is a link problem, and begins sending periodic in-service request messages to the switch.

  This prevents the position from appearing to have data connectivity to the switch when, in fact, connectivity has been lost.

- If the position receives an response to its audit (see previous bullet) and it has no call, but an operator is logged in and has keyed to accept calls, the position sends the switch another message requesting to accept calls.

  This facilitates recovery in case the switch has placed the position in a make busy state but the position did not receive the message informing it of its state.

# Chapter 5: TOPS QMS MIS-IP application

The TOPS-IP product implements Queue Management System Management Information System (QMS MIS) over an IP infrastructure. This chapter describes the TOPS QMS MIS-IP application, focusing on the following areas:

- background on traditional QMS MIS capabilities and connectivity
- introduction to QMS MIS-IP connectivity and messaging
- overview of datafill for QMS MIS-IP data links
- transition strategy for QMS MIS-IP

## QMS MIS background

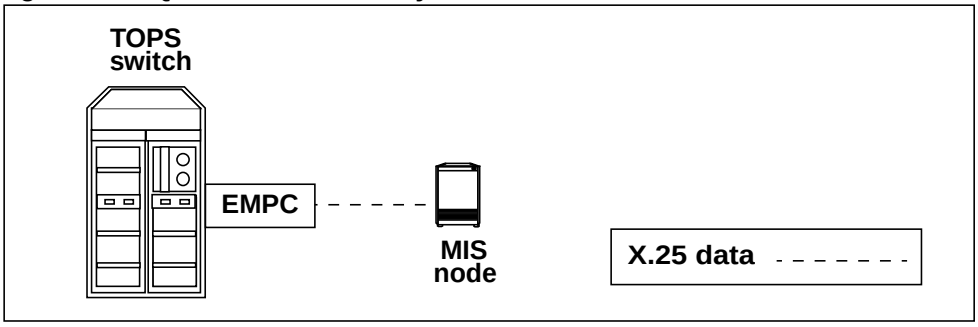
TOPS QMS MIS is a switch application that collects event-driven data about TOPS calls and sends this data to an external reporting facility, such as an MIS vendor server. With QMS MIS, the switch sends the data continuously and within a few seconds of the event. The MIS vendor can choose, depending on the event information, which real-time statistics and periodic reports to generate.

***Note:*** The switch does not receive any application-level messages from the MIS node; data communication is one-way only.

### QMS MIS data connectivity

Figure 101 shows an example of the traditional connectivity for TOPS QMS MIS. In the figure, TOPS QMS MIS data is through an X.25 interface and an enhanced multiprotocol controller (EMPC) card.

**Figure 101 QMS MIS connectivity without TOPS-IP**



## QMS MIS-IP introduction

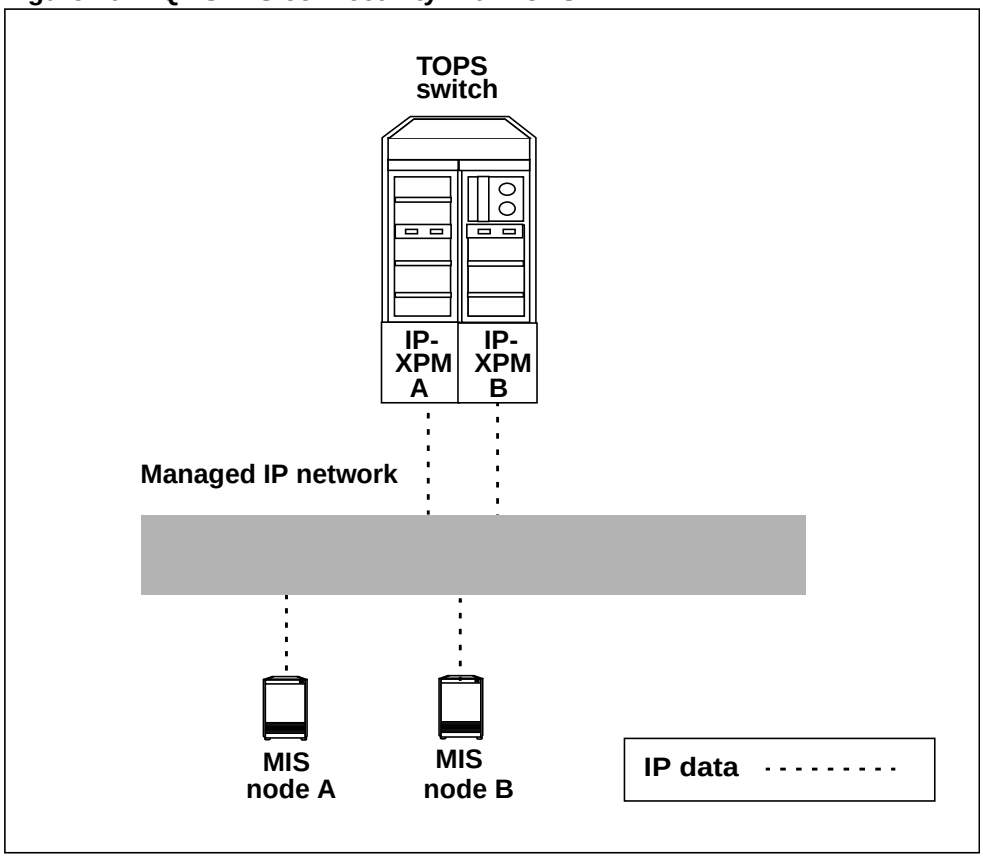
In a TOPS-IP network, a common IP infrastructure replaces the provisioning of X.25 data for the TOPS QMS MIS application. Using a DTC equipped with an SX05DA processor, the QMS MIS application sends data to an MIS node over the managed IP network.

With QMS MIS-IP, the TOPS switch can have up to two TCP (Transmission Control Protocol) connections that transmit the same MIS data across the network. This capability allows the TOPS switch to send MIS data to more than one vendor or to increase the reliability of the MIS data sent to a single vendor.

The peripheral that supports QMS MIS-IP must be a dedicated peripheral that does not contain 7X07 Gateway cards (which are used only for voice over IP applications). This peripheral cannot be used to support the OC-IP application. For details on engineering, refer to Chapter 7: "TOPS-IP engineering guidelines."

Figure 102 shows a TOPS switch having two QMS MIS-IP connections, one on each IP-XPM.

**Figure 102 QMS MIS connectivity with TOPS-IP**



***Note 1:*** TOPS-IP software does not remove the ability to use the existing X.25 data interface for QMS MIS. The switch may use *either* the IP interface or the X.25 interface to send TOPS QMS MIS data, but not both interfaces at the same time.

***Note 2:*** TOPS QMS MIS connectivity differs from OSSAIN QMS MIS connectivity, which is through an Ethernet interface and a peripheral module equipped with an Ethernet interface unit (EIU). Provisioning of Ethernet data for the OSSAIN MIS application is unchanged.

## MIS-IP messaging

The QMS MIS-IP application runs as a separate process in the TOPS switch. The application receives call and position event messages, buffers the messages, and sends them to the external MIS node. The switch is the client, and the MIS node is the server. No application-level messages are sent from the MIS node to the switch, and the switch does not store any QMS MIS buffers for later retrieval.

### Buffering MIS messages

The DMS switch buffers messages internally. The number of buffers is not datafillable. The TOPS QMS MIS-IP application sends the entire buffer to the MIS node after any of the following conditions are met:

- when the buffer is full
- when a report period ends
- when the specified maximum buffer transmit interval timeout expires
- after a warm restart

***Note 1:*** The maximum buffer transmit interval for the QMS MIS-IP application is set in table QMSMIS. For details on the datafill values, refer to Chapter 8: “TOPS-IP data schema.”

***Note 2:*** During a change of interface (from X.25 to IP or vice versa) any MIS buffers that have not been sent out are lost.

### Sending MIS messages

The QMSMIS protocol is used at the application layer to send MIS messages. TCP is used at the transport layer. Using TCP, the QMS MIS application sends a 1450 byte-message (including padding if the message has fewer than 1450 bytes) to the IP-XPM for transmission to the MIS node. The XPM establishes a TCP connection when the IP interface is datafilled or when the QMS MIS application tries to send a message buffer for the first time. After the connection is established, the QMS MIS application continues to send message buffers.

***Note 1:*** Table TQMISOPT (TOPS QMS MIS Options) contains parameters used by the QMS MIS application. Before provisioning MIS-IP, users should review the datafill for these parameters. For details, refer to *Customer Data Schema Reference Manual*.

***Note 2:*** For more information on the QMSMIS protocol, refer to *TOPS QMS MIS Protocol*, Q220-1.

### MIS-IP fault detection and correction

For information on correcting and recovering from faults during QMS MIS-IP processing, refer to Chapter 10: "TOPS-IP maintenance activities."

***Note:*** If a switch of activity (SWACT) in the XPM occurs, QMS MIS alarms and logs are generated to indicate that the TCP connection was taken out of service. In this scenario, when the SWACT completes, the TCP connections are eventually re-established and the alarms are cleared.

## Overview of datafill for QMS MIS-IP data links

This section introduces the datafill required for QMS MIS-IP data links in table QMSMIS. The QMS MIS-IP application depends on the IP data infrastructure, so datafill is first required in the following tables:

- LTCINV
- XPMIPGWY
- XPMIPMAP
- IPSVCS
- IPCOMID

***Note:*** For an overview of these tables, refer to Chapter 2: "TOPS-IP data and voice communication."

### QMSMIS

Table QMSMIS specifies provisioning information for each QMS MIS application on the TOPS switch. Datafill values include the application name, data connectivity type, maximum buffer transmit interval, and destination information. The TOPS QMS MIS-IP application supports up to two IP connections for transmitting the same MIS data stream.

***Note 1:*** Although table control allows datafill for four IP connections, only two are supported by TOPS-IP. The second MIS-IP data link may be provisioned for redundancy or for communication to a second MIS node. For engineering information, refer to Chapter 7: "TOPS-IP engineering guidelines."

***Note 2:*** To minimize TCP re-establishment delays, it is recommended that table IPSVCS be datafilled with a PORT value of 0 for the QMS MIS-IP service tuple. A value of 0 is used to request the IP-XPM to randomly assign a port number.

In the following example, the TOPS QMS MIS application specifies the IP interface, IP address, port, and desired status of the destination MIS node. Also, the IP connection references a unique COMID from table IPCOMID, which indirectly identifies the IP address and port on the IP-XPM used for the data connection.

**Figure 103 MAP display example for table QMSMIS**

```
INDEX        DATALINK
-------------------------------------------------------------
TOPS         IP  10 (123 15 3 5    2003     ACTIVE     30) $
```

***Note:*** When the destination status of the node is set to INACTIVE, the switch does not send MIS message buffers to this node.

## Transition strategy for QMS MIS-IP

The strategy for transitioning traditional TOPS QMS MIS to the IP interface involves the following broad steps:

1 Determine the number of QMS MIS-IP data links and IP-XPMs to provision at the TOPS switch. Refer to Chapter 7: "TOPS-IP engineering guidelines."

2 Datafill the IP infrastructure in tables LTCINV, XPMIPGWY, and XPMIPMAP. Refer to Chapter 8: "TOPS-IP data schema." Also refer to this chapter for the range of valid values and possible error messages for all TOPS-IP-related tables.

3 Datafill the QMS MIS-IP application in tables IPSVCS, IPCOMID, and QMSMIS. Example datafill is shown in "Changing the QMS MIS interface."

***Note 1:*** An office that is currently using the traditional MIS (X.25) interface is automatically switched to use the MIS-IP interface after it is datafilled.

***Note 2:*** TOPS-IP software does not remove the ability to use the existing X.25 data interface for QMS MIS. The switch may use *either* the IP interface or the X.25 interface to send TOPS QMS MIS data, but not both interfaces at the same time.

### Changing the QMS MIS interface

This section shows example QMS MIS-IP datafill in three tables:

- IPSVCS
- IPCOMID
- QMSMIS (before and after)

### IPSVCS

The following example shows datafill in table IPSVCS. The PORT field is datafilled with a value of 0 to avoid TCP re-establishment delays. This value is used to request the XPM to randomly assign a port number.

**Figure 104 MAP display example for table IPSVCS**

```
SERVICE           PORT       PROTOCOL
-------------------------------------------------------------------
QMSMIS            0          TCP
```

### IPCOMID

The following example shows datafill in table IPCOMID. DTC 20 supports the port and protocol identified by the service name QMSMIS.

**Figure 105 MAP display example for table IPCOMID**

```
COMID     SERVICE          XPMNAME
-----------------------------------------------------
30        QMSMIS           DTC 20
```

### QMSMIS

The following example shows datafill in table QMSMIS *before* changing the MPC interface. The type of data link is MPC for the X.25 interface.

**Figure 106 MAP display example for table QMSMIS—MPC (X.25) interface**

```
INDEX        DATALINK
-------------------------------------------------------------
TOPS         MPC 1 2 4
```

The following example shows datafill *after* changing the interface to IP. The type of data link is changed to IP, with a maximum buffer transmit interval of 10 seconds.

**Figure 107 MAP display example for table QMSMIS—IP interface**

```
INDEX        DATALINK
-------------------------------------------------------------
TOPS         IP  10 (123 15 3 5    2003     ACTIVE     30) $
```

***Note:*** During a change of interface, any MIS buffers that have not been sent out are lost.

# Part 3: Interactions

Part 3: Interactions includes the following chapter:

# Chapter 6: TOPS-IP feature impact

This chapter lists the limitations and restrictions of TOPS-IP capabilities, focusing on the following areas:

- IP data communication
- IP voice communication
- IP-XPM
- managed IP network
- TOPS-IP product
- OC-IP application
- IP position application
- QMS MIS-IP application
- Simple Network Management Protocol (SNMP)

***Note:*** Chapter 7: "TOPS-IP engineering guidelines" also contains some limitations and restrictions that are not duplicated here.

## IP data communication limitations and restrictions

This section discusses limitations and restrictions for the following components of IP data communication:

- SX05DA processor
- IP port assignment datafill

### SX05DA processor

The following limitations and restrictions apply to using the SX05DA:

- Versions of the SX05 card that are previous to the DA version are not supported for TOPS-IP data communication.
- The firmware on the SX05DA card must be at release SXFWAG02 or higher. If the firmware is not at this level, the IP-XPM cannot be loaded with software and brought into service. The firmware load that is delivered with the XPM software release is recommended.

- During an XPM SWACT (including a warm SWACT), both TCP and UDP applications on the SX05DA may suffer a brief messaging interruption, and some calls may be dropped until the sockets are re-established.
- Although SX05DA-based and EIU-based IP functionality can co-exist on the same switch, they do not interact with each other. This means that IP tools for the EIU remain specific to the EIU, whereas IP tools for the SX05DA are specific to the IP-XPM.
- When the CM is responsible for SX05DA configuration, the CM downloads bootstrapping configuration datafill in table XPMIPMAP to the IP-XPM. If this datafill is inaccurate, the IP-XPM may fail to RTS, or if it does RTS, the messages sent from the IP-XPM may be misrouted. The datafill cannot be cross-checked before static data download, because the IP stack is located on the individual IP-XPM, not on the CM.
- When the CM is responsible for SX05DA configuration, users should update static data for the SX05DA whenever the GWINDEX field of table XPMIPMAP is changed. For details, refer to “Updating static data” on page 299.

  ***Note:*** When DHCP is selected as the configuration method, the IP-XPM receives configuration information from the DHCP server instead of from the CM.
- The SX05DA subnet is temporarily limited to a maximum of 32 IP operator positions. Offices with more than 32 positions must provision additional subnets and must provide routing facilities. XPM design is aware of this problem and is working toward a solution. Consult your Nortel Networks representative for updates and status on this open issue.
- Routing interfaces present in the SX05DA subnet must have the spanning tree algorithm disabled. Failure to disable spanning tree could result in the inability to bring the SX05DA in or to keep both units of the IP-XPM in service.

### IP port assignment datafill

The following limitations and restrictions apply to IP port assignment datafill for data communication:

- Ports datafilled in CM table IPSVCS can use port values in the range 2048 to 12287. Ports numbers outside this range are reserved for non-CM IP applications.

  ***Note:*** Port numbers 1 to 1024 are well-known industry-defined port numbers that are reserved for applications such as FTP (File Transfer Protocol), Telnet, and HTTP (Hypertext Transfer Protocol).

- Port numbers in table IPSVCS must be unique, with the exception of port number 0. A port number of 0 is used to request the XPM to randomly assign a port number in the range 32768 to 65535. More than one tuple may datafill a 0 in the PORT field. Port 0 should not be datafilled for the OC-IP or IP position applications. Only QMS MIS-IP can use port 0.

## IP voice communication limitations and restrictions

This section discusses limitations and restrictions for the following components of IP voice communication:

- dynamic trunk datafill
- dynamic trunk maintenance
- 7X07AA Gateway cards
- voice codecs

### Dynamic trunk datafill

This subsection describes how datafill affects the operation of dynamic trunks.

***Note:*** For more details on datafill requirements and possible error messages, refer to Chapter 8: "TOPS-IP data schema."

#### TRKGRP

The following limitations and restrictions apply to table TRKGRP:

- The trunk group type must be IT (intertoll) in table TRKGRP.
- The direction must be either 2W (two-way) or OG (outgoing).
- The value in the SELSEQ subfield should be set to MIDL (most idle) to ensure a uniform selection of members even if a 7X07 card is temporarily out of service.

#### TRKSGRP

The following limitations and restrictions apply to table TRKSGRP:

- Dynamic voice trunks require the following datafill:
  - subgroup number set to 0
  - card code set to DS1SIG
  - signaling selector set to C7UP
  - trunk direction must match table TRKGRP
  - protocol set to Q764
  - continuity testing set to 0
  - (2W only) glare set to CIC

### TRKOPTS

The following limitations and restrictions apply to table TRKOPTS:

- Dynamic voice trunks require the following datafill:
  - option set to DYNAMIC
  - call control signaling set to ISUP
  - network used for call control signaling set to IP
  - network used for voice (bearer) set to IP
  - application name set to OC or POS
- A single trunk group cannot be used for connections with both OC hosts and OC remotes.
- A single trunk group cannot be used for connections with both IP positions and OC remotes.
- The DYNAMIC option cannot be removed from a trunk group if members still exist in table TRKMEM, or if the CLLI group is datafilled against a Gateway entry in table IPINV.
- Certain fields in table TRKGRP and table TRKSGRP cannot be changed to inappropriate values if the trunk group is marked as DYNAMIC in table TRKOPTS. (For example, the Q764 value in table TRKSGRP cannot be changed to Q767.)

### IPINV

The following limitations and restrictions apply to table IPINV:

- For a TOPS Gateway type, the only fields that can be changed are LOAD and IPZONE, as follows:
  - The LOAD field is not used and should be datafilled with $.
  - The IPZONE field must match the IP address assigned to the 7X07 Gateway by the DHCP server. If it does not match, the Gateway will not come into service.
- For a TOPS Gateway type, the trunk CLLI name must be set to DYNAMIC in table TRKOPTS.
- For a TOPS Gateway type, a particular trunk CLLI name and starting trunk member number can be assigned to only one entry. An attempt to assign the same CLLI name and starting member number to another tuple is denied.
- Table IPINV must contain the appropriate number of TOPS Gateways that are associated with P-side links assigned in LTCPSINV, otherwise PM777 log reports are generated.
- A TOPS tuple cannot be deleted from table IPINV until its associated Gateway card is offline. The associated P-side links (LTCPSINV) must be manually busied at the PM level of the MAP.

- The trunk group size must be at least 48 in table CLLI; if not, adding Gateway cards in table IPINV fails.
- Removing TOPS entries in table IPINV automatically removes the associated members from table TRKMEM.

### TRKMEM

The following limitations and restrictions apply to table TRKMEM:

- Trunk groups typically have a maximum of 2048 members. Since IPINV allocates 48 members at a time, this maximum is limited to 2016 for dynamic trunk groups used by TOPS-IP applications. 2016 is the highest multiple of 48 that is less than 2048.
- No DYNAMIC trunk members may be manually added, deleted, or changed in table TRKMEM, because table IPINV automatically datafills TRKMEM with blocks of 48 dynamic trunks.

***Note:*** Refer to Chapter 2: "TOPS-IP data and voice communication" for information on limiting the use of dynamic voice trunks.

### TOPSTOPT

The following limitations and restrictions apply to table TOPSTOPT and the MAXCONNS (maximum connections) function for dynamic trunk groups:

- A value of 0 in the MAXCONNS field specifies no connections allowed for that trunk group.
- The effective maximum for the MAXCONNS field is 2016 members. Datafilling MAXCONNS with a value of 2016 or greater has no effect.
- The switch does not invoke the MAXCONNS function when the value in MAXCONNS is 2016 or greater, or when the dynamic trunk group is not datafilled in table TOPSTOPT. So if the MAXCONNS function is not desired for a trunk group, the tuple for the trunk group should be deleted from table TOPSTOPT, or the MAXCONNS value should be set to 2016. This will avoid unnecessary CPU real-time consumption on each TOPS-IP call.

### ISUPDEST and C7TRKMEM

The following limitations and restrictions apply to tables ISUPDEST and C7TRKMEM:

- Dynamic trunk subgroups cannot be added to table ISUPDEST. Consequently, dynamic trunk members cannot be added to table C7TRKMEM.
- The DYNAMIC option cannot be assigned to a trunk that has existing ISUPDEST datafill.

## Dynamic trunk maintenance

The following limitations and restrictions apply to dynamic trunk maintenance:

- Many TTP level commands are not supported for dynamic trunks. For a complete list, refer to “Dynamic voice trunk maintenance” on page 317.
- ISUP group blocking and unblocking are not supported on dynamic trunks.

### 7X07AA Gateway cards

The following limitations and restrictions apply to 7X07AA Gateway cards:

- During an XPM cold SWACT, all 7X07 Gateway cards transition to a SYSB state; however, after the cold SWACT completes, the Gateways will transition automatically back to an in-service state.
- The 7X07 Gateway has two Ethernet ports, only one of which is active at any time. It monitors the Ethernet links on both its ports, and automatically switches to the other port when it detects a failure on the active port. A brief interruption of service occurs while it is switching interfaces.
- A TOPS Gateway card will not come into service if the IP address downloaded to it from table IPINV (IPZONE field) does not match the IP address assigned by the DHCP server.
- Taking a 7X07 Gateway card out of service affects active calls. The DRAIN option for the BSY command at the PM;IPGW MAP level provides a controlled method for taking a Gateway card out of service. DRAIN allows calls in progress on a Gateway to remain up until completion, while preventing future call originations.
- Telnet and PMDEBUG access must not be performed on an in-service 7X07 Gateway. If such access is needed, the Gateway should be removed from service using the BSY DRAIN command at the IPGW level at the MAP.
- All 48 trunks on a Gateway card are assigned to the same trunk group.
- Different Gateway cards must be used for (a) connecting to IP positions in standalone and OC host calls, (b) connecting to OC remotes in OC host calls, and (c) connecting to OC hosts and IP positions in OC remote calls.
- Although up to 10 7X07 Gateway cards can be installed in the IP-XPM frame, the IP-XPM’s C-side links and inter-mate links cannot support the messaging that the OC-IP and IP position applications would generate for 10 fully-occupied 7X07s unless average hold times at the operator position are a minute or longer. See Chapter 7: “TOPS-IP engineering guidelines,” for provisioning information on 7X07 Gateway cards.
- The 7X07 Gateway cards must be distributed evenly among all the IP-XPM shelves on the switch. They should be installed in adjacent slots starting from the left-most slot.

### Codecs

The following limitations and restrictions apply to voice codecs:

- Two voice codecs are available at call set up: G.711 (uncompressed) and G.723 (compressed).
- Voice quality may be perceptibly affected when the G.723 codec is used.
- Service providers whose operators enter DTMF to interact with automated systems, and who are considering using G.723, should verify that DTMS is properly received with G.723. (Lab testing at Nortel Networks did not reveal any problem.)

  ***Note:*** Codec selection does not affect call arrival tones.
- In releases earlier than TOPS19 (SN06), the switch interpretation of codec datafill in table PKTVPROF depends both on whether patch CFX84 is applied and on whether it is activated. Refer to "Table PKTVPROF prior to TOPS19" on page 70 for more information.

## IP-XPM limitations and restrictions

The following limitations and restrictions apply to the IP-XPM:

- No TDM applications are supported on an IP-XPM. The IP-XPM is an IP-only peripheral that cannot be configured with any non-IP line or trunk cards. The only interfaces supported on the P-side of the IP-XPM are SX05DA and 7X07AA.
- All TOPS-IP applications require that C-side 14 extended messaging be provisioned for the IP-XPM. Six pairs of extended messaging links must be provisioned.
- Each pair of C-side links added to an IP-XPM reduces by one the total number of XPMs that can be supported on the switch. Each pair of links requires a port on the 9X17 message switch port card.
- TOPS-IP does not support the IP-XPM software load that is normally delivered for use with some CM software releases. For more information, see Table 62, "Compatibility between TOPS releases and NCL loads for TOPS-IP," on page 287.
- During an XPM SWACT (including a warm SWACT), both TCP and UDP applications on the SX05DA may suffer a brief messaging interruption, and some calls may be dropped until the sockets are re-established.
- During an XPM cold SWACT, all 7X07 Gateway cards transition to a SYSB state; however, after the cold SWACT completes, the Gateways will transition automatically back to an in-service state.
- Until the 7X07 Gateway card has correct datafill in both table LTCPSINV and table IPINV, the IP-XPM will have inconsistent information about is packfill and so diagnostics may be affected. The switch also will generate PM777 logs (wrong P-side card).
- A separate, dedicated IP-XPM must be used for QMS MIS-IP data communication.

- The IP-XPM does not support existing TOPS applications that use the Ethernet Interface Unit (EIU), such as OSSAIN data links, OSAC data links, and TOPS devices.

***Note:*** See Chapter 7: "TOPS-IP engineering guidelines," for more IP-XPM limitations and restrictions.

## Managed IP network limitations and restrictions

The following limitations and restrictions apply to the managed IP network:

- The packet data network used for TOPS-IP applications must be engineered to meet specific requirements for bandwidth, quality of service, security, and reliability. These requirement are documented in Chapter 7: "TOPS-IP engineering guidelines."
- IP positions and their host switch must be on IP networks or subnetworks within the same IP address space. OC-IP host switches and remote switches must also be in the same IP address space. It is not possible to place IP positions, their host switch, or their OC-IP remote switch behind a server that performs network address translation.
- Routers connected to the same local IP network as the IP-XPM must support the Virtual Router Redundancy Protocol (VRRP) or an equivalent protocol.
- The router redundancy scheme must support ping.
- A brief interruption of service will occur when a router fails and its backup router takes on its traffic. A brief interruption will also occur when control is returned to the original master router.
- Network routers must support BOOTP/DHCP relay capability if DHCP servers are not provided on each LAN segment.
- Routers and other nodes connected to the same local IP network as the IP-XPM must support the gratuitous Address Resolution Protocol (ARP).

***Note:*** See Chapter 7: "TOPS-IP engineering guidelines," for more managed IP network limitations and restrictions.

## TOPS-IP product limitations and restrictions

The following limitations and restrictions apply to the TOPS-IP product in general:

- TOPS-IP applications are available in the following loads:
  - North American load: OC-IP, IP position
  - Non-North American load: IP position

- TOPS-IP does not change the voice or data connectivity for any TOPS application or interface other than OC voice and data links, IWS position voice and data links, and TOPS QMS MIS-IP data links. For example, it does not change the data connectivity between the DMS switch and D1 data bases, LIDB databases, PARS nodes, OSSAIN service nodes, or the ISN-DA audio server.
- TOPS-IP does not change the following existing capacity limitations of TOPS switches:
  - A maximum of 1023 operator positions can be datafilled in a switch.
  - A maximum of 1364 conference three-port circuits (CF3P) can be provisioned on a switch. (A CF3P is required for each standalone or OC remote call with an operator.)
- The maximum distance between TOPS-IP nodes such as OC remote switches, OC host switches, and IP positions is constrained by latency and echo issues. There is no limit on the distance for TOPS-IP data transmission; this is configurable through standard IP practices. For a discussion of latency issues, refer to Chapter 7: "TOPS-IP engineering guidelines."
- TOPS-IP voice links do not use the SS7 network.

## OC-IP application limitations and restrictions

This section discusses limitations and restrictions for the OC-IP application, as follows:

- provisioning data and voice for OC-IP
- mixing OC-IP with traditional OC

### Provisioning data and voice for OC-IP

The following limitations and restrictions apply to provisioning data and voice for OC-IP:

- Both the OC-IP remote and OC-IP host must be upgraded to TOPS15 or higher before OC-IP calls can take place.
- The existing three-BCS rule applies: All TOPS switches and OPP positions in the OC network must be within three BCS levels of all other TOPS switches and OPP positions in the network.
- OC-IP is not available in non-North American loads.
- A maximum of 30 tuples can be datafilled in table OCOFC when HRNQT is used, or 31 tuples when it is not used.
- Since AMA records do not identify the host switch of the call, duplicate operator numbers in an OC network (across multiple hosts) should be avoided if there is a need to identify the operator.

- At most eight OC-IP data links can be datafilled for each distant office. The maximum number of OC-IP data links that can be datafilled on any switch is 248 (or 240 if HRNQT is used).
- The maximum number of OC-IP voice links depends on the call processing capacity of the IP-XPM. For details, refer to Chapter 7: "TOPS-IP engineering guidelines."
- OC remotes do not throttle requests for operators based on the number of available voice links. (However, OC-IP supports standard QMS deflection and overflow processing. Also, throttling based on virtual circuits is activated when a remote has 2048 calls queued or at position in a single host office.) For information on failure handling, refer to Chapter 3: "TOPS OC-IP application."
- As with traditional OC, trunks that are datafilled for use as OC voice links must not be used for normal call processing. If an attempt is made to use them for normal call processing, operator services will be disrupted and calls may be lost.

### Mixing OC-IP with traditional OC

OC-IP and traditional DCM or ETMS OC can no longer coexist in the same switch. TDM-OC links must be replaced by OC-IP links prior to an upgrade to SN08 or higher. Any OCHOST or OCHOSTQ tuple which references a TDM-OC link will cause a TABXFR to halt if not replaced prior to such an upgrade.

The following limitations exists:

- A position using an ETMS for data connectivity to a host will not be able to RTS or login.
- A remote using an ETMS for data connectivity to a host will not be able to send calls to that host.
- A host using an ETMS for data connectivity to a remote will stop receiving calls from that remote.

## IP position application limitations and restrictions

This section discusses limitations and restrictions for the IP position application, as follows:

- provisioning data and voice for IP positions
- IP position maintenance
- call processing
- supervisory functions
- force managements statistics

### Provisioning data and voice for IP positions

The following limitations and restrictions apply to provisioning data and voice for IP positions:

- A standalone or OC host switch must be upgraded to TOPS17 or higher before it can host IP positions.
- An OC remote switch must be upgraded to TOPS15 or higher before it can process calls served by IP positions in the host. This is true regardless of whether the OC remote uses OC-IP or TDM OC.
- It is recommended that all switches in the OC network be upgraded to TOPS15 or higher before operators who serve OC calls log into IP positions. Alternatively, new QMS call queues may be set up for operators who log into IP positions. If this approach is taken, remotes that have not yet upgraded to TOPS15 must not be datafilled to route calls to the new call queues.
- OPP positions (IP and TDM) and OC switches (IP and TDM) in the network must follow the existing three-BCS rule: All TOPS switches and OPP positions in the OC network must be within three BCS levels of all other TOPS switches and OPP positions in the network.
- IP position connectivity is supported only for Nortel Networks Intelligent Workstation System (IWS) positions. Third-party OPP-compatible operator positions continue to be supported, but only with TDM connectivity to the switch.
  ***Note***: The PC used for the IP position must be equipped with a PS/2 keyboard connection is using the custom IWS keyboard. A PS/2 to USB converter will not work.
- Positions with IP data connectivity must also have IP voice connectivity, and vice versa.
- At most eight COMIDs on each IP-XPM can by used for IP positions. For more information, see “Overview of datafill for IP position data links” on page 122.
- The maximum number of IP positions that can be supported on an IP-XPM depends on call characteristics and processing capacity of the IP-XPM. For details, refer to Chapter 7: “TOPS-IP engineering guidelines.”
- OC remote switches cannot route IP voice traffic through the OC host to forward to the IP position. Host voice bypass is always used when the OC links and position links are IP.
- Interfaces used by some third-party vendor applications to communicate with TDM-based positions are not compatible with IP positions. These include PARS and OIA (Open Interface Access) databases. Contact your vendor for information about plans to provide an interface for IP positions.
- There is no plan to upgrade the Nortel Networks Reference System to interwork with IP positions.

- IP positions cannot be datafilled as Service Assistance (SA) or In-Charge (IC).
- The following limitations exists:
  - A position using an ETMS for data connectivity to a host will not be able to RTS or login.
  - A remote using an ETMS for data connectivity to a host will not be able to send calls to that host.
  - A host using an ETMS for data connectivity to a remote will stop receiving calls from that remote.
  - TDM OC links must be replaced by OC-IP links.

### IP position maintenance

The following limitations and restrictions apply to maintenance of IP positions:

- If data connectivity between the switch and an IP position is lost because of a network outage, the position transitions to the CRES state at the MAP (on the next attempt to present a call to the position), rather than to SYSB. For more information, refer to "Maintenance states and transitions" on page 342 and "Failure handling" on page 151.

  The IWS itself does detect the link problem, and its display announces the problem. It may take several minutes before the IWS detects the problem and removes itself from service. It automatically returns to service when the network outage is corrected.
- If data connectivity between the switch and an IP position is lost because the position is improperly shut down, the position transitions to the CRES state rather than to SYSB. Refer to *TOPS IWS Base Platform User's Guide* for the procedure for shutting down the base application in a way that ensures the position will be able to notify the switch.
- A status mismatch can occur during a maintenance SWACT or ONP if an IP position initiates a state change between an in-service and an out-of-service state during a critical window of the maintenance activity. The mismatch can be corrected by off-lining the position until the maintenance activity is over.

### Call processing

The following limitations and restrictions apply to IP position call processing:

- IP position generate their own call arrival tones. This is unlike TDM positions, at which call arrival tones are generated by DMS XPMs. In countries where the call arrival tones generated by XPMs use a non-North American toneset, the tones generated by the IWS may sound somewhat different.

- When a call is placed on hold, the IP voice connection for the call is disconnected. A new voice connection is established when the call is reaccessed. Additional delay is incurred in re-establishing the IP voice connections, and it is possible for the re-establishment to fail.

### Supervisory functions

The following limitations and restrictions apply to monitoring and assistance requests:

- Monitoring between IP positions and TDM positions is not supported.
- If a monitoring session is initiated while the monitored position has a call, the monitor does not hear voice until the next new call arrives at the monitored position.
- The monitor does not hear the monitored operator when the operator does not have an active call.
- Other monitoring restrictions that apply to TDM positions also apply to IP positions. Refer to “Position monitoring” on page 148 for more information.
- Operators at IP positions cannot receive assistance from SA/IC positions. Only QMS CASE assistance is supported for IP positions. (The QMS CASE assistant, or CSE, may be at either an IP position or a TDM position.)

### Force management statistics

The following limitations and restrictions apply to FM statistics:

- Due to the processing overhead associated with establishing and clearing IP voice connections with operator positions, operator idle time (IDLT) will increase. Any statistics that are derived from IDLT will also be affected. An example is percent occupancy (%OCC), which will decrease.
- The switch continues to accumulate work volume for operators who simply disconnect the headset while the position is in a state to accept calls.
- UCP (unoccupied with call at position) and UCD (unoccupied with disconnected call) warnings are not available for IP positions, since these positions do not inform the DMS switch of the headset status.

## QMS MIS-IP application limitations and restrictions

The following limitations and restrictions apply to the QMS MIS-IP application:

- QMS MIS-IP is not supported. Customers with an interest in the application should discuss this with their MIS vendor and with TOPS Marketing.

- QMS MIS-IP requires a dedicated IP-XPM. (This IP-XPM need not contain 7X07 Gateway cards.) For details on engineering, refer to Chapter 6: “TOPS-IP engineering guidelines.”
- Only one QMS MIS-IP data link should be provisioned on an IP-XPM due to the bursty nature of QMS MIS traffic.
- QMS MIS-IP can only be implemented on TOPS OC hosts or TOPS standalone switches. MIS-IP is not available on pure TOPS OC remotes.
- To minimize TCP re-establishment delays, it is recommended that table IPSVCS be datafilled with a PORT value of 0 for the QMS MIS-IP service tuple. A value of 0 is used to request the XPM to randomly assign a port number.
- Only one type of TOPS QMS MIS interface—IP or X.25—can be active in an office at a time.
- When the IP interface is datafilled in table QMSMIS, it must have datafill for at least one IP connection (up to two).
- When a change of interface is made from X.25 to IP and vice versa, any messages that have not been sent out on the MPC link or the IP connection may be lost. It is recommended that users perform any interface change during periods of low traffic.
- The following changes to the IP interface in table QMSMIS are allowed only when the destination status (DESSTAT) is set to INACTIVE:
  - changing the value of DATALINK from IP to MPC
  - deleting the TOPS tuple
- When the DESSTAT field is changed from ACTIVE to INACTIVE, any messages that have not be sent out on the IP connection may be lost.
- As with the X.25 QMS MIS interface, MIS buffers in the switch that get full and cannot be transmitted to the off-board MIS server using the IP interface are discarded.

***Note:*** Refer to Chapter 8: “TOPS-IP data schema,” for details on datafill.

## SNMP limitations and restrictions

### SNMP and 7X07AA

The following limitations and restrictions apply to the use of SNMP on the 7X07AA Gateway:

- As of SN09,“public” is no longer the only supported SNMP community name. This value is datafillable and validated for incoming read and write messages. The datafilled community name is also sent in trap messages.
- As of SN09, three new SNMP settings include: SNMP community name, SNMP manager, and SNMP enable/disable. These settings only apply to TOPS 7X07AAs as datafilled in Table IPINV (field GW_TYPE is set to TOPS) and are added as individual office parameters in Table OFCENG.

The craftsperson must perform a PMRESET on each 7X07AA to download the SNMP settings.

- The 7X07AA supports SNMPv1 and SNMPv2c only. The 7X07AA does not support SNMPv2 or SNMPv3.
- If the Gateway goes system busy due to a Gateway self-reboot that is initiated from low-level Gateway software (Board Support Package), an SNMP GW_BUSY trap notification is not sent to the SNMP management node or nodes.
- The Gateway has some user-configured data that is maintained through SNMP and Telnet access to the Gateway, including writable variables in SNMP MIBs, configurable SNMP security settings, and the Gateway password. Some of this data may need to be reconfigured after a DMS PMRESET, a Gateway reboot, and reseating or replacing the 7X07 Gateway circuit pack. For details, refer to Appendix B: "TOPS-IP support for SNMP."
- Telnet and PMDEBUG access *must not* be performed on an in-service 7X07 Gateway. If such access is needed, the Gateway should be removed from service using the BSY DRAIN command at the IPGW level at the MAP.

### SNMP and SX05DA

The following limitations and restrictions apply to the use of SNMP on the SX05DA Gateway:

- The SX05DA does not support SNMP GetBulk operations.
- The SX05DA does not send SNMP traps.
- The SX05DA does not validate the SNMP manager IP address or set requirements.
- The SSX05DA only allows set requests on MIB-II objects in the system group.
- The SX05DA SNMP objects are not reset following a reload or BSY/RTS of the XPM.

# Part 4: Planning and engineering

Part 4: Planning and engineering includes the following chapter:

# Chapter 7: TOPS-IP engineering guidelines

This chapter provides guidelines for engineering TOPS-IP, focusing on the following areas:

- Network overview
- Data and voice transport in the IP-XPM
- C-side links to the IP-XPM
- IP-XPM provisioning
- MIS-IP requirements
- Switch hardware resources
- TOPS-IP data network requirements

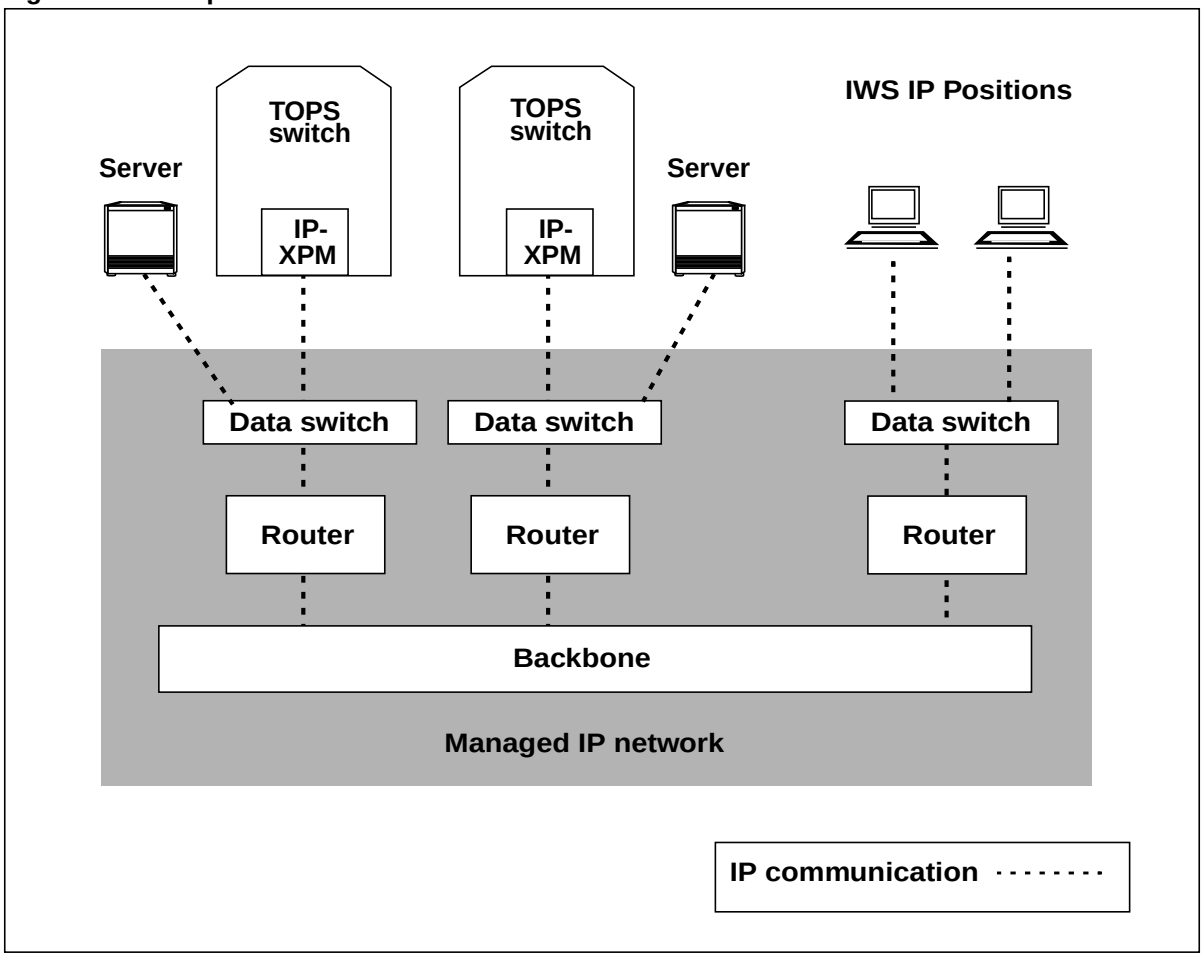
## Network overview

DMS TOPS switches interact with a wide variety of other nodes, including other TOPS switches (Operator Centralization), operator positions (such as Intelligent Workstations), DA audio nodes (such as NAV), DA databases (such as Directory One), and other databases (such as LIDB and QMS MIS). These nodes have traditionally been connected using dedicated, point-to-point data and voice connections. Adding or modifying nodes in this environment is a complex process.

The TOPS-IP product introduces a managed, unified IP voice and data network to interconnect the TOPS switches and off-switch nodes. Each switch and node is physically connected to a network of Ethernet switches, routers, and transport facilities. The managed IP network allows flexible assignment of logical paths as needed, rather than requiring separate dedicated voice and data facilities to be installed for each application. The network must be managed to ensure quality of service for the desired level of traffic.

The following figure shows a simple functional view of a TOPS-IP network configuration.

**Figure 108 Simple TOPS-IP network**




## Data and voice transport in the IP-XPM

The TOPS switch uses the IP-XPM to connect to the managed IP network. The IP-XPM is a specialized DTC configured with SX05DA processors, 7X07AA Gateway cards, MX76DA messaging cards, and a special software load to provide the following IP infrastructure:

- voice gateways between the DMS circuit-switched network and the IP network
- call control and other data messages between the TOPS software in the CM/Call Server and nodes on the TOPS-IP network

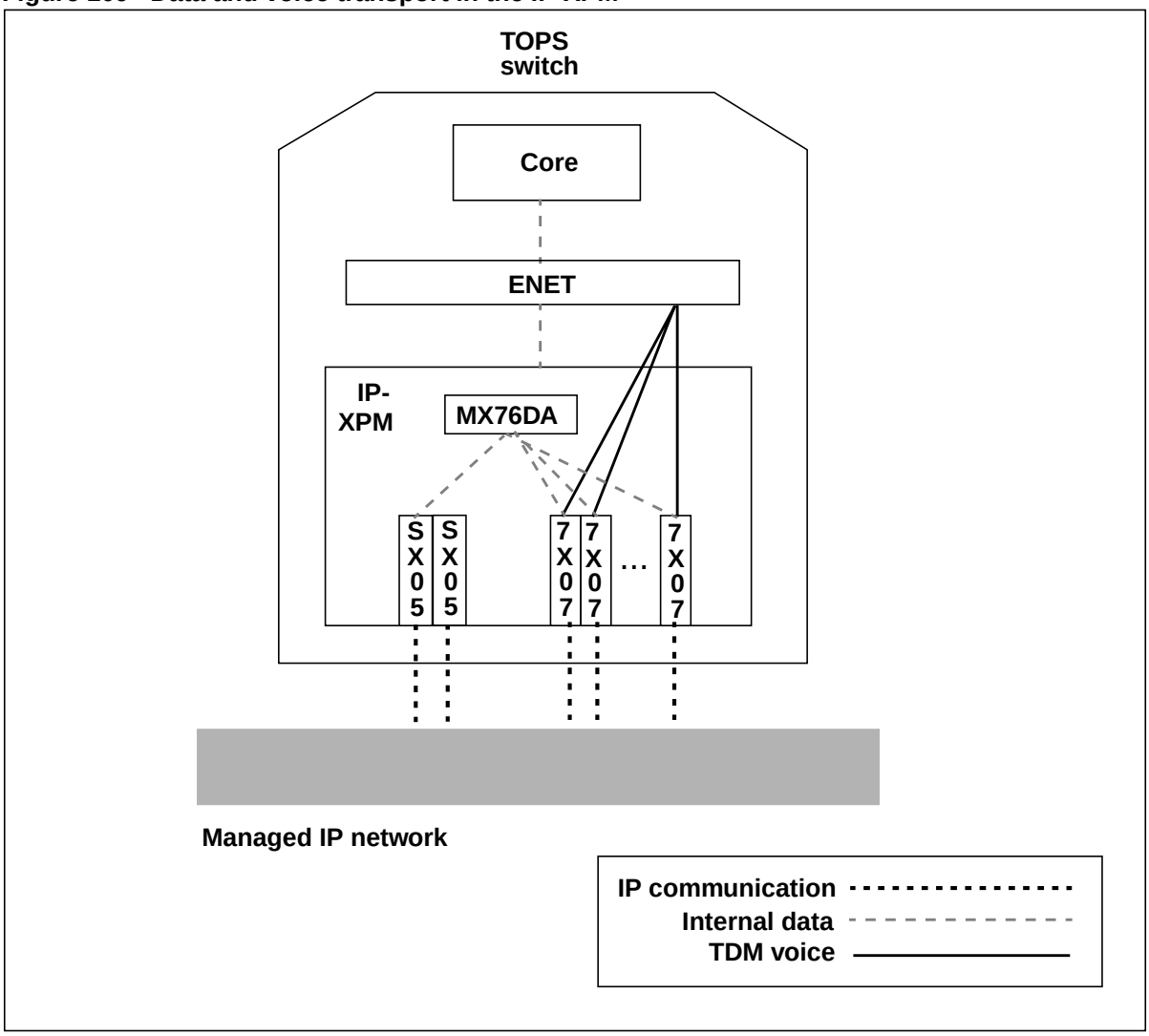
The 7X07 Gateway card can be viewed as the first element at the edge of the managed IP network even though it is physically located in the IP-XPM. The 7X07 receives software and IP network datafill from a DHCP network server on the IP network.

***Note:*** The SX05DA and 7X07AA cards require a new backplane version, so many existing peripherals cannot be upgraded in the field. For details refer to “Switch hardware resources” on page 201.

After a TOPS switch or other node is attached to the managed IP network, it can establish voice or data connections to any other switch or node on the network. Bandwidth for all TOPS-IP services uses a common IP/ATM network. As long as capacity remains on a given IP-XPM, additional traffic can be added.

Figure 109 provides an overview of the way the SX05DA, MX76DA, and 7X07AA are used to route data and voice through the IP-XPM.

**Figure 109 Data and voice transport in the IP-XPM**




***Note:*** Although an IP-XPM has two SX05DA cards as shown in Figure 109, only one is active at any time.

The SX05DA card transports data protocols between the DMS core and the IP network on its Ethernet port. The 7X07 card converts between TDM voice and IP packets and converts between internal signaling and SIP messages on the IP network. The MX76DA message and tone set card supports messaging from the SX05DA to the core and to the 7X07 Gateway cards.

## C-side links to the IP-XPM

The following provisioning rules apply to the IP-XPM's C-side links, which transfer data between the DMS core and the IP-XPM:

- TOPS-IP can be implemented only on switches provisioned with an ENET (enhanced network), and not on switches provisioned with JNET (junctored network) or on Succession Call Servers without ENET.
- Enhanced C-side messaging (SOC TEL00011) is required.
- 14 C-side links (6 pairs of extended messaging links) must be provisioned on each IP-XPM.
- C-side extended messaging requires fiber peripheral links.
- The ENET 9X17 chain cards must have a sufficient number of peripheral links available to provision the necessary number of C-side links to each IP-XPM.

  ***Note:*** Each pair of C-side links provisioned for the IP-XPM reduces by one the total number of XPMs that can be supported on the switch. Each C-side pair requires a port on the 9X17 chain card. A single IP-XPM with 14 C-side links occupies as many chain card ports as 7 XPMs (DTC or LGC, for example) which do not use extended C-side messaging.

  If an insufficient number of ENET ports are available, the 9X17 chain cards can be reconfigured for increased port capacity (up to 256 ports), or other ENET peripheral links must be eliminated.

Extended C-side messaging links are provisioned in table LTCINV. This is normally done by the CONVERTCSLINKS utility. For more information refer to "CONVERTCSLINKS" on page 427.

For details on IP-XPM hardware, refer to "Switch hardware resources" on page 201.

## IP-XPM provisioning

Two TOPS-IP applications use the IP infrastructure provided by the IP-XPM:

- Operator Centralization (OC-IP), described in Chapter 3: "TOPS OC-IP application," is available starting in TOPS15.
- IP positions, described in Chapter 4: "TOPS IP position application," are supported on TOPS hosts and standalone switches and Call Servers starting in TOPS17 (SN04). IP positions in an OC host can interwork with OC remotes that are at TOPS15 or higher.

This section provides provisioning rules for offices using IP-XPMs to support either or both of these applications. IP-XPM provisioning for a switch or Call Server entails first determining the number of 7X07 Gateway cards needed and then determining the number of IP-XPMs needed. The Gateway cards should be evenly distributed across the IP-XPMs. The data links for both applications should also be evenly distributed.

***Note:*** The QMS MIS-IP application has not been released as a Generally Available product, and this section does not include IP-XPM provisioning rules for QMS MIS-IP. See “MIS-IP requirements” on page 201 for more information.

## Determining the number of 7X07 Gateways

This section includes an introduction to 7X07 Gateway provisioning, an explanation of the provisioning methodology, and details for determining the number of 7X07s to support each of three TOPS-IP trunk groups that may be required in a particular switch.

### Introduction

The following considerations apply to provisioning of 7X07 Gateway cards.

- Voice links (TOPS-IP dynamic trunk members) are added in multiples of 48.
- OC-IP calls that are served by IP positions in the host do not use voice resources in the host. The voice connection for these calls is directly between the OC-IP remote and the IP position. Refer to page 79 in Chapter 3: “TOPS OC-IP application” for more information about host voice bypass.
- Different trunk groups are used for VoIP connections to hosted IP positions, to OC remotes, and to OC hosts and their IP positions. Depending on the configuration of a switch that supports TOPS-IP, the switch will require from one to three TOPS-IP trunk groups.
    - A switch that hosts IP positions requires one trunk group for VoIP connections to the positions. This trunk group is datafilled against the positions in table TOPSPOS. Most examples in this book use the name POSIPVL for this trunk group.

      ***Note:*** Although this trunk group is not used for OC-IP calls that use IP positions, the trunk group is still needed in a pure OC-IP host. This is explained in “Number of 7X07s for VoIP connections to hosted IP positions” on page 190.
    - An OC-IP host switch that has TDM positions requires a trunk group for VoIP connections to OC remote switches. This trunk group is datafilled against the remotes in table OCGRP. Most examples in this book use the name OCIPTOREMOTE for this trunk group.
    - An OC-IP remote switch requires a trunk group for connections to OC host switches or, if the host has IP positions, for connections directly to those positions. This trunk group is datafilled against the hosts in table OCGRP. Most examples in this book use the name OCIPTOHOST for this trunk group.

      ***Note:*** An OC-IP remote uses the *same* trunk group for VoIP connections to Gateways in the host (used when the host allocates a TDM position for an OC-IP call) and for connections to the OC

host's IP positions (host voice bypass, used when the host allocates an IP position for an OC-IP call).

- All 48 trunks associated with a Gateway card are added to the same trunk group.
- A single trunk group can use multiple Gateway cards on the same or different IP-XPMs.
- Different Gateway cards on the same IP-XPM can be assigned to different trunk groups.
- Redundancy in Gateway provisioning is achieved by provisioning (at least) one extra 7X07 card for each trunk group. The extra card functions as a hot spare. It enables call processing to continue without incident if one 7X07 associated with the trunk group has hardware problems, needs to be reloaded, or otherwise becomes unavailable.
- It is recommended that all voice links for hosted IP positions be assigned to a single trunk group regardless of where the positions are physically located. This minimizes 7X07 redundancy requirements.
- For the same reason, it is recommended that an OC host use only a single trunk group for VoIP connections to all of its remotes, and that an OC remote use only a single trunk group for VoIP connections to all of its hosts and their IP positions.

***Note:*** The IP-XPM does not support TDM speech cards, such as the 6X50.

7X07 Gateway cards are provisioned separately for each of the three TOPS-IP trunk groups that may be needed at the switch. The total number of 7X07s is the sum of those needed for each of the trunk groups.

### Provisioning methodology

This book assumes familiarly with basic concepts and terminology of telephony provisioning. Readers needing additional background may consult NTP 297-1001-304, "DMS100 Family Capacity Administration Guide."

7X07 provisioning uses the standard Erlang B (loss) formula or tables derived from that formula. Because of the way calls "bunch up," it is evident that a probabilistic model is needed for provisioning OC voice links in an OC remote switch. It may be less obvious that a probabilistic model is needed in a standalone or OC host switch; it may seem at first that provisioning one voice link per position would be sufficient. This does not work because the voice link holding time for a call is longer than the time that the operator is on the call. First, some of the signaling on the link occurs before the position is attached to the call, and second, the voice link is placed in a guard queue for a short time after it has been released from the position. Statistical variation occurs in the number of voice links in the guard queue, just as it occurs in the rate at which calls arrive.

ITU document “Extract from the Table of the Erlang Loss Formula,” downloadable from http://www.itu.int/itudoc/itu-d/dept/psp/ssb/planitu/plandoc/erlangt.html, provides Erlang B tables for loss probabilities as low as 0.00001 and number of devices (TOPS-IP dynamic trunks, or voice links) a little beyond the equivalent of six 7X07s. At the point where the table stops, the curves have pretty much leveled off. This implies that, for example, the capacity gain from adding a seventh or eighth 7X07 card is about the same as the capacity gain from adding the last group of 48 devices shown in the table.

Any equivalent table or Erlang B calculator may be used. However, the traffic calculators that are free for public use on the web are not generally recommended; some are inaccurate, and most support neither low blocking probabilities nor high numbers of resources. The table from the ITU is used in the example in this section.

Two pieces of information are needed to use an Erlang loss table to provision 7X07s: the desired loss (blocking) probability and the relevant traffic level in Erlangs.

- Loss probability

  Although the Erlang loss formula is the best tool for provisioning 7X07s, the specified blocking probability may not correspond closely to the actual observed frequency of failure to get a voice link. Some of the reasons for the discrepancies are understood. For example, the formula assumes that blocked calls are removed from the system, but TOPS re-queues blocked calls. (The standard Erlang queuing model is not applicable here, because TOPS re-queues for an *operator*, not for a voice link; it assumes a voice link will be available when an operator is.) If this re-queuing occurs frequently, the effective traffic level is raised beyond the level specified as input to the model.

  This chapter recommends different loss probabilities to use for different trunk groups and office configurations. The recommended probabilities take into account various factors that make the model a less than perfect fit. They are intended to ensure that resources are not wasted, but at the same time to ensure that failures to obtain a voice link are rare. Note that TOPS places a position in the make busy state whenever it fails to get a voice link.

- Relevant traffic level in Erlangs

  Relevant traffic is traffic that uses a member of the trunk group being provisioned. Which traffic is relevant for a particular trunk group depends on the trunk group and the office configuration. Identification of relevant traffic is addressed in the later sections that are specific to each trunk group.

This section assumes that the relevant traffic has been identified and its volume is known in calls/hour. This section also assumes that the operator average work time (AWT) for each service is known. All of this information can be computed from OMs and Force Management (FM) statistics in existing offices. New installations must estimate the numbers.

***Note:*** It is recommended that either high data busy hour (HDBH) or at least average busy season busy hour (ABSBH) traffic levels be used in provisioning 7X07s.

The steps in using the Erlang loss table to determine the number of 7X07s to provision for a TOPS-IP trunk group are outlined below.

1 For each service with a distinct AWT, determine the level of relevant traffic in calls/hour.

As noted above, later sections provide specific information about identifying relevant calls for each trunk group. The following traffic levels and AWTs are used as examples in this section:

| Service | Relevant traffic (calls per hour) | AWT (secs) |
|---|---|---|
| TA | 580 | 33.0 |
| DA | 6820 | 24.5 |
| NDA | 1790 | 34.8 |
| Intercept | 430 | 16.0 |

2 For each service, estimate the per-call voice link holding time by adding 1.5 seconds to the AWT.

Voice link holding time is longer than AWT for two reasons. First, a voice link is not made immediately available when it is released from a call. Instead, it is placed in a guard queue for between 0.75 and 1 second, during which time it is unavailable for use. Second, voice link holding time includes time for signaling on the link, and this time is not included in operator AWT.

The per-call voice link holding time values for our example are shown in the last column below.

| Service | Relevant traffic (calls per hour) | AWT (secs) | Per-call VL hold time (secs) |
|---|---|---|---|
| TA | 580 | 33.0 | 34.5 |
| DA | 6820 | 24.5 | 26.0 |
| NDA | 1790 | 34.8 | 36.3 |
| Intercept | 430 | 16.0 | 17.5 |

3 Compute the total hourly traffic in call-seconds by multiplying the traffic level (in calls/hour) for each service by the corresponding voice link holding time, and adding the products.

In our example, the total hourly traffic in call-seconds is
(580 x 34.5) + (6820 x 26.0) + (1790 x 36.3) + (430 x 17.5) = 269,832.

4 Convert from hourly call-seconds to Erlangs by dividing by 3600.

In our example, 269,832 / 3600 = 74.95.

5 Consult the Erlang loss table using the desired loss probability and the number of Erlangs of traffic on the voice links.

As noted earlier, different loss probabilities are recommended in later sections for different trunk groups and office configurations.

In our example, we look in Table A of the referenced ITU document under the 0.0001 column for the first entry at least as large as 74.95. The table tells us **n**, the number of devices needed for that traffic level and loss probability. In our example, **n** is 107. This is the number of voice links that are needed for call processing in the trunk group being provisioned.

6 Divide the number of voice links by 48 and round up, to determine the number of 7X07s needed for call processing.

In our example,
107 / 48 = 2.2; round up to 3.

7 Add one 7X07 for redundancy for this trunk group.

In our example,
3 + 1 = 4.

Again, if the offered voice link traffic for the trunk group is more Erlangs than the table shows, the incremental capacity gain from adding each 7X07 beyond the sixth can safely be considered to be equal to the incremental gain from adding the last 48 devices shown in the table. For convenience, the following table shows the predicted incremental gain (in voice link Erlangs of offered traffic) from adding each 7X07 beyond the sixth, at several loss probabilities.

**Table 2 Predicted gain in voice link Erlang capacity for each 7X07 beyond six**

| Loss probability | Predicted Erlang gain per 7X07 beyond six |
|---|---|
| 0.00001 | 42.62 |
| 0.00005 | 43.28 |
| 0.0001 | 43.60 |
| 0.0005 | 44.45 |
| 0.001 | 44.87 |
| 0.005 | 46.13 |

The following three sections are specific to the three trunk groups that may be needed in a TOPS-IP office.

## Number of 7X07s for VoIP connections to hosted IP positions

This section applies to all switches that host IP positions, regardless of whether the positions are used for standalone calls, TDM-OC calls, or OC-IP calls. The trunks group associated with the 7X07s provisioned in this section is datafilled against the positions in table TOPSPOS.

***Note:*** TDM OC links must be replaced by OC-IP links.

This section considers three configurations: (a) pure OC-IP host with all IP positions, (b) all IP positions and no OC-IP, and (c) all other configurations where the switch hosts IP positions.

- **Pure OC-IP host with all IP positions**

  In a pure OC-IP host with all IP positions, TOPS calls do not normally use voice resources in the host. However, the host must provision enough 7X07s for this trunk group to support certain calltypes that are typically low-runner.

  These calltypes include all "calls," internal or external, in which the operator keys to access an idle loop. For example, operators may access an idle loop to make a directed assistance request, to respond to a page, to retrieve a call from an external booked call database system, or perhaps to connect to the business office or to a customer who wanted to be called back. In many offices, the number of these operator-originated calls is so low that it can almost be disregarded. But in a pure OC-IP host with all IP positions, operator-originated calls must be considered so that some voice resources will be provisioned for them in the host.

  Estimate the maximum number of operators who may be simultaneously involved in the operator-originated calltypes described above. If the number is very small, just provision one 7X07 plus a spare for the trunk group. Otherwise, if it is possible to estimate traffic level and AWT for these calltypes, the method described in "Provisioning methodology" on page 186 may be used. No recommendation is made for the loss probability to use for these calls.

- **All IP positions and no OC-IP**

  This is a TOPS switch that hosts all IP positions (no TDM positions) and does not use OC-IP. The switch may process standalone calls, TDM-OC calls, or both.

  The recommended loss probability to use in the Erlang loss table for this configuration is 0.001. Although 0.001 suggests that about one call in 1000 will fail to get a voice link, the actual observed failures rate is not expected to be that high in this configuration. The reason is related to the less-than-perfect fit of the Erlang B model to this configuration.

  When calculating relevant traffic, include all calls that are presented to the positions. (Each recall and transfer position seizure counts as a separate call.)

- **All other configurations where the switch hosts IP positions**

  This includes offices that have IP positions and function both as OC-IP host and as TDM-OC host or standalone, and offices that have both TDM and IP positions.

  The recommended loss probability to use in the Erlang loss table for these configurations is 0.0001 or lower.

  When calculating relevant traffic, include all calls that *do* use IP positions and *do not* use OC-IP. Following are examples of determining relevant calltypes.

  ***Example* 1** Suppose the switch functions as standalone, TDM-OC host, and OC-IP host, and suppose all positions are IP. Then count all of the standalone and TDM-OC calls for each service, and count none of the OC-IP calls.

  ***Example* 2** Suppose all the calls for a particular service are either standalone or TDM-OC, and suppose that half the positions providing the service at any time will be IP positions. Then count half of the total traffic for the service.

  ***Example* 3** Suppose that for a particular service, a standalone/host switch handles 25% standalone calls, 15% TDM-OC calls, and 60% OC-IP calls. Suppose that at any time 80% of the positions providing the service will be IP positions, and 20% will be TDM positions. Then for this service, estimate the traffic that uses IP positions but not OC-IP as

  %IP-pos x (%standalone + %TDM-OC) x (total traffic for service), or

  0.80 x (0.25 + 0.15) x (total traffic for service).

### Number of 7X07s for VoIP connections to OC-IP remotes

This section applies to OC-IP host switches that have some or all TDM positions. The trunk group associated with the 7X07s provisioned in this section is datafilled against OC-IP remote offices in table OCGRP. (In an OC-IP host with *all* IP positions, this trunk group is not needed.)

***Note:*** TDM OC links must be replaced by OC-IP links.

This section considers two cases: (a) pure OC-IP host with all TDM positions, and (b) OC-IP host with some standalone or TDM-OC calls, mixture of TDM and IP positions, or both.

- **Pure OC-IP host with all TDM positions**

  This is an OC-IP host that processes no standalone calls. Also, it has no IP positions.

The recommended loss probability to use in the Erlang loss table for this configuration is 0.001. Although 0.001 suggests that about one call in 1000 will fail to get a voice link, the actual observed failures rate is not expected to be that high in this configuration. The reason is related to the less-than-perfect fit of the Erlang B model to this configuration.

When calculating relevant traffic, include all call that are presented to the positions. (Each recall and transfer position seizure counts as a separate call.)

- **OC-IP host with some standalone or TDM-OC calls, mixture of TDM and IP positions, or both**

  ***Note:*** TDM OC links must be replaced by OC-IP links.

  The recommended loss probability to use in the Erlang loss table for this configuration is 0.0001 or lower.

  When calculating relevant traffic for each service, include only calls from OC-IP remotes. Do not count standalone calls or TDM-OC calls. If the host has some IP positions, first determine the maximum percentage of logged-on positions providing that service that will be TDM. Then count only that percentage of the traffic from OC-IP remotes.

  ***Example*** Suppose a combined standalone/host switch functions as an OC-IP host for some of its remotes and as a TDM-OC host for other remotes. Suppose this switch hosts both TDM and IP positions, and at any time, at most 40% of the positions handling DA calls will be TDM. Then calculate relevant DA traffic as 40% of the DA traffic volume that is routed to this host from its OC-IP remotes.

### Number of 7X07s for VoIP connections to OC-IP hosts and their IP positions

This section applies to any switch that functions as an OC-IP remote. It applies regardless of whether the OC-IP hosts that serve this remote provide IP positions or TDM positions. The trunks group associated with the 7X07s provisioned in this section is datafilled against OC-IP host offices in table OCGRP.

The recommended loss probability to use in the Erlang loss table for this configuration is 0.0001 or lower.

When calculating relevant traffic for each service, include all calls in which the remote obtains an operator from any of its OC-IP hosts.

## Determining the number of IP-XPMs

This section explains how to determine the number of IP-XPMs needed in an office that supports OC-IP, IP positions, or both.

Physically, an IP-XPM can accommodate at most 10 7X07 Gateway cards. From a traffic perspective, an IP-XPM can safely handle at most 40,000 calls/hour if it is processing both voice and data for the calls, and 50,000 calls/hour if it is processing only data. “Data” refers here to OPP messages, by which the switch and position exchange information, and OC messages, by which an OC remote and host exchange information.

The data-only calls in TOPS-IP are the OC host calls that also use OC-IP. Recall that these calls all use host voice bypass. Although these calls do not use voice resources in the host, each of them must be counted as two calls in the host from a messaging traffic perspective. This is because each of these calls needs IP-XPM capacity for data messaging with both the OC remote and the position. Bypass calls in the host are the only currently-supported calls that have this attribute.

At a high level, the steps for determining the number of IP-XPMs needed at each switch are as follows. Steps 2 and 3 use the term *logical IP-XPM*. This specifies an amount of IP-XPM traffic-processing capacity. For example, 1.5 logical IP-XPMs refers to one and a half times the traffic-processing capacity of a single IP-XPM.

1 Determine the number of 7X07 Gateways needed.

   This step was described in “Determining the number of 7X07 Gateways” beginning on page 185.

2 From a traffic perspective, determine the number of logical IP-XPMs needed for calls that use only data resources at the switch.

   This step is described in “IP-XPM requirement for data-only calls” on page 194.

3 From a traffic perspective, determine the number of logical IP-XPMs needed for calls that use both voice and data resources at the switch.

   This step is described in “IP-XPM requirement for voice-and-data calls” on page 195.

4 Determine the total number of IP-XPMs needed for the office, taking into account the physical limitations, traffic capacity limitations, and other factors such as load balancing.

   This step is described in “Total number of IP-XPMs” on page 197.

High day busy hour (HDBH) traffic is used in provisioning IP-XPMs because incoming calls are not rejected when a messaging overload occurs. If the IP-XPM's capacity is exceeded, lost messages can affect calls in progress as well as new originations, and problems can occur if the XPM switches activity (SWACT). Also, performance degrades when the IP-XPM is trying to handle too much traffic.

New installations must estimate the maximum traffic levels. Existing offices can obtain traffic levels from OMs and FM statistics. If numbers are not available for HDBH traffic, it is necessary to estimate the percentage increase to apply.

When considering OC-IP calls, include calls in which the remote requests an operator from the host even if the call is deflected or abandoned before getting one. These unsuccessful calls do use IP-XPM messaging capacity.

### IP-XPM requirement for data-only calls

This section applies only to switches that function as OC-IP hosts *and* support IP positions. If either of those conditions does not apply, the number computed in this section is zero.

**First determine the number of HDBH call attempts that use both OC-IP and an IP position**.

- In a pure OC-IP host (no standalone traffic) with all IP positions, this is the number of requests for operators that the host receives from its OC remotes during HDBH.
- In an OC host switch that has all IP positions, but that only functions as an OC host on some subset of its calls, count only the calls for which the switch functions as an OC-IP host. Do not count the calls for which it functions as a standalone switch, or an OC remote.
- In an OC host that has some IP positions and some TDM positions, one can determine the percentage of the positions that are IP, and count only that percentage of the calls for which the switch functions as an OC-IP host. However, this strategy may under-provision IP-XPMs if an unexpected event, such as outage of a cluster of TDM positions, can cause more IP positions than anticipated to be logged-on.

Once the maximum number of calls/hour that use both OC-IP and IP positions has been determined, **multiply that number by two** (since these calls will need IP-XPM capacity for messaging with both OC remotes and operator positions), and **divide by 50,000** (the maximum number of data-only calls/hour that an IP-XPM can safely process).

This determines the number of logical IP-XPMs needed for data-only calls in an OC host. This number will be used in a later section. If the switch functions in other roles besides just as an OC-IP host for host voice bypass calls, additional IP-XPM capacity requirements will be calculated in the next section.

***Example 1*** Suppose a combined standalone/host switch, with all IP positions, receives 90,000 HDBH requests for operator from its OC-IP remotes. Then the number of logical IP-XPMs needed by this switch to process these calls, from a traffic perspective, is

(90,000 x 2) / 50,000 = 3.6.

***Example 2*** Suppose the same switch in Example 1 still has 90,000 requests from its OC-IP remotes during HDBH, but now only 20% of its positions are IP. If we can assume that no more than 20% of the logged-on positions at any time will be IP, then we can estimate the number of logical IP-XPMs needed by this switch to process its data-only calls as

(0.20 x 90,000 x 2) / 50,000 = 0.72.

As previously explained, this number may underestimate the IP-XPM message-processing capacity needed.

### IP-XPM requirement for voice-and-data calls

This section applies to all TOPS-IP switches *except* pure OC-IP hosts (no standalone or TDM-OC calls) that have only IP positions (no TDM positions). It applies to OC-IP remotes as well as to standalone switches and most OC hosts. For some configurations, both this section and the previous one may apply.

***Note:*** TDM OC links must be replaced by OC-IP links.

**First determine the number of HDBH TOPS-IP call attempts that do *not* use both OC-IP and an IP position**.

- In a standalone switch with all IP positions, a TDM-OC host with all IP positions, or a combined standalone/TDM host with all IP positions, this is the number of calls that are presented to operators at this switch during HDBH. (Transfers and recalls should always be counted as separate calls.)

  Here we are counting calls for which the switch has an IP voice connection to the position and exchanges IP data messaging with the position. These calls do not use OC-IP voice links or do OC-IP data messaging.

- In a pure OC remote switch (no hosted operators), this is the number of operators requested from OC-IP hosts during HDBH. Do not count operator requests that the remote makes to TDM-OC hosts.

  Here we are counting calls for which this switch has an IP voice connection to the position and exchanges IP data messages with the OC host. These calls do not have an IP voice connection to the OC host, and they do not exchanges data messages directly with the position.

- In a pure OC host switch with all TDM positions, this is the number of calls from OC-IP remotes that request an operator from the host during HDBH. Do not count requests from TDM-OC remotes.

  Here we are counting calls for which the switch has an IP voice connection to an OC remote and exchanges OC data messages with the OC remote. These calls do not have IP voice or data connections to the positions.

- In a switch that functions in multiple roles, so that more than one of the above three bullets apply, count all of the traffic that applies.

- In a standalone or host switch that has some IP and some TDM positions, one can determine the percentage of the positions that are IP and the percentage that are TDM, and count only the corresponding percentage of the calls that would otherwise be counted. However, this strategy may under-provision IP-XPMs if an unexpected event causes a different mix of positions to be logged on.

The bullets above describe how to determine the maximum number of TOPS-IP calls/hour that use both voice and data resources at the switch. Once that number has been determined, **divide by 40,000** (the maximum number of voice-and-data calls/hour that an IP-XPM can safely process). This yields the number of logical IP-XPMs needed by this switch for voice-and-data calls. The number will be used in the next section.

***Example 1*** Suppose a TOPS switch hosts all IP positions, and suppose it functions as a standalone switch for some calls and a TDM-OC host for others. Suppose FM data for this switch shows 60,000 total position seizures during HDBH. Then the number of logical IP-XPMs needed by this switch to process these calls, from a traffic perspective, is

60,000 / 40,000 = 1.5.

***Example 2*** Suppose a TOPS switch hosts all IP positions, and suppose it functions on different calls as a standalone, as an OC-IP host, and as an OC-IP remote. We do not count the calls for which it functions as an OC-IP host; these calls do not use voice resources at this switch, and they were counted in "IP-XPM requirement for data-only calls" on page 194. Supposed OMs show that during HDBH, this switch requests operators from OC hosts for 45,000 calls, and gets operators from its own pool for 50,000 (standalone) calls. Then the number of logical IP-XPMs needed by this switch to process these calls, from a traffic perspective, is

(45,000 + 50,000) / 40,000 = 2.38.

***Example 3*** Suppose a TOPS switch hosts all TDM positions, and functions on different calls as a standalone, as an OC-IP host, and as an OC-IP remote. We do not count the standalone calls, since they use no TOPS-IP resources. Suppose that at HDBH this switch requests 12,000 operators from OC-IP hosts, and receives 30,000 operator requests from OC-IP remotes. Then the number of logical IP-XPMs needed by this switch to process these calls, from a traffic perspective, is

(12,000 + 30,000) / 40,000 = 1.05.

***Example 4*** Suppose a TOPS switch has half TDM positions and half IP positions, and it does not use OC. Suppose that at HDBH this switch provides operators for 155,000 calls. If we believe that about 50% of the logged-on positions at any time will be IP, we can estimate the number of logical IP-XPMs for this switch as

(0.5 x 155,000) / 40,000 = 1.937.

In this example, we should strongly consider provisioning a third IP-XPM even if subsequent steps do not indicate we need to. Under the assumption of 50% of the logged-on positions being IP, the logical number of IP-XPMs needed is very close to 2, so we gain very little extra capacity by rounding up to a whole number of IP-XPMs. Adding a third IP-XPM would provide flexibility in whether operators use IP positions or TDM positions.

### Total number of IP-XPMs

At a high level, the steps in determining the total number of IP-XPMs needed at a switch are:

1 Determine the number of IP-XPMs needed to house the 7X07 Gateway cards.

2 Determine the number of IP-XPMs needed to handle the HDBH traffic.

3 Determine the total number of IP-XPMs, based on the number of Gateways, the traffic level, and other factors.

The number of Gateway cards needed was calculated in “Determining the number of 7X07 Gateways” on page 185. Divide this number by 10 and round up.

***Example*** Suppose a switch needs 33 Gateway cards. Then the number of IP-XPMs needed to house them is

(33 / 10) = 3.3, rounded up to 4.

The numbers of logical IP-XPMs needed to handle data-only calls, and voice-and-data calls, were calculated in “IP-XPM requirement for data-only calls” on page 194 and “IP-XPM requirement for voice-and-data calls” on page 195. Add these two numbers, then round up.

***Example*** Suppose the numbers of logical IP-XPMs calculated in previous sections are 4.5 and 0.2. Then the number of IP-XPMs needed to handle the traffic is

(4.5 + 0.2) = 4.7, rounded up to 5.

The total number of IP-XPMs needed is at least the larger of (a) the number needed to house the Gateways and (b) the number needed to handle the traffic.

***Example*** If 4 IP-XPMs are needed to house the Gateway cards and 5 IP-XPMs are needed to handle the traffic, then at least 5 IP-XPMs are required.

There are some considerations that may cause an operating company to provision one more IP-XPM than the number that has been determined so far. These include the following:

- **Redundancy**. If an operating company views operator services as essential, it may choose to put two IP-XPMs in a switch for which the computations so far indicate that only one is needed. Although IP-XPMs are designed with redundancy in all their critical components, this would offer additional protection against a catastrophic problem with one of them.
- **Load balancing across IP-XPMs**. The calculations so far have assumed that if an office has more then one IP-XPM, the traffic load will be evenly distributed across them. It may not be possible to distribute the traffic perfectly. For example, an odd number of Gateway cards cannot be evenly divided between two IP-XPMs. In may cases, the rounding-up steps previously described will result in enough extra capacity that this is not an issue. However, if the rounding-up steps provide little or no extra capacity, consideration should be given to adding an extra IP-XPM.
- **Load balancing across position types**. If a standalone or OC host switch has both TDM and IP positions, and if the traffic calculation assumed that traffic would be distributed across positions in proportion to the number of installed positions of each type, it may have underestimated the number of logical IP-XPMs needed. Consideration should be given to adding one more IP-XPM if the rounding-up steps provided little or no extra capacity.

## Load balancing

In an office with more than one IP-XPM, it is important that the hardware and software provisioning be done in a way that distributes the traffic evenly over the IP-XPMs. The objectives here are (a) to stay within each IP-XPM's capacity limits and (b) to provide maximum processing capability in the unlikely event that one IP-XPM is unable to process calls.

The following guidelines should be followed:

- Distribute 7X07 Gateway cards evenly over the IP-XPMs, both overall and within each trunk group.

  ***Example*** Suppose a switch has two IP-XPMs, and needs 4 Gateways for one trunk group and 5 Gateways for another trunk group. The first trunk group should have 2 Gateways in each IP-XPM, and the second should have 3 Gateways in one IP-XPM and 2 in the other.

- Datafill OC-IP data links (table OCIPDL) in a way that evenly distributes the OC data messaging across the IP-XPMs.

  ***Example*** Suppose an OC-IP host has two IP-XPMs and provides operators for three OC-IP remotes. Datafill an OC-IP data link to each remote on each of the IP-XPMs.

- Datafill IP position data links (table TOPSPOS) in a way that evenly distributes the messaging to positions across the IP-XPMs.

  ***Example*** Suppose a switch hosts 900 IP positions and has three IP-XPMs. 300 positions should be datafilled to use each IP-XPM.

  ***Note:*** If different positions are dedicated to different services, and if the services have different AWTs or messaging characteristics, then distribute the positions that handle each service evenly across the IP-XPMs.

- Datafill trunk group selection algorithm MIDL (most idle) against TOPS-IP dynamic trunk groups in table TRKGRP.

***Note 1:*** For more information about the three trunks groups that may be used with TOPS-IP, refer to “Determining the number of 7X07 Gateways” on page 185.

***Note 2:*** For more information about datafilling OC-IP data links, refer to Chapter 3: “TOPS OC-IP application.”

***Note 3:*** For more information about datafilling IP positions, refer to Chapter 4: “TOPS IP position application.”

## Monitoring IP-XPM resource use

Logs, OMs, and FM statistics should be used to monitor resource utilization and to ensure that the desired grade of service is being provided. This section includes information about some of the things to look for.

A trend toward increased utilization of the 7X07s in a trunk group can be caught before shortages actually occur by monitoring the usage registers in OM group TRK for persistent changes. Since the maximum utilization that can be safely reached depends on the number of Gateways and the trunk holding time, it is more important to look for changes than to expect some absolute number.

If too few 7X07 Gateways are provisioned in a trunk group to provide voice resources for the offered load, frequent pegs will occur in OM register TRK_NOVFLATB, and frequent TOPS133 or TOPS134 logs will appear with trouble code VOICE_LINK_NOT_AVAILABLE. Operators may complain about positions being dropped to the assigned activities screen.

OM group XPMMSGOC may be useful in detecting changes in the messaging load on IP-XPMs. Refer to Chapter 13: “TOPS-IP OMs” for more information about the XPMMSGOC OM group.

When an IP-XPM is processing more calls than it can safely process, symptoms include degraded performance, lost messages, and problems over SWACTs. Note, however, that message loss can also occur at various places in the IP network.

### Limiting the use of dynamic voice links

The MAXCONNS field in table TOPSTOPT can be used to limit the number of TOPS-IP trunks that are available for call processing, to a number lower than the number of trunk members that are automatically datafilled in table TRKMEM when the Gateways are datafilled. There are two reasons why an operating company might want to do this.

- Since TOPS-IP trunks are added in multiples of 48, it is possible that an unexpected surge in traffic could cause the Gateways to generate more traffic than the IP network was engineered to handle. MAXCONNS could be used to make this less likely to happen.
- Since the "spare" Gateway in each trunk group processes calls just like all the others, it is possible that traffic levels could increase to the extent that a Gateway that was engineered to be a spare was actually needed to handle the offered load. The operating company would want to know this, and to obtain another Gateway for redundancy. Setting MAXCONNS for a trunk group to 48 less than the number of members in the group would ensure that spare capacity was reserved as intended.

When MAXCONNS for a TOPS-IP dynamic trunk group is set to a number less than 2016, a usage limit is automatically calculated for each in-service Gateway associated with that trunk group. These per-card usage limits are automatically re-calculated whenever Gateways associated with the trunk group are brought into service or removed from service, and they are maintained in a way that distributes the traffic evenly over the in-service Gateways. For example, if MAXCONNS is set to 100 and there are three in-service Gateway cards, then the first card is limited to 34 members and the second and third cards are limited to 33 each.

Calls in progress are not affected when usage limits are set or changed. When usage limits are set or changed, it may take several minutes of normal call processing before the limit is fully in effect.

Trunks that are unavailable because of MAXCONNS datafill appear as restricted idle (RES) at the MAP. They do not peg any usage registers in OM group TRK. They are counted in both the NCCT and NWCCT Info fields for the TRK OM tuple.

If the MAXCONNs value is low enough that not all of the offered traffic can be served, pegs will occur in OM register TRK_NOVFLATB, and TOPS133 or TOPS134 logs will appear with trouble code VOICE_LINK_NOT_AVAILABLE. Operators may complain about being dropped to the assigned activities screen.

***Note 1:*** For details on datafilling MAXCONNS in table TOPSTOPT, refer to Chapter 8: "TOPS-IP data schema."

***Note 2:*** For more information about the maintenance of TOPS-IP dynamic trunks, refer to Chapter 10: "TOPS-IP maintenance activities."

## MIS-IP requirements

QMS MIS-IP is an optional TOPS-IP application that was designed for TOPS standalone switches and OC hosts. QMS MIS-IP has not yet been made generally available. To investigate the use of MIS-IP, contact the Nortel Networks Operator Services organization. This section provides preliminary provisioning information for QMS MIS-IP.

The use of QMS MIS-IP places a heavy data load on the C-side links between the DMS core and the IP-XPM. The MIS-IP application, therefore, requires a dedicated IP-XPM (not used for OC-IP or IP positions). No 7X07 Gateway cards are provisioned in the MIS-IP-XPM. Up to two MIS-IP data links can be provisioned per OC host or standalone switch. A separate IP-XPM may be required for each MIS data link.

***Note:*** Contact your Nortel Networks representative to determine specific MIS-IP provisioning requirements for your configuration.

## Switch hardware resources

This section discusses the switch hardware resources that support the TOPS-IP network.

***Note:*** For detailed information on IP-XPM hardware and engineering rules, contact your Nortel Networks representative.

### Core hardware requirements

TOPS-IP requires a DMS Supernode core. TOPS-IP applications are supported on XA-Core and BRISC processors that are at least at the baseline level for the release. TOPS-IP is not supported on the Supernode/SE (SNSE) cores.

### XPM c-side link hardware requirements

The IP-XPM interface to the CM must be ENET. The CM, message switch (MS), and ENET interface must be configured to support enhanced messaging with 6 pairs of extended messaging links for each IP-XPM. SOC TEL00011 must be activated.

***Note:*** Refer to “C-side links to the IP-XPM” on page 184 for more information.

### IP-XPM shelf pack fill requirements

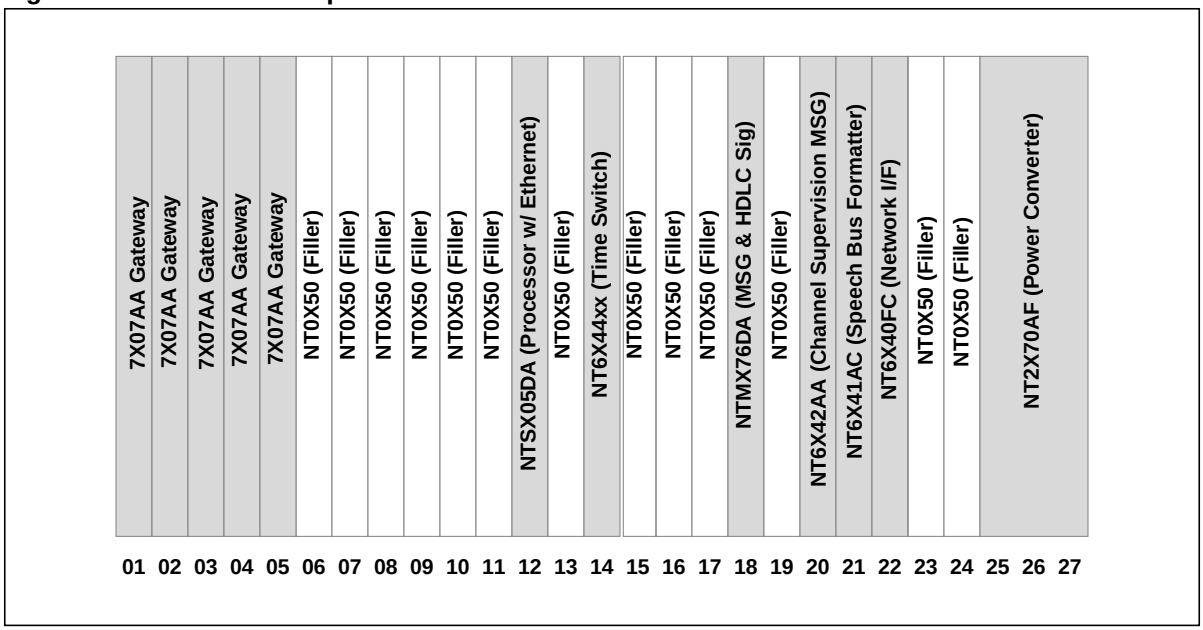
The IP-XPM can be deployed in either a frame configuration that complies with North American standards (NT6X01AF) or a C28 cabinet configuration that complies with European Union (EU) standards (NTRX46CG).

The required circuit pack fill is the same for both applications except that the cabinetized version (NTRX46CG) will support a maximum of 8 NT7X07 gateways, whereas the frame version (NT6X01AF) can support up to 10.

## IP-XPM frame configuration

Figure 110 lists the IP-XPM packfill (NT6X02MG).

**Figure 110 IP-XPM shelf packfill**




The following rules apply to the IP-XPM frame configuration for TOPS-IP applications:

- Provision up to five NT7X07AA gateway cards starting at slot 01 and progressing to slot 05 of each shelf (ten cards per IP-XPM).

  ***Note:*** Refer to the section “IP-XPM provisioning” on page 184 for important capacity information on the maximum number of 7X07 cards to provision.

- Two p-side cards per shelf are required for proper p-side bus termination. NT6X50AB cards can be substituted to meet this requirement if 7X07 engineering rules call for less than 2 cards per shelf. NT6X50ABs used as substitutions cannot be used for call processing and should not be datafilled.

- Provision one NTSX05DA unified processor card in slot 12 of each shelf (two cards per IP-XPM). Verify that backplane pins 7A and 8A are strapped together. This strap indicates the absence of other bus master cards such as the NTBX01 ISDN signaling processor.

- Provision one NT6X44 timeswitch card in slot 14 of each shelf (two cards per IP-XPM). The NT6X44AA is provisioned in North American markets. Non-North American markets using GTOPS should provision the NT6X44EA timeswitch.

- Provision one NTMX76DA messaging card in slot 18 of each shelf (two cards per IP-XPM).

- Provision one NT6X42AA channel supervision message card in slot 20 of each shelf (two cards per IP-XPM).
- Provision one NT6X41AC speech bus formatter card in slot 21 of each shelf (two cards per IP-XPM).
- Provision one NT6X40FC network interface card in slot 22 of each shelf (two cards per IP-XPM).
- Provision one NT2X70AF power converter in slots 26 and 27 of each shelf (two converters per IP-XPM).
- Verify that NTMX71AA bus termination cards are installed in backplane slot 19 of each shelf (two termination cards per IP-XPM).

### IP-XPM cabinet configuration

The IP-XPM C28 cabinet configuration complies with European Union (EU) standards (NTRX46CG) and will support a maximum of 8 NT7X07 gateways.

The rules discussed for the frame configuration also apply to the IP-XPM cabinet configuration for TOPS-IP applications with the following additions:

- When provisioning the NT7X07AA gateway cards, start at slot 01 (left most) and distribute them evenly among all IP-XPM shelves on the switch.
- Verify that NTMX71AA bus termination cards are installed in backplane slot 19 or 20 of each shelf (two termination cards per IP-XPM).
- Verify that backplane pins 7A and 8A are strapped together in slot 12 of each shelf.

### Frame, cabinet, and shelf requirements

The IP-XPM may be used in either a frame or cabinet configuration.

The IP-XPM frame (NT6X01AF) requires two IP-XPM shelves (NT6X0261), each equipped with a backplane. Earlier versions of XPM shelves cannot be used for an IP-XPM. A Connector Key Bracket (P0912903) aligns and secures the IP-XPM cable to the backplane.

The IP-XPM cabinet configuration (NTRX46CG) also requires two IP-XPM shelves (NT6X0261), each equipped with a backplane. Limitations on earlier versions of XPM shelves also apply.

***Note:*** Many of the provisionable components are the same in the frame and cabinet IP-XPM configuration.

### Ethernet patch panel requirements

In the IP-XPM frame configuration, the Ethernet patch panel (A0802978) is an *optional* component that provides a cross-connect point from the TOPS switch located in a central office, to data switches in the managed IP network. The patch panel is provisioned when structured cabling practices require it, but it *cannot* be used in applications that require NEBS compliance for LANs.

For cabinet deployments, the Ethernet patch panel is not an option.

### IP-XPM cable requirements

The frame IP-XPM requires two system cables, either two NT0X96NW or two NT0X96NV. If an Ethernet patch panel is not used, the NT0X96NW cables interconnect the backplanes directly to compatible Ethernet switches on the LAN. If the Ethernet patch panel is used, the NT0X96NV cables interconnect the backplanes to the patch panel.

The cabinetized IP-XPM requires two NTRX26HB cables to connect the cabinet backplane to the Ethernet switch. The TOPS-IP Ethernet cable kit, NTNX1236, is also required to connect the shelf to the cabinet backplane.

### IP-XPM firmware requirements

The firmware on the SX05DA card *must be at release SXFWAG02 or higher.* If the firmware is not at this level, the IP-XPM cannot be loaded with software and brought into service. Use of the firmware provided with each IP-XPM release software load is recommended.

To verify that the IP-XPM has the correct version of firmware, users can follow this procedure at the MAP:

1 Post the IP-XPM (DTC) at the MAPCI;MTC;PM level at the MAP.

2 Issue the QUERYPM CNTRS command. The firmware version is displayed as the “EEPRom Load.”

***Note 1:*** If the firmware load is incorrect, contact Nortel Networks technical support.

***Note 2:*** In this procedure, the CM queries the IP-XPM for what is actually loaded; this may not necessarily be the same as what is datafilled. Users should ensure that tables PMLOADS and LTCINV are datafilled with the correct firmware load name.

## TOPS-IP data network requirements

This section lists and explains the requirements for the packet data network used for TOPS-IP applications. The requirements are grouped as follows:

- Network performance requirements for packet loss, latency, and jitter
- 100-Mbps switched Ethernet port requirements

- Bandwidth requirements
- Redundancy and availability requirements
- Security requirements
- Other network requirements

***Note 1:*** These requirements are intended for use by a trained data network designer.

***Note 2:*** Appendix C: "TOPS-IP Network Configuration" contains additional information to assist in planning and configuring a data network for TOPS-IP.

Before implementing a data network, it is important to develop an IP address plan for the entire network. For TOPS, the plan may include IP-XPMs, IP positions, directory databases, MIS systems, OIA databases, and other nodes. Specific information about developing an IP address plan is outside the scope of this book.

## Network performance requirements for packet loss, latency, and jitter

This section includes data network quality of service (QoS) requirements for end to end packet loss, latency (delay), and jitter (variation in delay) across the packet data network.

TOPS-IP introduces several different types of network traffic. The different types of traffic have different QoS requirements. For example, the requirements for call control messages are different from the requirements for speech packets, although both are important.

For call control messages, (OC, OPP, and SIP protocols), packet loss must absolutely be minimized. A lost OC, OPP, or SIP data packet can result in a lost call or a "hung" operator position. Although latency of these packets is not critical for correct call processing, it *is* important for efficient use of operators' time. The higher the latency, the more time operators spend waiting rather than processing calls. Jitter is not relevant for call control packets.

For VoIP packets (RTP protocol), latency and jitter are critical for achieving carrier grade voice. End-to-end latency greater than 150 msec becomes noticeable to most people. Jitter buffers compensate for some amount of jitter, but they do so at the expense of adding to end-to-end delay. Also, highly variable jitter can increase packet loss, so jitter must be both small and consistent. Up to a point, packet loss is less critical for voice than latency or jitter, since lost RTP packets are masked. When packet loss gets too high, however, voice quality is affected. Packet loss less than 0.1% is not noticeable to most people.

Other packet types used by TOPS-IP have less stringent data network requirements, as shown in Table 3. For each message type, the table shows the specific requirements for packet loss, latency, and jitter; indicates a priority (importance), and provides additional explanation where applicable.

**Table 3 Packet loss, latency, and jitter requirements for TOPS-IP message types**

| Message type | Priority | Requirements | | | Comments |
|---|---|---|---|---|---|
| | | Packet loss | Latency | Jitter | |
| Call setup and control (SIP, OC, OPP) | highest | < 0.0001% | < 45 ms | N/A | This level of packet loss could result in up to one in one million calls being lost and/or calls resulting in hung operator positions. |
| VoIP (RTP, RTCP) | second highest | < 0.1% (see Note 1) | < 45 ms (see Note 2) | < 20 ms (see Note 2) | Processing in the 7X07 and IWS contributes up to 75 ms latency. PSTN delay may contribute another 25 or 30 msec. 45 msec latency in the data network should keep the end-to-end delay within the 150 ms target. |
| SNMP, DHCP | third highest | < 0.001% | < 150 ms | N/A | These packets must be delivered even under degraded network conditions. |
| 7X07 Gateway loading (FTP) and QMS MIS | best effort | < 0.1% | < 150 ms | N/A | These use TCP. |

***Note 1:*** For VoIP packets, the requirement for the percentage of lost packets includes both lost packets and late packets. A late packet is one that arrives outside the jitter buffer window of time.

***Note 2:*** The above VoIP requirements for latency and jitter are minimal requirements for what most people consider carrier grade voice. The best voice quality will be achieved if the data network provides latency less than 40 ms and jitter less than 10 ms.

Routers and other equipment in the data network can be configured to differentiate and prioritize traffic, based on port and protocol numbers, to provide the required QoS for each packet type. Customers whose WAN facilities are leased should have QoS service level agreements that ensure the WAN and LAN together meet the requirements. Table 4 lists the port numbers used for the different kinds of TOPS-IP packets.

**Table 4 Ports and protocols used for TOPS-IP data packets**

| Packet type | Port / Protocol |
|---|---|
| SIP | 5060 / UDP |
| OC-IP, OPP | ports configurable, 8600-8899 / UDP recommended |
| RTP, RTCP | 2326-2444 / UDP |

| Packet type | Port / Protocol |
|---|---|
| DHCP/Bootp | 67-68 / UDP |
| SNMP | 161 / UDP |
| FTP | 20-21 / TCP |
| QMS MIS | ports configurable / TCP |

If the data network is not configured to differentiate and prioritize traffic, delivery of *all* packets must meet the most stringent requirements for packet loss, latency, and jitter (< 0.0001% loss, < 45 ms latency, and < 20 ms jitter).

## 100-Mbps switched Ethernet port requirements

This section describes the Ethernet port requirements for TOPS-IP central offices (CO), operator services centers (OSC), and other sites with equipment needed for TOPS-IP.

All Ethernet ports must be switched, and must operate at 100 Mbps. Cables provided by Nortel Networks, such as the NT0X96NW (which connects the SX05DA cards in IP-XPMs) and NT0X96NW (which connects the 7X07AA cards in IP-XPMs), have RJ-45 connectors. CAT-5 (or better) cabling is required for 100Base-T.

Each TOPS-IP CO is provisioned with one or more IP-XPMs. The number of ports required is based on the number of IP-XPMs at the site, the number of 7X07AA Gateway cards in the IP-XPMs, and the need for redundant switches to eliminate a potential single point of failure.

Each IP-XPM has two SX05DA cards, each of which requires one port. An IP-XPM also has between zero and ten 7X07AA cards, each of which requires two ports.

A minimum of two Ethernet switches are required at the CO to provide redundant paths. This is explained further in “Redundancy and availability requirements” on page 210.

An OSC that has IP positions requires one 100-Mbps switched port for each position. If the OSC is very small and the service provider is willing to take the risk of an Ethernet switch failure isolating the entire OSC, one Ethernet switch may be sufficient. However, most OSCs will require at least two switches. A large TOPS host switch can support a maximum of 1023 positions, and these could be all at one OSC or distributed over numerous OSCs.

As shown in the table below, a small number of additional ports are needed for a pair of DHCP servers and an SNMP network management station. It is also recommended that a port be reserved at each subnet for attaching a sniffer when needed. Finally, for service providers who use QMS MIS-IP (when available), one or two additional 100 Mbps ports may be needed at the OSC.

**Table 5 100-Mbps switched Ethernet port requirements**

| Use | Location | Number of ports |
|---|---|---|
| SX05DA connections | central office | 2 per IP-XPM |
| 7X07AA connections | central office | 2 per 7X07 (0 to 10 7X07s per IP-XPM) |
| DHCP servers | 2 servers; location is part of network design | 1 per server |
| SNMP manager | service provider's choice | consult vendor documentation |
| IP positions | OSCs | 1 per position<br>(max 1023 positions per DMS switch) |
| QMS MIS-IP<br>(not yet available) | service provider's choice; probably OSC | 1 per MIS data link (max 2) |
| sniffer connection | all sites (recommended) | Nortel Networks will be better able to help resolve some problems if a sniffer can be connected, especially at the OSC. |
| ***Note 1:*** This table shows the requirements without consideration for redundancy.<br>***Note 2:*** Ports may also be needed for connecting other systems, such as TOPS force management devices and products that provide automated operator services. This table includes only the port requirements for the TOPS-IP product, and this product does not include all of the IP functionality that TOPS supports. | | |

## Bandwidth requirements

This section explains how to determine the LAN bandwidth requirements for TOPS-IP. It takes into account only the requirements for the TOPS-IP product. Other products supported by TOPS and IWS may require additional bandwidth at the CO, the OSC, or both.

### Bandwidth requirements for TOPS-IP CO LANs

To support flexibility in moving traffic from one OC host to another, each OC host office LAN must have sufficient bandwidth available to handle all current and anticipated future traffic. Similar considerations apply to TOPS standalone and OC remote offices.

Most of the bandwidth needed for TOPS-IP at the CO is for processing calls. Two main factors determine the bandwidth needed at the CO to process a call: the role in which the TOPS switch is functioning on the call, and the speech encoding used for the call.

- Role of TOPS switch

  When the TOPS switch acts as an OC-IP host for a call with an IP position, the VoIP connection is directly between the OC remote switch and the position. Since the VoIP connection bypasses the host, the OC host LAN does not require bandwidth for voice packets on this type of call.

For all other roles in which a TOPS switch can function on a TOPS-IP call—standalone call with IP position and OC-IP remote with TDM or IP position—the bandwidth requirement depends almost entirely on the speech encoding.

- Speech encoding

  TOPS-IP supports G.711 and G.723 codecs. The bandwidth requirements for G.723 are much lower. (DMS datafill for codec selection is in tables PKTVPROF and TQCQINFO.)

***Note:*** Even in a pure OC-IP host switch with all IP positions, there are likely to be some standalone calls. The reason is that all operator-originated calls, including directed assistance requests and responses to pages, are handled as standalone calls. See “Operator-originated calls” on page 149 for more information.

QMS MIS-IP (when available and if provisioned) requires additional bandwidth at an OC host or standalone TOPS switch. Bandwidth for QMS MIS-IP is estimated based on the number of positions (TDM and IP) hosted by the TOPS switch.

The following table shows how to compute TOPS-IP bandwidth requirements for a CO LAN. The per-call requirements include bandwidth for both voice packets and data (call control) packets.

**Table 6 TOPS-IP CO bandwidth requirements**

| **Bandwidth per (max) concurrent call** | | | | **QMS MIS-IP bandwidth (if provisioned)** | **Additional bandwidth** |
|---|---|---|---|---|---|
| **Bypass call (OC-IP host with IP position)** (see Note 1) | | **All other standalone, OC remote, or OC host calls involving OC-IP or IP position** | | | |
| **G.711** | **G.723** | **G.711** | **G.723** | | |
| 10 Kbps | 10 Kbps | 128 Kbps | 40 Kbps | 30 Kbps per 100 logged-in operators<br>(see Note 2) | Add an additional 1%<br>(see Notes 3 and 4) |

***Note 1:*** Even in a pure OC-IP host with all IP positions, not all calls are bypass calls. See “Operator-originated calls” on page 149.

***Note 2:*** When QMS MIS-IP is available, it will require CO bandwidth only at standalone and OC host switches at which it is provisioned. As an example of computing bandwidth for QMS MIS-IP, 300 Kbps bandwidth is required if the max number of operators who will be simultaneously logged into the TOPS switch is 1000.

***Note 3:*** The additional 1% is to cover traffic such as SNMP, DHCP, and maintenance messaging.

***Note 4:*** A TOPS CO LAN may have additional bandwidth requirements beyond those of the TOPS-IP product. For example, the CO may host TOPS force management devices or an OSSAIN service node. Bandwidth must be independently provisioned for such applications.

## Bandwidth requirements for TOPS-IP OSCs

To support flexibility in moving traffic from one OSC to another, each OSC must have sufficient bandwidth available to handle all current and planned operator positions.

Most of the bandwidth needed is for processing calls, and the requirement depends on whether G.711 or G.723 voice encoding is used. Additional bandwidth is needed for QMS MIS-IP if the MIS system is at the OSC. And a small amount of additional bandwidth is needed for miscellaneous TOPS-IP messaging, such as SNMP and maintenance messaging.

***Note:*** This book does not include bandwidth requirements for directory assistance database access, EISA (Enhanced Information Services Access), SMS (Short Message Service) messaging, email, OIA (Open Information Access) applications such as ORDB and Reference, TOPS force management devices, or other applications that may be in use at the OSC. It only includes the bandwidth needed for the applications described in the book.

The following table shows how to compute TOPS-IP bandwidth requirements for an OSC LAN. The per-call requirements include bandwidth for both voice packets and data (call control) packets.

**Table 7 TOPS-IP bandwidth requirements for OSC**

| Bandwidth per IP position | | QMS MIS-IP bandwidth (if provisioned at OSC) | Additional bandwidth for TOPS-IP |
|---|---|---|---|
| G.711 | G.723 | | |
| 128 Kbps | 40 Kbps | 30 Kbps per 100 logged-in operators<br>(see Note 1) | Add an additional 1%<br>(see Notes 2 and 3) |

***Note 1:*** As an example of computing bandwidth for QMS MIS-IP, 300 Kbps bandwidth is required if the max number of operators who will be simultaneously logged into the TOPS switch is 1000.

***Note 2:*** The additional 1% is to cover traffic such as SNMP and maintenance messaging.

***Note 3:*** A TOPS OSC LAN may have additional bandwidth requirements beyond those of the TOPS-IP product. For example, operators may access a directory assistance database, a web browser, or a UDP OIA application. Bandwidth must be independently provisioned for each application.

## Redundancy and availability requirements

The data network must be configured in a way that prevents any single failure from isolating nodes. At the CO, this includes certain failures in IP-XPMs as well as failures in data network equipment.

- The two SX05DA cards in an IP-XPM must have different paths to the network (connected to different Ethernet switches, with Ethernet switches both connected to a redundant pair of routers).

  ***Note:*** The IP-XPM actively uses only one SX05DA at a time. It uses ICMP echo (ping) monitoring to detect loss of connectivity to its default gateway router(s). If the active SX05DA loses connectivity, but the

inactive SX05DA does have connectivity, the IP-XPM autonomously switches activity (SWACT) to the other SX05DA.

- The two Ethernet ports on each given 7X07AA card must have different paths to the network.

  ***Note:*** The 7X07AA card uses only one port at a time. It monitors the Ethernet links on both its ports, and automatically switches to the other port when it detects a failure on the active port.

- At least one of the two DHCP servers must be reachable in the presence of any single network fault.
- A redundant pair of routers on each subnet must implement VRRP (Virtual Router Redundancy Protocol, see RFC2338) or a similar redundancy scheme, to ensure that a secondary router will immediately assume the load that was handled by a failed router. Convergence time less than two seconds is expected following a failure.
- Network availability of 99.999% or better is expected. This is an end-to-end requirement.

***Note 1:*** See "Example TOPS-IP network topologies" on page 577 for illustrations of example redundant network topologies, including provisioning of independent paths for the two SX05DA cards in an IP-XPM and the two ports on each 7X07AA.

***Note 2:*** If an office has more than one IP-XPM, multiple IP-XPMs may use the same pairs of redundant switches and routers, as long as port and bandwidth capacity is available.

Each OSC should also be provisioned with fully redundant paths. However, an exception may be made in the case of very small OSCs, if the service provider understands and is willing to accept the fact that the OSC can be isolated by a single failure.

### Security requirements

Firewall and/or router filtering protection must be implemented to ensure that only transactions from within the Directory and Operator Services network can reach the TOPS-IP LAN subnets and DHCP servers. TOPS-IP applications assume they are running in a secure environment.

***Note:*** IWS positions, OC hosts, and their OC remotes must all be in the same IP address space. IP routes between these networks or subnetworks must exist. It is not possible to place IP positions, their host switch or OC remote switch behind a server that performs network address translation.

### Other network requirements

Most service providers' networks are geographically dispersed enough to need a WAN for TOPS-IP. (If the TOPS switch and the OSC are co-located, and OC-IP is not used, a WAN may not be needed.) TOPS-IP does not specify the WAN implementation. For example, it could be Gigabit Ethernet, ATM, DWDM, Frame Relay, T1, T3, or OC-3.

TOPS-IP places certain requirements on the WAN. QoS, bandwidth, redundancy, and security requirements have been described in earlier sections. Note that WAN implementations typically have some additional bandwidth requirement for WAN transport packet overhead.

In addition, TOPS-IP has the following requirements for the data network:

- An SNMPv1 or SNMPv2 based network management system (provided by the customer) should be provisioned somewhere in the network in order to utilize the MIBs provided by the IP-XPM and other network equipment.
- Two DHCP network servers (Windows 2000 servers running Optivity NetID) must be provisioned somewhere within the secure TOPS-IP network to support 7X07 initialization and loading. Depending on customer datafill, DHCP may also be used in SX05DA initialization. These servers each require a 100 Mbps connection.
- The network must support forwarding of network server requests as unicast relays for a specific server (DHCP forwarding).
- The router redundancy scheme must support ping, either using a virtual IP address or physical addresses. This is because the SX05DA uses ping to detect the presence of its gateway router.

  ***Note:*** As defined in RFC2338, VRRP virtual IP addresses do not respond to ping messages. Vendor implementations may differ. If a virtual address does not respond to ping, the physical router addresses must be datafilled for the SX05DA in table XPMIPGWY (at the switch) or in the DHCP server.
- Routers and other nodes connected to the same local IP network as an IP-XPM must process gratuitous ARP broadcast requests.

Router uplinks depend on the WAN implementation. The following table shows the TOPS-IP call processing capabilities of T1, DS-3, and OC-3 links.

**Table 8 TOPS-IP call processing capacities of T1, DS3, and OC3 router uplinks**

| Transport | Capacity (number of concurrent calls) | |
|---|---|---|
| | **G.711** | **G.723** |
| T1 | 12 | 36 |
| DS3 | 320 | 1000 |
| OC3 | 1000 | 3000 (see Note) |
| ***Note:*** TOPS supports max 1023 operators at a host switch. | | |

The entire network should be engineered with enough capacity, and redundant facilities and paths, that the remaining paths or components can handle the entire traffic load when any one path or component fails.

***Caution:*** Provisioning for reduced capacity under network failure conditions is not recommended. This may be an acceptable strategy with TDM facilities, since nailed-up TDM facilities are reserved for each voice and data link. While new TDM calls may not get facilities, calls in progress are not affected. Since IP connections all share the same facilities, and since there is no mechanism to throttle new originations when the network is degraded, the consequences of a network failure are potentially more severe.

Service providers can select from two alternative solutions if the cost of doubling the bandwidth to provide full redundancy for G.711 to the OSC is prohibitive:

- use G.723 for all IP position VoIP connections
- use auto-compression

Auto-compression is a method by which IP position voice connections can normally use G.711 when sufficient bandwidth is available for acceptable voice quality, but can change to using G.723 when network conditions degrade. If auto-compression is enabled, it is only necessary to provision the amount of bandwidth from the OSC for all IP positions to use G.711 without redundancy.

***Note 1:*** Auto-compression is not available for VoIP connections between OC host and remote switches.

***Note 2:*** See Chapter 4: “TOPS IP position application” for a more detailed description of auto-compression.

# Part 5: Provisioning

Part 5: Provisioning includes the following chapters:

# Chapter 8: TOPS-IP data schema

This chapter provides information on how to datafill the switch tables used to provision TOPS-IP. It discusses each table and the datafill dependencies among the tables. Datafill information given is specific to TOPS-IP, with an explanation of fields, valid values, and examples.

## TOPS-IP datafill requirements

The descriptions and examples of TOPS-IP datafill in this chapter are organized around the following areas:

- IP infrastructure datafill (page 219)

  This datafill provisions the IP data and voice infrastructure at the switch so that various TOPS-IP CM applications can use the managed IP network for transport and routing.

- OC-IP datafill (page 264)

  This datafill provisions the OC-IP application at the switch so that OC hosts and OC remotes can have data and voice connectivity with each other over the managed IP network. This datafill also allows OC-IP remotes to have direct IP voice connectivity with IP positions that are datafilled in OC-IP hosts.

- IP position datafill (page 274)

  This datafill provisions the IP position application at a standalone or OC host switch, so that the switch and operator positions have data and voice connectivity with each other over the managed IP network.

- QMS MIS-IP datafill (page 280)

  This datafill provisions the TOPS QMS MIS-IP application at a standalone or OC host switch so that MIS data can be sent to an MIS vendor node on the managed IP network.

- XIPVER datafill (page 284)

  This datafill provisions the XIPVER test tool at the switch so that users can test IP data communication through IP-XPMs.

## Alphabetical reference for tables

The following table lists each table in alphabetical order and the page where its description begins.

**Table 9 Alphabetical reference for TOPS-IP table descriptions**

| Table name | Page number |
|---|---|
| CLLI | page 238 |
| CARRMTC | page 225 |
| IPCOMID | page 236 |
| IPINV | page 247 |
| IPSVCS | page 234 |
| LTCINV | page 222 |
| LTCPSINV | page 226 |
| MTCFAIL | page 278 |
| MTCTEST | page 279 |
| OCGRP | page 267 |
| OCIPDL | page 269 |
| OCOFC | page 266 |
| OFCENG | page 257 |
| OFCVAR | page 272 |
| PKTVPROF | page 261 |
| QMSMIS | page 281 |
| SITE | page 246 |
| TOPSPARM | page 273, page 277 |
| TOPSPOS | page 274 |
| TOPSTOPT | page 255 |
| TQCQINFO | page 263 |
| TRKGRP | page 239 |
| TRKMEM | page 253 |
| TRKOPTS | page 243 |
| TRKSGRP | page 241 |
| XPMIPGWY | page 228 |
| XPMIPMAP | page 230 |

## IP infrastructure datafill

The IP infrastructure tables provision IP data and voice at the TOPS switch. This datafill specifies hardware and software for the SX05DA card, reserves software ports on the IP-XPM used for data communication, defines the 7X07 Gateway cards, and establishes trunk groups and packetized voice profiles to be used in voice communication.

***Note 1:*** Before beginning to datafill the IP infrastructure tables, users should understand their network engineering requirements. For more information, refer to Chapter 7: "TOPS-IP engineering guidelines."

***Note 2:*** TOPS-IP CM applications (OC-IP, IP position, QMS MIS-IP) are dependent on IP infrastructure datafill. For more discussion of the datafill for a particular application, refer to the corresponding subsection in this chapter.

***Note 3:*** The 7X07 Gateways receive software load and configuration information from the DHCP server instead of from switch datafill. For more information, refer to Appendix A: "DHCP server guidelines."

### Table datafill dependencies

The following IP infrastructure tables are listed in the order in which they should be datafilled.

**Table 10 IP infrastructure datafill sequence**

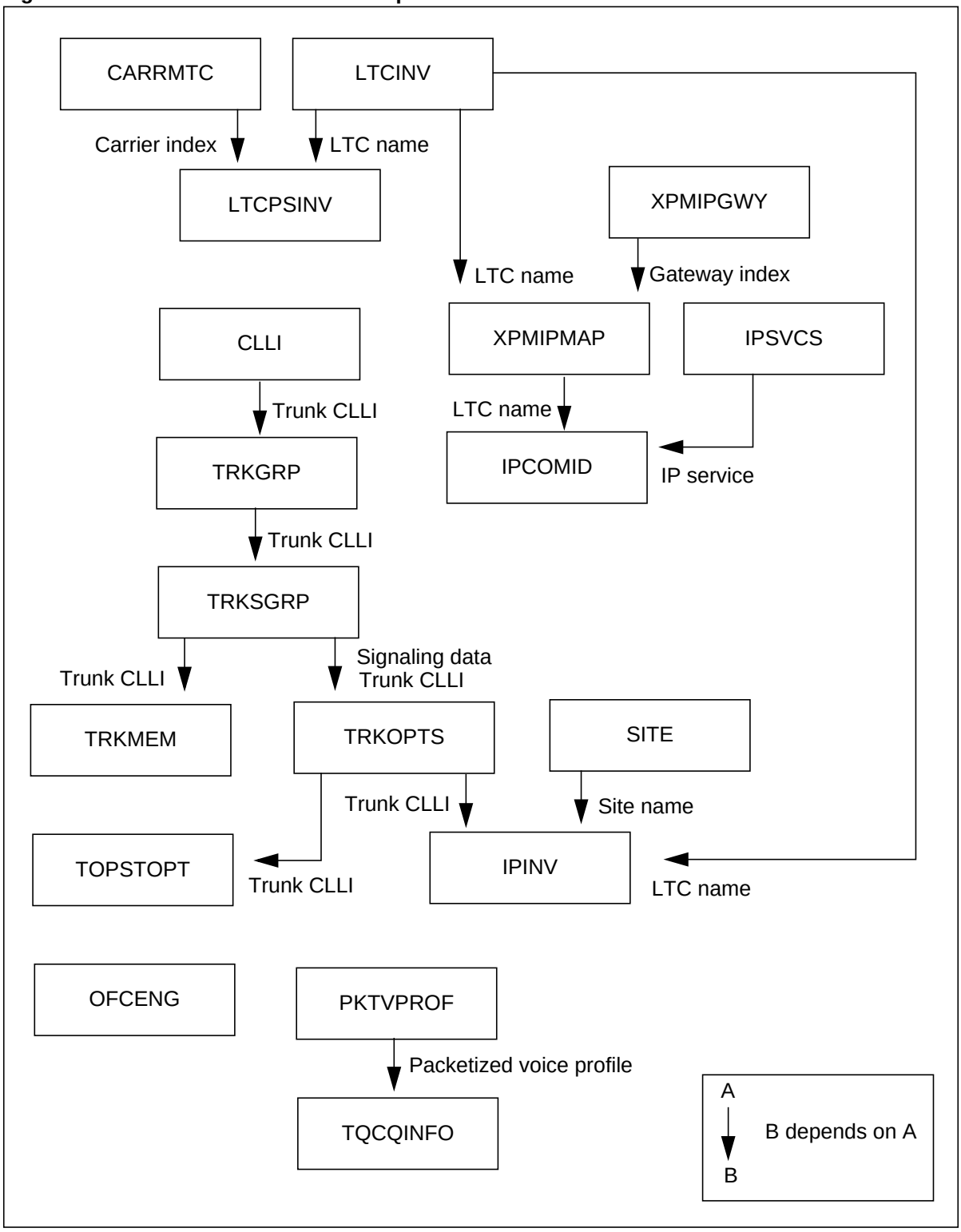
| Table name | Definition |
|---|---|
| **Hardware provisioning tables** | |
| LTCINV | Line Trunk Controller Inventory. This table defines hardware for the IP-XPM (see Note 1). |
| CARRMTC | Carrier Maintenance. This table defines maintenance control information for peripheral modules, such as the IP-XPM (DTC). |
| LTCPSINV | LTC P-side Inventory. This table defines peripheral-side links for the IP-XPM. |
| **Data provisioning tables** | |
| XPMIPGWY | XPM IP Gateway. This table contains information on gateway routers for the SX05DA card in the XPM. |
| XPMIPMAP | XPM IP Mapping. This table defines IP configuration information for the SX05DA card in the XPM. |
| IPSVCS | IP Services. This table defines local IP transport service names and associates a software port and protocol with each service name. |
| IPCOMID | IP Communication Identifier. This table defines COMIDs and associates with each COMID an IP transport service and an IP-XPM. This specifies local connectivity information. |

**Table 10 IP infrastructure datafill sequence**

| **Voice provisioning tables** | |
|---|---|
| CLLI | Common Language Location Identifier. This table defines the names and maximum number of members of voice link groups. |
| TRKGRP | Trunk Group. This table defines each voice trunk group. TOPS-IP applications that require voice trunks (such as OC-IP and IP position) use the IT (intertoll) group type. |
| TRKSGRP | Trunk Subgroup. This table contains signaling information for each voice trunk subgroup. |
| TRKOPTS | Trunk Options. This table defines options for trunk groups. TOPS-IP applications that require voice trunks use the DYNAMIC option. |
| SITE | Site. This table defines a name for a group of 7X07 Gateway cards datafilled in table IPINV. |
| IPINV | Internet Protocol Inventory. This table defines the individual 7X07 Gateway cards in the IP-XPMs used for TOPS-IP applications. |
| TRKMEM | Trunk Members. This table defines each voice link member and its hardware address. For dynamic trunks, this table is automatically datafilled by table IPINV (see Note 2). |
| TOPSTOPT | TOPS Trunk Options. This table defines options for TOPS-supported trunks. A maximum usage limit for TOPS-IP dynamic trunks may be set in the MAXCONNS field. |
| OFCENG | Office Engineering. This table contains office-wide engineering parameters. |
| PKTVPROF | Packetized Voice Profiles. This table specifies packetized voice profiles, which are used in selecting a voice codec for a call. |
| TQCQINFO (See Note 3.) | TOPS QMS Call Queue Information. This table specifies information about TOPS QMS call queues, including which packetized voice profile to use for calls associated with each queue. |
| ***Note 1:*** Table PMLOADS must be datafilled before table LTCINV. See the explanation for the LOAD field (page 222) and the E2PROM field (page 224) for more information.<br><br>***Note 2:*** When the DYNAMIC trunk option is set in table TRKOPTS, table IPINV automatically datafills table TRKMEM with individual trunk members.<br><br>***Note 3:*** Table TQCQINFO is really an application table. It is discussed with the infrastructure tables because it is used by both the OC-IP application and the IP position application. | |

Figure 111 summarizes the dependencies among the IP infrastructure tables. Arrows point to dependent tables and indicate the dependent information. Examples for each table are shown after the figure.

**Figure 111 IP infrastructure datafill dependencies**



## LTCINV

Table LTCINV specifies hardware inventory information for each XPM (excluding the P-side link assignments). The value in field LTCNAME is referenced by tables LTCPSINV, XPMIPMAP, IPCOMID, and IPINV.

The following table shows the datafill specific to TOPS-IP for table LTCINV. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 11 Datafilling table LTCINV**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| LTCNAME | | See subfields | LTC name. This field consists of subfields XPMTYPE and XPMNO. |
| | XPMTYPE | DTC | XPM type. Enter DTC for the type of XPM. |
| | XPMNO | 0 to 255 | XPM number. Enter the number of the XPM. |
| LOAD | | QTP22xx | Load. Enter the load name. For TOPS22/ SN09, the valid value is QTP22<version>.<br>***Note1:*** The load name QTP22<version> represents the load name for IP access. This value must first be datafilled in table PMLOADS.<br>***Note2:*** Refer to Table 62 on page 287 for a list of the supported IP-XPM loads for each CM load. |
| OPTCARD | | MX76C14 | Optional card. Enter MX76C14 and datafill the MX76LOC refinement. |
| | MX76LOC | HOST | MX76 location. Enter HOST. |
| TONESET | | NORTHAA | Tone set. Enter the toneset. For an IP-XPM, NORTHAA is the only value that LTCINV accepts.<br>***Note:*** This entry is only to satisfy table control and diagnostics. The IP-XPM does not use this toneset to generate tones. |
| PROCPEC | | SX05DA | Processor PEC. Enter SX05DA $ for each unit of the Unified Processor card. |

**Table 11 Datafilling table LTCINV**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| EXTLINKS | | 0 or 6 | Extended links. This number identifies the number of pairs of C-side 14 extended messaging links.<br>***Note:*** Enter 0 if the CONVERTCSLINKS utility will be used to provision the extended messaging links. CONVERTCSLINKS automatically adjusts the EXTLINKS value. For more information, refer to "CONVERTCSLINKS" on page 427. Enter 6 if the CONVERTCSLINKS utility will not be used. |
| E2LOAD | | firmware loadname released with the XPM load (for example, SXFWAJ02) | EEPROM firmware load. Enter the firmware load name.<br>***Note:*** The firmware load name must first be datafilled in table PMLOADS. To verify the version of firmware that is actually loaded in the IP-XPM, users can issue the QUERYPM CNTRS command at the MAP. See "IP-XPM firmware requirements" on page 204 for more information. |
| OPTATTR | | CCS7 | Option attributes. Enter CCS7.<br>***Note:*** This entry is only to satisfy table control. The IP-XPM does not use the SS7 network. |
| PEC6X40 | | 6X40FC | PEC 6X40 version. Enter 6X40FC for ENET with fiber links. This is the only network interface that the IP-XPM supports. |

## LTCINV example

The following example shows datafill for three DTCs.

**Figure 112 MAP display example for table LTCINV**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
--------------------------------------------------------------------------
DTC 10   1001   LTE    0    51    0     C   0    6X02AF  QTP22xx (ABTRK DTCEX)$
   (0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5) (0 11 0 6) (0 11 0 7)
(0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11) (0 11 0 12) (0 11 0 13) (0 11 0 14) (0 11 0
15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6         SXFWAJ02      (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0    6X02AF   QTP22xx (ABTRK DTCEX)$
   (0 11 1 0) (0 11 1 1) (0 11 1 2) (0 11 1 3) (0 11 1 4) (0 11 1 5) (0 11 1 6) (0 11 1 7)
(0 11 1 8) (0 11 1 9) (0 11 1 10) (0 11 1 11) (0 11 1 12) (0 11 1 13) (0 11 1 14) (0 11 1
15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6          SXFWAJ02     (CCS7) $
       6X40FC    N
DTC 20  1002   LTE    0    51    0     C   0    6X02AF   QTP22xx (ABTRK DTCEX)$
   (0 12 1 0) (0 12 1 1) (0 12 1 2) (0 12 1 3) (0 12 1 4) (0 12 1 5) (0 12 1 6) (0 12 1 7)
(0 12 1 8) (0 12 1 9) (0 12 1 10) (0 12 1 11) (0 12 1 12) (0 12 1 13) (0 12 1 14) (0 12 1
15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6          SXFWAJ02     (CCS7) $
       6X40FC    N
```

## LTCINV error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 12 Error messages for table LTCINV**

| Error message | Explanation |
|---|---|
| `Peripheral datafilled in table XPMIPMAP.` | The user tries to delete an XPM that is referenced by table XPMIPMAP. |
| `Change from Power-PC type processor not allowed since XPM is datafilled in table XPMIPMAP.` | The user tries to change the PROCPEC value to a non-Power PC processor type for an XPM that is referenced by table XPMIPMAP. |
| `Please quit table LTCINV and enter CONVERTCSLINKS to change to or from extended links.` | The user tries to modify the EXTLINKS field in an existing tuple, without using the CONVERTCSLINKS utility. |

## CARRMTC

Table CARRMTC specifies maintenance control information for peripheral modules (PM), such as the DTC. The value in field TMPLTNM is referenced by table LTCPSINV.

The following table shows the datafill specific to TOPS-IP for table CARRMTC. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 13 Datafilling table CARRMTC**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| CSPMTYPE | | DTC | C-side node PM type. Enter DTC. |
| TMPLTNM | | Alphanumeric up to 16 characters | Template name. Enter the template name that is associated with the TOPS-IP 7X07 Gateway cards.<br>***Note:*** It is recommended that the template name match the alphanumeric site name for the Gateway cards in table SITE. |
| ATTR | | See subfields | Attributes. This field consists of SELECTOR and refinements based on the selector. |
| | SELECTOR | DS1 | Selector. For a DTC, enter DS1 and datafill the CARD, FF, ZLG, and BERB refinements. |
| | CARD | NT7X07AA | Card. Enter NT7X07AA for the Gateway card. |
| | FF | SF | Frame format. Enter SF. |
| | ZLG | ZCS | Zero logic. Enter ZCS. |
| | BERB | BPV | Bit error rate base. Enter BPV. |

## CARRMTC example

The following example shows datafill for the XPM type (DTC) used by the Gateways for voice over IP communication.

**Figure 113 MAP display example for table CARRMTC**

```
CSPMTYPE TMPLTNM  RTSML  RTSOL  ATTR
------------------------------------------------------------------------------
DTC      TGWY     255    255    DS1 NT7X07AA  MU_LAW SF ZCS BPV NILDL N 250 1000
50 50 150 1000 3 6 864 100 17 511 4 255
```

## LTCPSINV

Table LTCPSINV specifies the P-side link assignments that are associated with voice over IP at the DTC. Tuples in this table use the same key as table LTCINV. Datafill values include port numbers and signaling interface data for the 7X07 Gateways (defined in table IPINV).

***Note 1:*** An entry in table LTCPSINV is added automatically when an XPM is datafilled in table LTCINV. All the P-side link types initially default to NILTYPE. P-side links that do not have hardware assigned must remain NILTYPE. Unequipped software-assigned P-side links generate service-affecting problems.

***Note 2:*** After the P-side links for a Gateway are added to table LTCPSINV, the corresponding datafill for the Gateway must be entered in table IPINV. Otherwise the IP-XPM will have inconsistent information about its packfill, and diagnostics may be affected. The switch also will generate PM777 logs (wrong P-side card). For details on the correct datafill for port mapping, refer to “LTCPSINV-to-IPINV port mapping” on page 249.

The following table shows the datafill specific to TOPS-IP for table LTCPSINV.

**Table 14 Datafilling table LTCPSINV**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| LTCNAME | | See subfields | LTC name. This field consists of subfields XPMTYPE and XPMNO. |
| | XPMTYPE | XPM type from table LTCINV | XPM type. Enter the XPM type. |
| | XPMNO | XPM number from table LTCINV | XPM number. Enter the XPM number. |
| PSLINKTAB | | See subfields | P-side link table. This field consists of subfield EXP_SIDES and its refinements. |
| | EXP_SIDES | N | Extended peripheral sides. Enter N. Also datafill the PSLINK refinement. |
| | PSLINK | 0 to 19 | P-side link. For each P-side link, datafill the port number and the PSDATA refinements. Also datafill the port+1 information.<br>***Note:*** A P-side link pair (port, port+1) assigned in table LTCPSINV for the IP-XPM must have a corresponding Gateway card and port number defined in table IPINV (page 247). |
| | PSDATA | See refinements | P-side data. This field consists of the AREASELECT, CARRIDX, and ACTION refinements. |

**Table 14 Datafilling table LTCPSINV**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| | AREASELECT | DS1 | Area selector. Enter DS1 and datafill the CARRIDX and ACTION refinements. |
| | CARRIDX | TMPLTNM from table CARRMTC | Carrier index. Enter the template name. |
| | ACTION | N | Action. Enter N. |

## LTCPSINV example

The following example shows the P-side link assignments for three IP-XPMs (DTCs). DTC 10 is datafilled with eight P-side link assignments, to support four Gateway cards. DTC 11 is datafilled with six P-side link assignments, to support three Gateway cards. The other P-side links are unassigned and so must be datafilled with a value of NILTYPE.

***Note:*** In this example, DTC 20 does not require P-side link datafill in table LTCPSINV, because it does not perform any voice over IP (for example, it is dedicated to a QMS MIS-IP data link). No Gateway cards are installed, so the P-side links remain NILTYPE.

**Figure 114 MAP display example for table LTCPSINV**

```
LTCNAME   PSLINKTAB
------------------------------------------------------------------------
DTC 10    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N) (8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 DS1 TGWY N) (13 DS1 TGWY N) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $

DTC 11    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N)(8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $

DTC 20    N (0 NILTYPE) (1 NILTYPE) (2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 NILTYPE) (7 NILTYPE)(8 NILTYPE) (9 NILTYPE)
(10 NILTYPE) (11 NILTYPE) (12 NILTYPE) (13 NILTYPE) (14 NILTYPE)
(15 NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $
```

## XPMIPGWY

Table XPMIPGWY specifies gateway router information for the SX05DA. The value in field GWINDEX is referenced in table XPMIPMAP when the CM configuration method is datafilled. Datafill in table XPMIPGWY is never used when the DHCP configuration method is datafilled.

***Note 1:*** The term *gateway* in the context of routers does not refer to the 7X07 Gateway card in the IP-XPM.

***Note 2:*** The actual number of routers to provision depends on administrative factors, network configuration, and capacity issues. For more information, refer to Chapter 7: "TOPS-IP engineering guidelines."

***Note 3:*** An IP address in switch datafill consists of four octets separated by a single spaces (no periods).

The following table shows the datafill specific to TOPS-IP for table XPMIPGWY.

**Table 15 Datafilling table XPMIPGWY**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| GWINDEX | | 0 to 255 | Gateway index. Enter an index number to identify the tuple. |
| DESTADDR | | IP address of 4 octets from 0 to 255 | Destination address. Enter the IP address of a destination. Depending on the value in field RTEMASK, this address indicates either a specific host or a network.<br>***Note:*** A special set of IP addresses (127 x x x) is used for loop-back testing, and is not recommended for TOPS-IP applications. |
| RTEMASK | | Subnet mask of 4 octets from 0 to 255 | Route mask. Enter the mask that is applied to the destination IP address in field DESTADDR. The mask determines which part of the destination IP address pertains the subnetwork and which pertains to the host.<br>***Note:*** A DESTADDR of 0.0.0.0 with a RTEMASK of 0.0.0.0 indicates a default route. |
| GWIPADDR | | IP address of 4 octets from 0 to 255 | Gateway IP address. Enter the IP address of the router used to route data to its destination. |
| METRIC | | 0 | Metric. Enter 0, because this field is not currently used. |

### XPMIPGWY example

The following example shows two tuples specifying default routers.

**Figure 115 MAP display example for table XPMIPGWY**

```
GWINDEX   DESTADDR       RTEMASK            GWIPADDR       METRIC
-------------------------------------------------------------------
0         0 0 0 0        0 0 0 0            47 192 3 1     0
1         0 0 0 0        0 0 0 0            47 192 3 2     0
```

### XPMIPGWY error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 16 Error messages for table XPMIPGWY**

| Error message | Explanation |
|---|---|
| `ERROR: INVALID IP ADDRESS FOR DESTADDR.` | The user tries to add an invalid value for DESTADDR. |
| `ERROR: INVALID MASK FOR RTEMASK.` | The user tries to add an invalid value for RTEMASK. |
| `ERROR: INVALID IP ADDRESS FOR GWIPADDR.` | The user tries to add an invalid value for GWIPADDR. |
| `ERROR: INSERVICE XPM IN TABLE XPMIPMAP IS USING THIS INDEX.` | The user tries to change a gateway index while its associated XPM (from table XPMIPMAP) is in service. |

## XPMIPMAP

Table XPMIPMAP specifies various IP information for the SX05DA, including the bootstrapping configuration method used when the XPM is brought into service.

***Note:*** The GWINDEX field may be changed while the associated XPM is in service; however, the change causes the XPM to go in-service trouble (ISTb) when the standard CM/XPM audit checks the static data between the XPM and CM. Static data download of the changes to this field does not occur until the next RTS. After changing this field, users should perform a cold SWACT on the IP-XPM. Any in-service 7X07 Gateways on the XPM will go SYSB and recover automatically after the cold SWACT completes. For more information, refer to "Updating static data" on page 299.

The following table shows the datafill specific to TOPS-IP for table XPMIPMAP.

**Table 17 Datafilling table XPMIPMAP**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| XPMNAME | | See subfields | XPM name. This field consists of subfields XPMTYPE and XPMNO. |
| | XPMTYPE | XPM type from table LTCINV | XPM type. Enter the XPM type (DTC). |
| | XPMNO | XPM number from table LTCINV | XPM number. Enter the XPM number. |
| AUTONEG | | AUTO | Autonegotiation. Enter AUTO for the XPM to automatically select the Ethernet speed (10BT or 100BT) by negotiating with the network. |
| SUBNMASK | | Subnet mask of 4 octets from 0 to 255 | Subnet mask. Enter the subnet mask that is used for the local subnet network. |
| IPCONFIG | | CM or DHCP | IP configuration. Enter the configuration method used to provide the XPM with IP bootstrapping information, as follows:<br>- Enter CM if the CM configures the XPM. Also datafill the following refinements: ACTADDR, INADDR, UNIT0, UNIT1, GWINDEX, DNSINFO.<br>- Enter DHCP if the DHCP server configures the XPM. No further datafill is required. |

**Table 17 Datafilling table XPMIPMAP**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| ACTADDR | | IP address of 4 octets from 0 to 255 | Active unit IP address. Enter the IP address of the active unit of the XPM. The last octet of the active address must be divisible by 4 (for example, 47.192.3.24). |
| INADDR | | IP address of 4 octets from 0 to 255 | Inactive unit IP address. Enter the IP address of the inactive unit of the XPM. The inactive address is always ACTADDR + 1 (for example, 47.192.3.25). |
| UNIT0 | | IP address of 4 octets from 0 to 255 | Unit 0 IP address. Enter the IP address of unit 0 of the XPM. The unit 0 address is always ACTADDR + 2. The XPM uses this address internally for diagnostics. |
| UNIT1 | | IP address of 4 octets from 0 to 255 | Unit 1 IP address. Enter the IP address of unit 1 of the XPM. The unit 1 address is always ACTADDR + 3. The XPM uses this address internally for diagnostics. |
| GWINDEX | | Gateway index from table XPMIPGWY | Gateway index. Enter up to 10 indexes from table XPMIPGWY. |
| DNSINFO | | N | Domain name server information. Enter N, because this field is not currently used. |
| SNMP | | Y/N | Simple Network Management Protocol.This field indicates whether SNMP is enabled on the IP-XPM.<br>If SNMP is Y, datafill the SNMP community name in the additional field COMMNAME.<br>If SNMP is N, no additional fields can be datafilled. |
| | COMMNAME | One to sixteen characters<br>Non-alpha-numeric symbols and lowercase letters can be entered using single quotes. | Community name. This field appears when field SNMP is set to Y.<br>This field indicates the SNMP community name for SNMP read and write operations on the IP-XPM. |

## XPMIPMAP example

The following example shows datafill for three XPMs. Both DTC 10 and DTC 11 use the CM method, so the switch will download the IP information to these XPMs when they are brought into service. DTC 20 uses the DHCP method, so IP information will be sent from the DHCP server in the IP network.

**Figure 116 MAP display example for table XPMIPMAP**

```
XPMNAME  AUTONEG  SUBNMASK       IPCONFIG  SNMP        ACTADDR       INADDR
      UNIT0         UNIT1          GWINDEX           DNSINFO
-------------------------------------------------------------------------------
DTC 10   AUTO     255 255 255 0  CM         N           47 192 3 24   47 192 3 25
      47 192 3 26   47 192 3 27     (0) (1) $        N
DTC 11   AUTO     255 255 255 0  CM         Y  public   47 192 3 116  47 192 3 117
      47 192 3 118   47 192 3 119   (0) (1) $        N
DTC 20   AUTO     255 255 240 0  DHCP
```

## XPMIPMAP error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 18 Error messages for table XPMIPMAP**

| Error message | Explanation |
|---|---|
| ERROR: XPM NOT DATAFILLED IN TABLE LTCINV. | The user tries to add an XPM that is not datafilled in table LTCINV. |
| ERROR: ONLY DTC OR PDTC TYPE XPM ARE ALLOWED. | The user tries to add an XPM whose type is not DTC or PDTC.<br>***Note:*** For TOPS-IP applications, the XPM type must be DTC. |
| ERROR: BOTH UNITS ON THE XPM MUST BE SX05 TYPE PROCESSORS. | The user tries to add an XPM whose PROCPEC type is not SX05. |
| ERROR: AUTONEG CHANGE NOT ALLOWED WHILE XPM IS INSERVICE. | The user tries to change the value for AUTONEG while the associated XPM is in service. |
| ERROR: IPCONFIG CHANGE NOT ALLOWED WHILE XPM IS INSERVICE. | The user tries to change the value for IPCONFIG while the associated XPM is in service. |
| ERROR: SUBNET MASK CHANGE NOT ALLOWED WHILE XPM IS INSERVICE. | The user tries to change the value for SUBNMASK while the associated XPM is in service. |
| ERROR: IP ADDRESS CHANGE NOT ALLOWED WHILE XPM IS INSERVICE. | The user tries to change an IP address while the associated XPM is in service. |
| ERROR: AN INVALID SUBNET MASK WAS ENTERED. | The user tries to add an invalid value for SUBNMASK. |
| ERROR: AN INVALID XPM IP ADDRESS WAS ENTERED. | The user tries to add an invalid value for IP address. |

**Table 18 Error messages for table XPMIPMAP**

| Error message | Explanation |
|---|---|
| ERROR: THE ACTIVE ADDRESS MUST BE EVENLY DIVISIBLE BY FOUR. | The user tries to add a value for ACTADDR that is not divisible by 4. |
| ERROR: IP ADDRESS FOR ACTADDR, INADDR, UNIT0, AND UNIT1 MUST BE SEQUENTIAL. | The user tries to datafill IP addresses that are not sequential. |
| ERROR: ONE OR MORE OF THE IP ADDRESSES ENTERED IS IN USE BY ANOTHER XPM IN THIS TABLE. | The user tries to add an IP address that is associated with another XPM in table XPMIPMAP. |
| ERROR: GATEWAY INDEX <#> IS NOT PRESENT IN TABLE XPMIPGWY. | The user tries to add a value for GWINDEX that is not datafilled in table XPMIPGWY. |
| ERROR: INVALID DNSNAME ENTERED. | The user tries to add an invalid value for DNS name. |
| ERROR: AT LEAST 1 DNS SRVADDRS MUST BE ENTERED. | The user tries to add a DNS name without an associated server IP address. |
| ERROR: AN INVALID IP ADDRESS FOR A SRVADDRS WAS ENTERED. | The user tries to add an invalid server IP address. |
| WARNING: ADDING OR CHANGING DATAFILL FOR AN INSERVICE XPM MAY CAUSE A STATIC DATA MISMATCH TO OCCUR. | The user tries to add or change datafill for an XPM that is in service. |
| ERROR: XPM IN USE BY TUPLE <#> IN TABLE IPCOMID. | The user tries to delete an XPM that has an associated COMID in table IPCOMID. |
| ERROR: DELETES NOT ALLOWED FOR AN INSERVICE XPM. | The user tries to delete an XPM that is in service. |

## IPSVCS

Table IPSVCS defines local IP transport services. Each service name represents a software port and transport protocol. The service name is referenced by table IPCOMID.

The switch can use port values in the range 2048 to 12287. Port numbers outside this range are reserved for non-CM IP applications. Port numbers in table IPSVCS must be unique, with the exception of port number 0. A port number of 0 is used to request the XPM to randomly assign a port number to the application. More than one application may datafill a 0 in the PORT field.

***Note 1:*** When an application uses a port of 0, the XPM randomly assigns a port in the range 32768 to 65535.

***Note 2:*** Port numbers 1 to 1024 are well-known industry-defined port numbers that are reserved for applications such as FTP (File Transfer Protocol), Telnet, and HTTP (Hypertext Transfer Protocol).

The following table shows the datafill specific to TOPS-IP for table IPSVCS.

**Table 19 Datafilling table IPSVCS**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| SERVICE | | Alphanumeric up to 16 characters | Service. Enter an IP transport service name. |
| PORT | | 0 and 2048 to 12287 | Port. Enter the software port number. This number reserves the same port on all IP-XPMs that are datafilled at the switch.<br>***Note 1:*** Refer to Chapter 7: “TOPS-IP engineering guidelines” for recommended port ranges for TOPS-IP applications.<br>***Note 2:*** QMS MIS-IP is the only TOPS-IP application that should use port number 0. |
| PROTOCOL | | UDP, TCP, or TCP_UDP | Protocol. Enter the protocol used for transport. |

## IPSVCS example

The following example shows datafill for several IP transport services. The services used for OC-IP and IP positions use the UDP protocol. QMSMIS uses the TCP protocol. XIPVER can use either TCP or UDP for testing data communication at the TOPS switch.

**Figure 117 MAP display example for table IPSVCS**

```
SERVICE           PORT       PROTOCOL
-----------------------------------------------------------------------
REMOTE1_IPSVC     8660       UDP
HOST1_IPSVC       8670       UDP
HOST2_IPSVC       8680       UDP
POSIPSVC          8700       UDP
QMSMIS            0          TCP
XIPVER            11777      TCP_UDP
```

## IPSVCS error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 20 Error messages for table IPSVCS**

| Error message | Explanation |
|---|---|
| `ERROR: THE VALID PORT RANGE IS 0 AND 2048 TO 12287.` | The user tries to add a value for PORT that is outside the valid range. |
| `ERROR: THE PORT SPECIFIED IS ALREADY IN USE.` | The user tries to add a duplicate value for PORT. Only a value of 0 may be duplicated. |
| `ERROR: THE PORT SPECIFIED IS ALREADY DATAFILLED` | The user tries to change the value for PORT to a value that is used by another service. |
| `ERROR: CHANGES TO THIS SERVICE ARE NOT CURRENTLY ALLOWED BY THE APPLICATION <application name>.` | The user tries to change a tuple, and the application does not allow it.<br>***Note:*** Each TOPS-IP application has its own rules for changing or deleting service datafill. For details, refer to information on the specific application. |

## IPCOMID

Table IPCOMID defines communication identifiers (COMID). Each COMID represents local connection information for TOPS-IP applications. This information includes the port and protocol (specified by the IP transport service name in table IPSVCS) and the name of the IP-XPM used for data communication.

The following table shows the datafill specific to TOPS-IP for table IPCOMID.

**Table 21 Datafilling table IPCOMID**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| COMID | | 0 to 1023 | Communication identifier. Enter the COMID. |
| SERVICE | | Service name from table IPSVCS | Service. Enter the name of the IP transport service.<br>***Note:*** A given service may be used by more than one COMID number, but only if the COMIDs are datafilled with different XPM names. |
| XPMNAME | | XPM type and number from table XPMIPMAP | XPM name. Enter the XPM type and number from table XPMIPMAP. |

## IPCOMID example

The following example shows datafill for nine IP COMIDs. REMOTE_IPSVC, HOST_IPSVC, POSIPSVC, and XIPVER distribute data communication over both DTC 10 and DTC 11. QMSMIS uses DTC 20.

**Figure 118 MAP display example for table IPCOMID**

```
COMID     SERVICE          XPMNAME
-----------------------------------------------------------
1         REMOTE1_IPSVC    DTC 10
2         REMOTE1_IPSVC    DTC 11
8         HOST1_IPSVC      DTC 10
9         HOST1_IPSVC      DTC 11
12        HOST2_IPSVC      DTC 10
13        HOST2_IPSVC      DTC 11
20        POSIPSVC         DTC 10
21        POSIPSVC         DTC 11
30        QMSMIS           DTC 20
40        XIPVER           DTC 10
41        XIPVER           DTC 11
```

### IPCOMID error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 22 Error messages for table IPCOMID**

| Error message | Explanation |
|---|---|
| ERROR: XPM IS NOT DATAFILLED IN TABLE XPMIPMAP. | The user tries to add a COMID for an XPM that is not datafilled in table XPMIPMAP. |
| ERROR: SERVICE AND XPM ALREADY DATAFILLED FOR COMID <#>. | The user tries to add values for SERVICE and XPMNAME that are used by another COMID. |
| ERROR: CHANGES TO THIS COMID ARE NOT CURRENTLY ALLOWED BY THE APPLICATION <application name>. | The user tries to change a COMID for the specified application. See Note. |
| ERROR: COMID DELETION IS NOT CURRENTLY ALLOWED SINCE IT IS IN USE BY AN APPLICATION <application name>. | The user tries to delete a COMID used by the specified application. See Note. |
| ***Note:*** Each TOPS-IP application has its own rules for changing or deleting a COMID. For details, refer to information on the specific application. | |

## CLLI

Table CLLI specifies the trunk group names and the maximum number of members in each trunk group. The value in field CLLI is referenced by the trunk group tables that specify voice links for TOPS-IP applications.

The following table shows the datafill specific to TOPS-IP for table CLLI.

**Table 23 Datafilling table CLLI**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| CLLI | | Alphanumeric up to 16 characters | Common language location identifier. Enter the CLLI name for the dynamic voice trunk groups used for the IP application. |
| ADNUM | | 0 to 8191 | Administrative number. Enter a unique administrative number associated with this CLLI. |
| TRKGRSIZ | | 0 to 2047 | Trunk group size. Enter the maximum number of members of the trunk group.<br>***Note:*** Entering a value higher than 2016 for trunk groups used for TOPS-IP applications wastes resources. |
| ADMININF | | Alphanumeric up to 32 characters | Administrative information. Enter your administrative information. |

### CLLI example

The following example shows datafill for a switch that uses two trunk groups (OCIPTOREMOTE and OCIPTOHOST) for OC-IP and one trunk group (POSIPVL) for hosted IP positions. In the example, CLLI OCIPTOHOST is used in an OC remote for connecting to the host's 7X07 Gateway when the host selects a TDM position for the call, and for connecting directly with the position when the host selects an IP position.

**Figure 119 MAP display example for table CLLI**

```
CLLI             ADNUM     TRKGRSIZ      ADMININF
-----------------------------------------------------------------
OCIPTOREMOTE     356       2016          OCIP_TOREMOTE_VOICE_LINK
OCIPTOHOST       367       2016          OCIP_TOHOST_VOICE_LINK
POSIPVL          484       2016          IP_POSITION_VOICE_LINK
```

## TRKGRP

Table TRKGRP specifies the trunk group type, direction, and other information for each trunk group. TOPS-IP trunks use the IT (intertoll) trunk group type. Table TRKOPTS, where trunk groups are defined as IP, enforces this restriction.

***Note:*** Translations and screening information in TRKGRP is not used for TOPS-IP dynamic voice trunks and should be datafilled with default values. No options should be datafilled in the OPTIONS subfield.

The following table shows the datafill specific to TOPS-IP for table TRKGRP. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 24 Datafilling table TRKGRP**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| GRPKEY | | CLLI name from table CLLI | Group key. Enter the CLLI for the trunk group. |
| GRPINFO | | See subfields | Group information. This field consists of subfield GRPTYP and refinements specific to the group type. |
| | GRPTYP | IT | Group type. Enter IT for intertoll and also datafill the DIRDATA refinement. |
| | DIRDATA | 2W, OG | Direction. Enter the direction of the traffic flow, as follows:<br>- Enter 2W for two-way (used for incoming).<br>- Enter OG for outgoing. |
| | SELSEQ | MIDL | Selection sequence. Enter MIDL. |

## TRKGRP example

The following example shows trunk information for the trunk groups defined in table CLLI.

**Figure 120 MAP display example for table TRKGRP**

```
GRPKEY          GRPINFO
-------------------------------------------------------------------
OCIPTOREMOTE IT 0 NPDGP NCRT 2W OA MIDL 000 NPRT NSCR 619 619 000 N N $
OCIPTOHOST   IT 0 NPDGP NCRT OG OA MIDL 000 NPRT NSCR 619 619 000 N N $
POSIPVL      IT 0 NPDGP NCRT OG OA MIDL 000 NPRT NSCR 619 619 000 N N $
```

## TRKGRP error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 25 Error messages for table TRKGRP**

| Error message | Explanation |
|---|---|
| `Table TRKOPTS DYNAMIC OC option is assigned. The trunk group direction must be OG or 2W.` | The user tries to change the direction of a trunk group that is defined as DYNAMIC OC in table TRKOPTS. Only 2W or OG are valid directions. |
| `Table TRKOPTS DYNAMIC POS option is assigned. The trunk group direction must be OG.` | The user tries to change the direction of a trunk group that is defined as DYNAMIC POS in table TRKOPTS. Only OG is a valid direction. |
| `Table TRKOPTS DYNAMIC OC or POS option is assigned. No options are allowed in table TRKGRP.` | The user tries to add options to a trunk group that is defined as DYNAMIC OC or POS in table TRKOPTS. No options are allowed. |
| `Table TRKOPTS DYNAMIC OC or POS option is assigned.The trunk group selection sequence must be MIDL or LIDL.` | The user tries to change the selection sequence for a trunk group that is defined as DYNAMIC OC or POS in table TRKOPTS. Only MIDL and LIDL are valid. MIDL is recommended. |

## TRKSGRP

Table TRKSGRP defines additional trunk group information such as signaling. TOPS-IP applications use dynamic trunking (ISUP trunks).

***Note:*** No options should be datafilled in the OPTIONS subfield.

The following table shows the datafill specific to TOPS-IP for table TRKSGRP. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 26 Datafilling table TRKSGRP**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| SGRPKEY | | See subfields | Subgroup key. This field consists of subfields CLLI and SGRP. |
| | CLLI | CLLI name from table TRKGRP | Subgroup key. Enter the CLLI for the trunk group. |
| | SGRP | 0 | Subgroup number. Enter 0. |
| CARDCODE | | DS1SIG | Card code. Enter DS1SIG. |
| SGRPVAR | | See subfield | Subgroup variable data. This field consists of subfield SIGDATA. |
| | SIGDATA | C7UP | Signaling data selector. Enter C7UP. |
| SGRPVAR | | See subfields | Subgroup variable data. This field consists of subfield DIR and refinements specific to the signaling selector (C7UP) and direction. |
| | DIR | 2W, OG | Direction. Enter the same direction for the subgroup as in table TRKGRP. Also datafill the PROTOCOL and COTREQ refinements.<br>***Note:*** Other refinement values are not used for TOPS-IP, but still require default datafill. |
| | PROTOCOL | Q764 | Protocol. Enter Q764. |
| | COTREQ | 0 | Continuity test required. Enter 0. |

### TRKSGRP example

The following example shows signaling information for the trunk groups datafilled in table TRKGRP.

**Figure 121 MAP display example for table TRKSGRP**

```
SGRPKEY          CARDCODE SGRPVAR  SGRPVAR
-------------------------------------------------------------------
OCIPTOREMOTE 0   DS1SIG C7UP 2W N N UNEQ NONE Q764 THRL 0 NIL $ NIL CIC
OCIPTOHOST 0     DS1SIG C7UP OG N N UNEQ NONE Q764 THRL 0 NIL $ NIL
POSIPVL  0       DS1SIG C7UP OG N N UNEQ NONE Q764 THRL 0 NIL $ NIL
```

## TRKSGRP error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 27 Error messages for table TRKSGRP**

| Error message | Explanation |
|---|---|
| `Table TRKOPTS DYNAMIC OC [or POS] option is assigned. The SGRPVAR must be C7UP.` | The user tries to change the signaling data selector for a trunk subgroup that is defined as DYNAMIC OC or POS in table TRKOPTS. Only C7UP is allowed. |
| `Table TRKOPTS DYNAMIC OC [or POS] option is assigned. The PROTOCOL must be Q764.` | The user tries to change the protocol for a trunk subgroup that is defined as DYNAMIC OC or POS in table TRKOPTS. Only Q764 is allowed. |
| `Table TRKOPTS DYNAMIC OC [or POS] option is assigned. Tuples for this CLLI must be deleted from Table TRKOPTS.` | The user tries to delete a tuple for a trunk subgroup that is defined as DYNAMIC OC or POS in table TRKOPTS. |
| `Table TRKOPTS DYNAMIC OC [or POS] option is assigned. Continuity checking is not supported; COTREQ must be 0.` | The user tries to change the continuity test requirement value for a trunk subgroup that is defined as DYNAMIC OC or POS in table TRKOPTS. Only 0 is allowed. |
| `Table TRKOPTS DYNAMIC OC option is assigned. The trunk group direction must be OG or 2W.` | The user tries to change the direction of a trunk subgroup that is defined as DYNAMIC OC in table TRKOPTS. Only 2W and OG are allowed. |
| `Table TRKOPTS DYNAMIC POS option is assigned. The trunk group direction must be OG.` | The user tries to change the direction of a trunk subgroup that is defined as DYNAMIC POS in table TRKOPTS. Only OG is allowed. |
| `Table TRKOPTS DYNAMIC OC [or POS] option is assigned. No options are allowed in table TRKSGRP.` | The user tries to add options to a trunk subgroup that is defined as DYNAMIC OC or POS in table TRKOPTS. No options are allowed. |

## TRKOPTS

Table TRKOPTS specifies additional trunk group options, including the dynamic option required by TOPS-IP voice trunks. Datafill in TRKOPTS is used to define entire trunk groups as IP trunks.

The following table shows the datafill specific to TOPS-IP for table TRKOPTS.

**Table 28 Datafilling table TRKOPTS**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| OPTKEY | | See subfields | Option key. This field consists of subfields CLLI and OPTION. |
| | CLLI | CLLI name from table TRKSGRP | CLLI. Enter the CLLI for the trunk group. |
| | OPTION | DYNAMIC | Option. Enter DYNAMIC. |
| OPTINFO | | See subfields | Option information. Enter the DYNAMIC option and datafill its refinements. |
| | SIGNALING | ISUP | Signaling. Enter ISUP. |
| | SIGNALING_ NETWORK | IP | Signaling network. Enter IP. |
| | BEARER_ NETWORK | IP | Bearer network. Enter IP |
| | APPLICATION | OC, POS | Application. Enter the TOPS-IP application for the trunk group, as follows:<br>- OC is used for all OC-IP remote calls, regardless of the type of position selected by the host. OC is also used in OC hosts for IP voice connections to remotes (used only when the host selects a TDM position).<br>- POS is used in a standalone or OC host switch, for trunks that connect to IP positions on standalone or TDM OC calls.<br>***Note:*** TDM OC links must be replaced by OC-IP links. |

### TRKOPTS example

The following example shows the trunk options for the dynamic trunk groups.

**Figure 122 MAP display example for table TRKOPTS**

```
OPTKEY                 OPTINFO
-------------------------------------------------------------
OCIPTOREMOTE DYNAMIC   DYNAMIC ISUP IP IP OC
OCIPTOHOST DYNAMIC     DYNAMIC ISUP IP IP OC
POSIPVL DYNAMIC        DYNAMIC ISUP IP IP POS
```

## TRKOPTS error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 29 Error messages for table TRKOPTS**

| Error message | Explanation |
|---|---|
| `ERROR: Changes not allowed for tuples with the DYNAMIC option.` | The user tries to change a tuple for a DYNAMIC trunking application. |
| `For the TOPS-IP OC [or POS] dynamic trunking application: Tuples for this CLLI must be deleted from Table IPINV.` | The user tries to delete or add a tuple for a DYNAMIC trunking application that has datafill in table IPINV. |
| `For the TOPS-IP OC dynamic trunking application: Tuples for this CLLI must be deleted from Table OCGRP.` | The user tries to delete or add a tuple for the DYNAMIC OC trunking application that has datafill in table OCGRP. |
| `For the TOPS-IP POS dynamic trunking application: Tuples for this CLLI must be deleted from Table TOPSPOS.` | The user tries to delete or add a tuple for the DYNAMIC POS trunking application that has datafill in table TOPSPOS. |
| `TOPS dynamic trunks are not supported in this load.` | The user tries to add a tuple for a DYNAMIC trunk group when the software load does not contain CCM (DMS100 common software). |
| `For the TOPS-IP OC [or POS] dynamic trunking application: The trunk group type must be IT.` | The user tries to add a DYNAMIC tuple whose group type is not IT in table TRKGRP. |
| `For the TOPS-IP OC [or POS] dynamic trunking application: Only trunk subgroup 0 is allowed.` | The user tries to add a DYNAMIC tuple whose subgroup is 1 in table TRKSGRP. |
| `For the TOPS-IP OC [or POS] dynamic trunking application: Trunk subgroup 0 must be datafilled for this CLLI in Table TRKSGRP.` | The user tries to add a DYNAMIC tuple whose subgroup is not datafilled in table TRKSGRP. |
| `For the TOPS-IP OC dynamic trunking application: The trunk group direction must be OG or 2W.` | The user tries to add a DYNAMIC OC tuple whose direction is not OG or 2W. |
| `For the TOPS-IP POS dynamic trunking application: The trunk group direction must be OG.` | The user tries to add a DYNAMIC POS tuple whose direction is not OG. |

**Table 29 Error messages for table TRKOPTS**

| Error message | Explanation |
|---|---|
| For the TOPS-IP OC [or POS] dynamic trunking application: The SGRPVAR must be C7UP. | The user tries to add a DYNAMIC tuple whose subgroup variable is not C7UP in table TRKSGRP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: The PROTOCOL must be Q764. | The user tries to add a DYNAMIC tuple whose protocol is not Q764 in table TRKSGRP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: Continuity checking is not supported; COTREQ must be 0. | The user tries to add a DYNAMIC tuple whose continuity test requirement is not 0 in table TRKSGRP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: Tuples for this CLLI must be deleted from Table TRKMEM. | The user tries to add a DYNAMIC tuple whose CLLI is present in table TRKMEM. |
| For the TOPS-IP OC [or POS] dynamic trunking application: Tuples for this CLLI must be deleted from Table ISUPDEST. | The user tries to add a DYNAMIC tuple whose CLLI is present in table ISUPDEST. |
| For the TOPS-IP OC [or POS] dynamic trunking application: SIGNALING attribute must be ISUP. | The user tries to add a DYNAMIC tuple whose signaling attribute is not ISUP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: SIGNALING_NETWORK attribute must be IP. | The user tries to add a DYNAMIC tuple whose signaling network is not IP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: BEARER_NETWORK attribute must be IP. | The user tries to add a a DYNAMIC tuple whose bearer network is not IP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: No options are allowed in Table TRKGRP. | The user tries to add a a DYNAMIC tuple that has options assigned in table TRKGRP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: No options are allowed in Table TRKSGRP. | The user tries to add a a DYNAMIC tuple that has options assigned in table TRKSGRP. |
| For the TOPS-IP OC [or POS] dynamic trunking application: The trunk group selection sequence must be MIDL or LIDL. | The user tries to add a DYNAMIC tuple whose selection sequence is not MIDL or LIDL in table TRKGRP. (MIDL is recommended.) |

## SITE

Table SITE identifies a site name associated with the 7X07 Gateway cards datafilled at the switch. The value in field NAME is referenced by table IPINV as well as by application-specific tables.

***Note:*** The Gateway card does not refer in any way to a gateway router. A gateway router is a component of the managed IP network and is used to forward IP packets to other networks.

The following table shows the datafill specific to TOPS-IP for table SITE.

**Table 30 Datafilling table SITE**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| NAME | | 4 alphanumeric characters | Site name. Enter the site name associated with the Gateway cards. The first character must be alphabetical. |
| LTDSN | | 0 | Line equipment number site number. Enter 0. |
| MODCOUNT | | 0 | Module count. Enter 0. The system updates the value to reflect the number of Gateway cards on the site. |
| OPVRCLLI | | VER90 | Operator verification CLLI. Enter VER90. |
| ALMDATA | | $ | Alarm data. Enter $. |

### SITE example

The following example shows datafill for site name TGWY. Additional fields in SITE are unused and should be set to default values.

***Note:*** After table IPINV is datafilled, the system automatically updates the MODCOUNT field to reflect the number of Gateway cards on the site.

**Figure 123 MAP display example for table SITE**

```
NAME   LTDSN  MODCOUNT OPVRCLLI ALMDATA
-------------------------------------------------------
TGWY   0      0        VER90    $
```

## IPINV

Table IPINV defines the individual 7X07AA Gateway cards at the switch. Datafill values include the Gateway site name, frame, and unit number; the associated IP-XPM; primary IP address; the type of Gateway (such as TOPS); and Gateway-specific refinements, such as the associated trunk group and the starting trunk member number.

***Note 1:*** When a TOPS entry is added to table IPINV, trunk members are automatically datafilled in table TRKMEM (page 253). Removing TOPS entries from table IPINV automatically removes the associated TRKMEM members. Table TRKMEM does not allow members associated with a Gateway card to be manually added or removed.

***Note 2:*** Each DTC port supports 24 channels, whereas the 7X07 Gateway supports 48. When a Gateway card is datafilled in table IPINV, 24 channels are allocated against the port number in the tuple, and another 24 channels are allocated against the next port number (PORT + 1). To prevent inadvertent overlap, only even port numbers may be datafilled in the PORT field for TOPS Gateways. Refer to Table 32 on page 249 for information on how to map the P-side links that are datafilled in table LTCPSINV to port numbers for IPINV.

***Note 3:*** Trunk groups typically have a maximum of 2048 members. Since IPINV allocates 48 members at a time, this maximum is limited to 2016 for dynamic trunk groups used for TOPS-IP. 2016 is the highest multiple of 48 that is less than 2048.

The following table shows the datafill specific to TOPS-IP for table IPINV.

**Table 31 Datafilling table IPINV**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| IPNO | | See subfields | IP number. This field consists of subfields SITE, FRAME, and UNIT. |
| | SITE | SITE name from table SITE | Site. Enter the site name (from table SITE) associated with the TOPS-IP 7X07AA Gateway cards. |
| | FRAME | 0 to 511 | Frame. Enter the frame number. |
| | UNIT | 0 to 9 | Unit. Enter the unit number. This identifies the specific 7X07 Gateway, and does not refer to the unit of the IP-XPM. |
| PMTYPE | | XPM type from table LTCINV | Peripheral module type. Enter the XPM type (DTC). |
| PMNO | | XPM number from table LTCINV | PM number. Enter the XPM number. |

**Table 31 Datafilling table IPINV**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| IPPEC | | 7X07AA | IP PEC. Enter 7X07AA for the Gateway card. |
| LOAD | | Alphanumeric up to 19 characters | Load. Enter $, because this field is not currently used. |
| PORT | | 0 to 18 | Port. Enter an even number that corresponds to the DS1 P-side link pair assigned to the 7X07 Gateway card in table LTCPSINV (page 226). Refer to Table 32 on page 249. |
| IPZONE | | See subfields | IP zone. This field consists of subfields PRIMARY and SECONDARY. |
| | PRIMARY | IP address of 4 octets from 0 to 255 | Enter a primary IP address for the Gateway card.<br>***Note:*** This field must contain the same IP address that is assigned to the Gateway by the DHCP server. Any mismatch between DHCP datafill and CM datafill for a Gateway will prevent the Gateway from coming into service. |
| | SECONDARY | IP address of 4 octets from 0 to 255 | Secondary IP address. The secondary IP address is unused and should be datafilled with 0 0 0 0. |
| GWTYPE | | See subfields | Gateway type. This field consists of subfield GWTYPE and refinements specific to the type. |
| | GW_TYPE | TOPS | Gateway type. Enter TOPS and datafill the TRKCLLI and MEMSTART refinements. |
| | TRKCLLI | CLLI name from table TRKOPTS | Trunk CLLI. Enter the CLLI name for the trunk group. The CLLI must be defined as DYNAMIC in table TRKOPTS. |
| | MEMSTART | 0 or multiple of 48 less than 2047 | Trunk member. Enter the start of a 48-member block, beginning with 0 or a multiple of 48. |

## LTCPSINV-to-IPINV port mapping

Refer to Table 32 for the correct port mapping.

***Note:*** Until the correct port datafill is present, the switch will generate PM777 log reports.

**Table 32 LTCPSINV-to-IPINV port mapping**

| LTCPSINV subfield PSLINK | IPINV field PORT |
|---|---|
| 0,1 | 0 |
| 2, 3 | 2 |
| 4, 5 | 4 |
| 6, 7 | 6 |
| 8, 9 | 8 |
| 10, 11 | 10 |
| 12, 13 | 12 |
| 14, 15 | 14 |
| 16, 17 | 16 |
| 18, 19 | 18 |

## IPINV example

The following example shows datafill for seven Gateway cards, all using the TGWY site from table SITE. Two trunk groups are datafilled for OC-IP: OCIPTOREMOTE with 96 members, and OCIPTOHOST with 144 members. One trunk group is datafilled for IP positions: POSIPVL with 96 members.

***Note:*** Users can number the Gateways in the IPNO field with the following method (as shown in the figure): FRAME represents the DTC number and UNIT represents the port number (in the PORT field) divided by two. So for example, TGWY 10 3 is datafilled on DTC 10, PORT 6 (and so on).

**Figure 124 MAP display example for table IPINV**

```
IPNO       PMTYPE  PMNO IPPEC  LOAD PORT  IPZONE                GWTYPE
-------------------------------------------------------------------------------
TGWY 10 3  DTC     10   7X07AA  $    6     47 192 3 100 0 0 0 0  TOPS OCIPTOREMOTE 0
TGWY 10 4  DTC     10   7X07AA  $    8     47 192 3 101 0 0 0 0  TOPS OCIPTOHOST 0
TGWY 10 5  DTC     10   7X07AA  $    10    47 192 3 102 0 0 0 0  TOPS OCIPTOHOST 48
TGWY 10 6  DTC     10   7X07AA  $    12    47 192 3 103 0 0 0 0  TOPS POSIPVL 1920
TGWY 11 3  DTC     11   7X07AA  $    6     47 192 3 110 0 0 0 0  TOPS OCIPTOHOST 96
TGWY 11 4  DTC     11   7X07AA  $    8     47 192 3 111 0 0 0 0  TOPS OCIPTOREMOTE 48
TGWY 11 5  DTC     11   7X07AA  $    10    47 192 3 112 0 0 0 0  TOPS POSIPVL 1968
```

## IPINV error and information messages

The following table lists possible error and information messages related to adding, changing, or deleting tuples.

**Table 33 Error and information messages for table IPINV**

| Error message | Explanation |
|---|---|
| `ERROR: Port must be an even number.` | The user tries to add a Gateway card whose PORT is not an even number. |
| `ERROR: IPGW must be offl to delete tuple.` | The user tries to delete a Gateway card that is not in the OFFL state. |
| `ERROR: Associated trunk members not INB.` | The user tries to delete a Gateway card that has been off-lined but whose 48 trunk members have not yet transitioned to the installation busy (INB) state. Wait a moment and retry the delete command. |
| `ERROR: Cside links must be MBsy or Offl to delete tuple.` | The user tries to delete a Gateway card while its C-side links are still in service. Manually busy the C-side links to the Gateway card before retrying the deletion.<br>***Note:*** To determine the C-side links in question, check the PORT field for the Gateway in table IPINV. The links are represented by ports n and n+1. Next, busy the links by posting the DTC at the PM level and issuing the BSY command for each link. |
| `ERROR: CLLI not assigned DYNAMIC option in Table TRKOPTS.` | The user tries to add a tuple whose CLLI is not DYNAMIC in table TRKOPTS. |
| `ERROR: CLLI not datafilled in Table TRKGRP.` | The user tries to add a tuple whose CLLI is not datafilled in table TRKGRP. |
| `ERROR: PMTYPE, PMNO, and PORT combination already datafilled.` | The user tries to add a tuple whose PM type, number, and port are already present. |
| `ERROR: Host PM must be a DTC for the TOPS variant.` | The user tries to add a tuple whose PM type is not DTC. |
| `ERROR: PORT must be in range 0 to 18.` | The user tries to add a tuple whose port is outside of the 0 to 18 range. |
| `ERROR: TRKCLLI and MEMSTART combination already datafilled.` | The user tries to add a tuple whose TRKCLLI and MEMSTART combination are already present. |
| `ERROR: MEMSTART must not be greater than 1968.` | The user tries to add a tuple whose MEMSTART value is greater than 1968. The maximum member number is 2015, so the maximum starting number is 1968. |
| `ERROR: MEMSTART not 0 or a multiple of 48.` | The user tries to add a tuple whose MEMSTART value is not 0 or a multiple of 48. |

**Table 33 Error and information messages for table IPINV**

| Error message | Explanation |
|---|---|
| INFO: The next lower available MEMSTART for this TRKCLLI is <num>. | The next lower available MEMSTART value for this TRKCLLI is specified. |
| INFO: No lower MEMSTART is available for this TRKCLLI. | No lower MEMSTART value is available for this TRKCLLI. |
| INFO: The next higher available MEMSTART for this TRKCLLI is <num>. | The next higher available MEMSTART value for this TRKCLLI is specified. |
| INFO: No higher MEMSTART is available for this TRKCLLI. | No higher MEMSTART value is available for this TRKCLLI. |
| ERROR: For TOPS gateway type, only field LOAD may be changed. | The user tries to change a TOPS tuple. |
| ERROR: CLLI assigned DYNAMIC option in Table TRKOPTS. | The user tries to add a non-TOPS Gateway type using a DYNAMIC CLLI in table TRKOPTS. |
| Cannot add any more trunk groups to internal table. Reuse an existing CLLI name in Table IPINV.<br>ERROR: Operation disallowed by TOPS checks. | The user tries to exceed the number trunk groups that can be associated with the application. The current maximum is 409. |
| Could not allocate store.<br>ERROR: Operation disallowed by TOPS checks. | The store could not be allocated for the table control request. Follow standard procedures for increasing the amount of store available to table control. |
| Unable to allocate IPINV store.<br>ERROR: Operation disallowed by TOPS checks. | The store could not be allocated for the table control request. Follow standard procedures for increasing the amount of store available to table control. |
| INFO: This IPGW will be used for TOPS OC-IP remote processing. | The user adds a tuple that will be used for OC-IP remote processing. |
| INFO: This IPGW will be used for TOPS OC-IP host processing | The user adds a tuple that will be used for OC-IP host processing. |
| WARNING: In an OC host, field IPZONE: PRIMARY must contain a valid IP address. | The user tries to add a tuple whose PRIMARY IP address value is not valid. |

**Table 33 Error and information messages for table IPINV**

| Error message | Explanation |
|---|---|
| `Internal mapping errors. Please run the IPL code of module YOCIPGWT, then perform a nil change on all TOPS tuples in Table IPINV. While performing nil changes, all calls for which this switch is a NON-BYPASS OC-IP HOST will FAIL. Other call types will be unaffected. Contact Nortel Networks for assistance.`<br>`ERROR: Operation disallowed by TOPS checks.` | If the internal IPGW mapping has become corrupted (as evidenced by the appearance of a mapping error message), the operating company can rebuild the mapping by positioning on each TOPS IPGW tuple in table IPINV and performing a nil change. SWERs (software errors) are generated from module YOCIPGWT when rebuilding the mapping. Successful rebuilding results in SWERs with reasons in the range #20-#2F, while unsuccessful SWERs have reasons in the range #10-#1F. Contact Nortel Networks for assistance when performing this operation. |
| `Problem clearing internal trunk group to IPGW mapping.` | Contact Nortel Networks technical support. |
| `Trunk group to IPGW mapping error.` | Contact Nortel Networks technical support. |

## TRKMEM

Table TRKMEM defines the individual trunk members associated with a trunk group. In the case of trunks defined as DYNAMIC in table TRKOPTS and used for TOPS-IP applications, manual datafill in TRKMEM is not allowed because tuples are *automatically* datafilled by table IPINV (page 247) when a Gateway card is datafilled. Table IPINV datafills the members in blocks of 48.

The following table shows the datafill specific to TOPS-IP for table TRKMEM.

**Table 34 Datafilling table TRKMEM**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| CLLI | | CLLI name from table TRKOPTS | CLLI. Automatically datafilled for dynamic trunks. |
| EXTRKNM | | 0 to 2015 | Trunk member. Automatically datafilled for dynamic trunks. |
| SGRP | | 0 | Subgroup. Automatically datafilled for dynamic trunks. |
| MEMVAR | | See subfields | Member variables. This field consists of subfield PMTYPE and refinements specific to the PM type. |
| | PMTYPE | DTC | PM type. Automatically datafilled for dynamic trunks. |
| | DTCNO | 0 to 511 | DTC number. Automatically datafilled for dynamic trunks. |
| | DTCCKTNO | 0 to 19 | DTC circuit number. Automatically datafilled for dynamic trunks. |
| | DTCCKTTS | 1 to 24 | DTC circuit time slot. Automatically datafilled for dynamic trunks. |

### TRKMEM example

The following example shows some of the 192 trunk members that would be automatically datafilled by table IPINV for DTC 10, for the example IPINV datafill on page 249.

**Figure 125 MAP display example for table TRKMEM**

```
CLLI           EXTRKNM  SGRP  MEMVAR
-------------------------------------------------
OCIPTOREMOTE   0        0     DTC 10 6 1
OCIPTOREMOTE   1        0     DTC 10 6 2
...
OCIPTOREMOTE   23       0     DTC 10 6 24
OCIPTOREMOTE   24       0     DTC 10 7 1
...
OCIPTOREMOTE   47       0     DTC 10 7 24
OCIPTOHOST     0        0     DTC 10 8 1
...
OCIPTOHOST     47       0     DTC 10 9 24
OCIPTOHOST     48       0     DTC 10 10 1
...
OCIPTOHOST     95       0     DTC 10 11 24
POSIPVL        1920     0     DTC 10 12 1
POSIPVL        1921     0     DTC 10 12 2
...
POSIPVL        1967     0     DTC 10 13 24
```

## TRKMEM error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 35 Error messages for table TRKMEM**

| Error message | Explanation |
|---|---|
| `Table TRKOPTS DYNAMIC OC [or POS] option is assigned. Manual operations are not allowed in Table TRKMEM.TRKMEM data conflicts with data in table TRKOPTS.` | The user tries to change or delete a member of a trunk group that is defined as DYNAMIC OC or DYNAMIC POS in table TRKOPTS. |

## TOPSTOPT

Table TOPSTOPT specifies options for TOPS trunk groups. Although TOPS-IP dynamic trunk groups are datafilled and maintained in blocks of 48 trunks, users can reduce the number of dynamic trunks that are available for call processing. The MAXCONNS field in table TOPSTOPT specifies the maximum number of trunks per trunk group that may be used by call processing. This value applies only to dynamic trunk groups.

If the MAXCONNS function is not desired for a TOPS-IP dynamic trunk group, either the trunk group should be deleted from table TOPSTOPT or its MAXCONNS value should be set to 2016. This will avoid unnecessary CPU real-time consumption on each TOPS-IP call.

***Note:*** For more information, refer to "Limiting the use of dynamic voice links" on page 200.

The following table shows the datafill specific to TOPS-IP for table TOPSTOPT. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 36 Datafilling table TOPSTOPT**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| GRPKEY | | CLLI name from table TRKOPTS | Group key. Enter the CLLI name for the trunk group. |
| MAXCONNS | | 0 to 32767 | Maximum connections. Enter the maximum number of voice connections supported by this dynamic trunk group.<br>***Note 1:*** A value of 0 specifies no connections allowed for that trunk group, if it. is defined as DYNAMIC in table TRKOPTS.<br>***Note 2:*** For TOPS-IP dynamic trunks, the effective maximum for this field is 2016 members. Datafilling MAXCONNS with a value greater than 2016 has no effect. |

## TOPSTOPT example

The following example shows datafill for the three trunk groups.

**Figure 126 MAP display example for table TOPSTOPT**

```
GRPKEY    ORGAREA  DISPCLG  ADASERV  ADASANS  ANITOCLI  OLNSQRY  DCIBIDX
  LNPCLGAM     XLASCHEM  SPIDPRC  TRKSPID  BILLSCRN  ANIFSPL  MAXCONNS  DISPSPID
-------------------------------------------------------------------------------
OCIPTOREMOTE N      N       NONE      NA        N         NONE        0
  N              N         N         N         N         N       48        N
OCIPTOHOST   N      N       NONE      NA        N         NONE        0
  N              N         N         N         N         N       96        N
POSIPVL      N      N         NONE    NA        N         NONE        0
  N              N         N         N         N         N       48        N
```

## TOPSTOPT error messages

The following table lists possible warning and error messages related to adding, changing, or deleting tuples.

**Table 37 Warning and Error messages for table TOPSTOPT**

| Warning or Error message | Explanation |
|---|---|
| `Trunk group not marked as a dynamic trunking application in Table TRKOPTS. MAXCONNS must be 0.` | The user tries to increase the MAXCONNS value for a trunk group that is not defined as DYNAMIC. These trunk groups do not use the MAXCONNS field, and table control requires that it be datafilled as 0. |
| `Warning: MAXCONNS is set to 0. No connections will be allowed on this trunk group.` | The user changes the MAXCONNS value to 0 for a DYNAMIC trunk group. A value of 0 does not allow the trunk group to make connections. |
| `Warning: MAXCONNS is set higher than the maximum per trunk group. A maximum of 2016 connections will be used by call processing.` | The user increases the MAXCONNS value to greater than 2016 connections, which is the effective maximum for dynamic trunk groups. |
| `Warning: TOPS VoIP usage limits are not supported in this load. MAXCONNS will be set to the maximum per trunk group, which is 2016.` | The user changes the MAXCONNS value when voice over IP usage limits are not supported in the switch software. (MAXCONNS functionality requires the CCM DRU.). The value is set to 2016, and voice over IP usage limits will not be used. |

## OFCENG

Table OFCENG contains office-wide parameters. The following table shows the datafill relevant to TOPS-IP for table OFCENG.

**Table 38 Datafilling table OFCENG**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| IPGW_PCM_SELECTION | AUTO, MANUAL | AUTO | This parameter specifies the speech companding law and bit inversion pattern on the 7X07 Gateway cards' C-side links. In all standard office configurations, the value of this parameter should be set to AUTO (default).<br>***Note*:** Any change in the value of this parameter requires the Gateway card to be reloaded. |
| IPGW_SNMP_COMMUNITY_NAME | One to sixteen letters, digits, non-alphanumeric symbols, or any combination thereof | public | This parameter specifies the Internet Protocol Gateway Simple Network Management Protocol Community Name. The craftsperson can configure one SNMP community name for SNMP read, write, and trap operations on the 7X07AA.<br>***Note:*** The new community name does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. For all cards to be updated, all cards must be PMRESET. This should be done sequentially using the existing IPGW DRAIN command. |

**Table 38 Datafilling table OFCENG**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| IPGW_SNMP_MANAGER | Y,N | N (no manager datafilled) | This parameter specifies the Internet Protocol Gateway Simple Network Management Protocol Manager. The craftsperson can configure the IP address of one SNMP manager (also known as a trap manager). The 7X07AA cards will send traps to this IP address.<br>***Note1:*** If IPGW_SNMP_MANAGER is set to Y, a second field, IPADDR, appears. The craftsperson datafills the IP address of the SNMP manager. For example, IP address 47.142.225.193 would be datafilled as: Y 47 142 225 193<br>**Note2:** The new SNMP manager does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. |
| IPGW_SNMP_ENABLED | Y,N | N | This parameter specifies the Internet Protocol Gateway Simple Network Management Protocol Enabled. This allows the craftsperson to enable or disable SNMP on the 7X07AA.<br>***Note1:*** Defaults to N unless TOPS IPGWs are present in Table IPINV on the pre-SN09 dump side, in which case this parameter defaults to Y.<br>**Note2:** The new SNMP manager does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. |
| IPGW_TELNET_ENABLED | Y,N | N | This parameter specifies the Internet Protocol Gateway Telnet Enabled. This allows the craftsperson to enable or disable Telnet on the 7X07AA.<br>***Note 1:*** Default is N.<br>***Note 2:*** If the telco is not using Telnet on the 7X07, this parameter should be set to N. |

**Table 38 Datafilling table OFCENG**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| NUMCALLPROCESSES | 1 to 2000 | 70 | This parameter allocates call processes, a software resource that uses memory. More call processes are needed in a switch that hosts IP positions than in one that hosts TDM positions.<br><br>The exact number needed depends on many factors besides just the number of IP positions. The following existing OMs are useful in monitoring usage and availability of call processes: CP_CPSZ/CPSZ2 (seizures), and CP2_CPHI (high water mark). |
| NUMCPWAKE | 1 to 65535 | 2000 (XA-Core) | This parameter allocates call processing wakeup blocks, a software resource that uses memory. More wakeup blocks are needed in a switch that hosts IP positions than in one that hosts TDM positions.<br><br>The exact number needed depends on many factors besides just the number of IP positions. The following existing OMs are useful in monitoring usage and availability of CP wakeup blocks: CP_WAKESZ/WAKESZ2 (seizures), and CP2_WAKEHI (high water mark). |
| NUMPERMEXT | 0 to 32767 | 1 | This parameter allocates data structures for calls. It specifies the number of permanent extension blocks. For TOPS-IP, this value should be incremented by one for each member of each dynamic trunk group, except it does not need to be incremented for dynamic trunk members in OC hosts that are used to connect to OC remotes.<br><br>***Note:*** NUMPERMEXT does not appear in table OFCENG if it is automatically provisioned in table OFCAUT. |

**Table 38 Datafilling table OFCENG**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| TOPS_NUM_OC_EXT | 0 to 32767 | 100 | This parameter allocates data structures for calls. It specifies the number of OC extension blocks. These are used for OC host calls. One OC extension block is needed for each OC host call that is either at position or queued for an operator. None are needed in a pure OC remote or standalone office. (See Note.) |
| TOPS_OC_ENVIRONMENT | HOST, REMOTE | HOST | This parameter specifies whether the switch is an OC host or an OC remote. It is not typically consulted when HRNQT is used. (See Note.) |
| ***Note:*** TOPS-IP does not change the datafill required for this parameter. | | | |

## OFCENG example

The following figure shows example datafill for the OFCENG parameters.

**Figure 127 MAP display example for table OFCENG**

```
PARMNAME                    PARMVAL
------------------------------------------------------------
IPGW_PCM_SELECTION          AUTO
NUMCALLPROCESSES            2000
NUMCPWAKE                   2800
NUMPERMEXT                  244
TOPS_NUM_OC_EXT             1000
TOPS_OC_ENVIRONMENT         HOST
```

## PKTVPROF

Table PKTVPROF defines profiles used for packetized voice. The profile index identifies the tuple, and is referenced by application tables such as TQCQINFO. The other fields specify the codec for calls that use the profile. A primary codec is always datafilled. A selector allows each profile to specify whether it supports auto-compression. If the profile supports auto-compression, a compressing codec is also datafilled.

For auto-compression to be used, the profile must support it and the IP voice connection must be to an IP position. OC-IP calls that use TDM positions always use the codec datafilled in the CODEC field; they are not eligible for auto-compression even if the profile supports it.

***Note:*** Refer to "Voice encoding and auto-compression" on page 117 for more information about auto-compression.

The following table shows the datafill specific to TOPS-IP for table PKTVPROF.

**Table 39 Datafilling table PKTVPROF**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| PROFNUM | | 0 to 63 | Profile number. Enter the profile index. |
| CODEC | | G711, G723 | Codec. Enter the voice codec for the profile. If the USEAC field is Y, enter G711 in the CODEC field.<br>If the USEAC field is N, enter G711 in the CODEC field for uncompressed voice, or G723 for compressed voice. |
| AUTOCOMP | | See subfields | Auto-compression. This field contains subfield USEAC and refinements specific to the value entered. |
| | USEAC | Y, N | Use auto-compression. Enter Y to indicate that the profile supports auto-compression, and also datafill refinement ACCODEC. Enter N to indicate that the profile does not support auto-compression. |
| | ACCODEC | G723 | Auto-compression codec. This refinement field is present only when USEAC=Y. Enter G723. |

### PKTVPROF error messages

The following table lists possible error messages related to adding or changing tuples.

**Table 40 Error messages for table PKTVPROF**

| Error message | Explanation |
|---|---|
| G729 is no longer supported as a CODEC. | The user tries to enter G729 in the CODEC or ACCODEC field. Although G729 still appears in the ranges of these fields, it is no longer supported and cannot be datafilled. |
| G729 is no longer supported as an ACCODEC. | |
| ACCODEC must provide more compression than CODEC. | The user tries to datafill a profile that supports auto-compression, but the ACCODEC provides no more compression than the CODEC. This is not allowed. |

***Note:*** Table PKTVPROF contains two default tuples, 0 and 1.

### PKTVPROF example

The following example shows datafill for three packetized voice profiles.

**Figure 128 MAP display example for table PKTVPROF**

```
PROFNUM  CODEC   AUTOCOMP
------------------------------------------------------------------------
0        G711    N
1        G723    N
2        G711    Y G723
```

### Pre-TOPS19 considerations for table PKTVPROF

Table PKTVPROF was significantly changed in TOPS19. Changes in the field names and ranges were not patched to earlier loads. However, patch CFX84 changes the interpretation of the fields in the earlier data schema. Refer to “Table PKTVPROF prior to TOPS19” on page 70 for an explanation.

In an ONP from a pre-TOPS19 load to TOPS19 or later, table PKTVPROF is populated as shown in the following table. This preserves the same codec use after the ONP, as before the ONP with CFX84 applied.

**Table 41 Population of table PKTVPROF over ONP from pre-TOPS19 to TOPS19 or higher**

| FROM side field PKTVFLDS | FROM side status of patch CFX84 | TO side fields CODEC and AUTOCOMP |
|---|---|---|
| G711 | activated | G711 Y G723 |
| G711 | not activated | G711 N |
| G729 NOSILSUP<br>- or -<br>G729 SILSUP | activated or not activated | G723 N |

## TQCQINFO

Table TQCQINFO provides information about TOPS call queues, including the packetized voice profile index that applies to the call queue for OC-IP and IP position calls. This is really an application table, but it is discussed with the infrastructure tables because two applications use it.

The switch that initiates the IP voice connection is the one that consults tables TQCQINFO and PKTVPROF to find the codec information. For an OC-IP call this is always the OC remote, regardless of whether the position is TDM or IP. For a TDM-OC call with an IP position, this is always the OC host.

The following table shows the datafill specific to TOPS-IP for table TQCQINFO. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 42 Datafilling table TQCQINFO**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| PKTVPROF | | Profile number from table PKTVPROF | Packetized voice profile. Enter the profile number that applies to the call queue. |

### TQCQINFO example

The following example shows datafill for three packetized voice profile indexes against call queues.

**Figure 129 MAP display example for table TQCQINFO**

```
QTYPE   QMSSERV   CWOFF   CWON    TREAT ALTAREA PKTVPR0F
-----------------------------------------------------------
CQ131   TOPS_TA   500     1000    VACT    N         0
CQ132   TOPS_TA   500     1000    VACT    N         1
CQ133   TOPS_TA   500     1000    VACT    N         2
```

## OC-IP datafill

Datafill in the OC-IP tables specifies IP data and voice connectivity for OC hosts and OC remotes.

***Note:*** The OC-IP application depends on the IP infrastructure, so datafill is *first* required in all the tables described in "IP infrastructure datafill" beginning on page 219.

### Table datafill dependencies

The following OC-IP tables are listed in the order in which they should be datafilled.

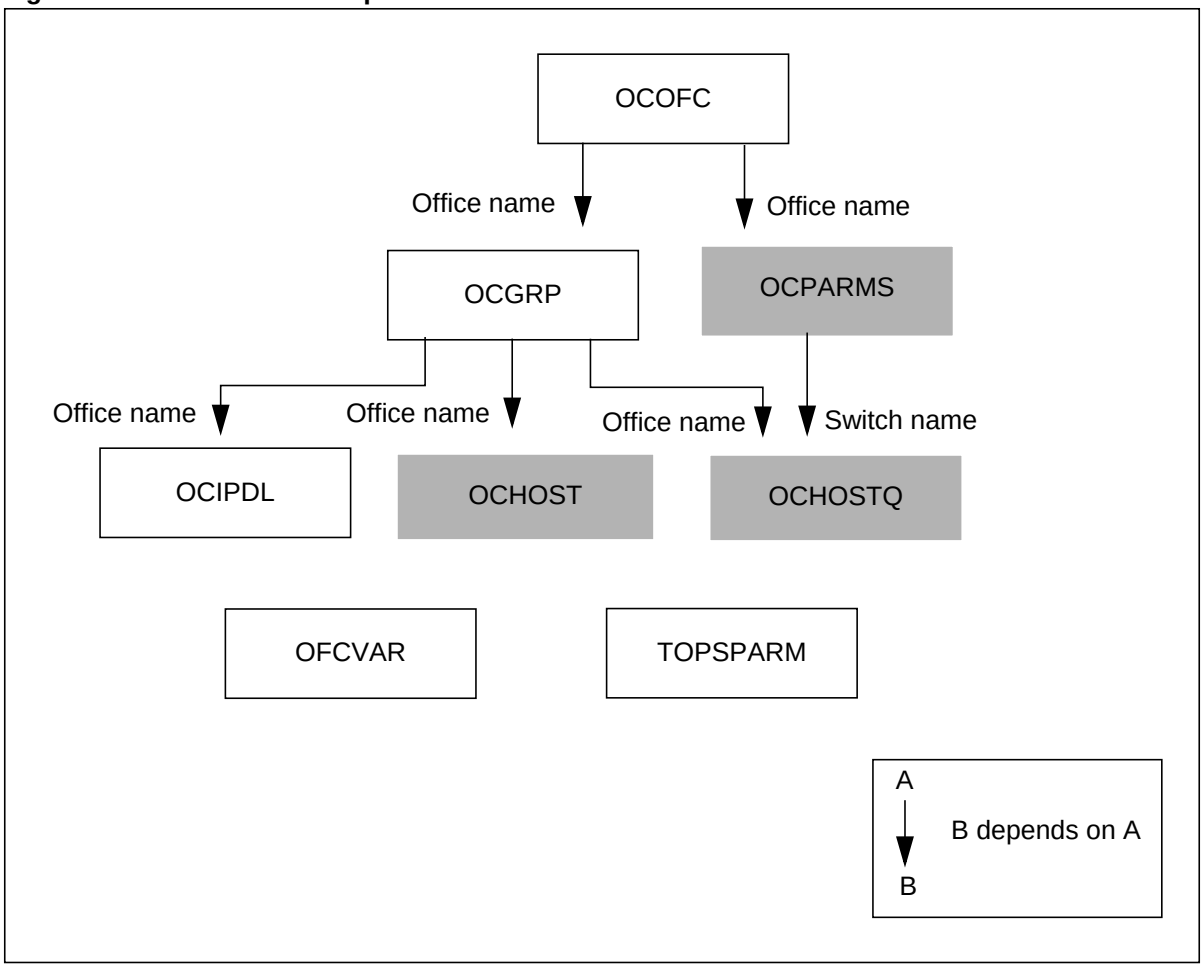
**Table 43 OC-IP datafill sequence**

| Table name | Definition |
|---|---|
| OCOFC | Operator Centralization Office. This table defines the names of offices in the OC network. |
| OCGRP | OC Group. This table defines an OC office as either host or remote and associates voice and data connectivity information with each office. |
| OCIPDL | OC IP Data Link. This table defines the IP connectivity for each OC-IP data link. |
| OFCVAR | Office Variables. This table contains office-wide variable parameters. |
| TOPSPARM | TOPS Parameters. This table contains office parameters that are specific to TOPS applications. |

***Note:*** Table TQCQINFO is another OC-IP application table. However, because it is also used by the IP position application, it is described with the infrastructure tables (see page 263).

Figure 130 summarizes the dependencies among the OC-IP tables. Arrows point to dependent tables and indicate the dependent information. Examples for each table are shown after the figure, except where noted.

**Figure 130 OC-IP datafill dependencies**




***Note 1:*** Tables OCPARMS, OCHOST, OCHOSTQ are shown in Figure 130 to indicate their dependencies; however, TOPS-IP does not change their use. *TOPS-IP User's Guide* does not document the data schema for these tables. For complete information, refer to *Customer Data Schema Reference Manual*.

***Note 2:*** Table OCHOST is not consulted when Host Remote Networking by Queue Type (HRNQT) is used.

## OCOFC

Table OCOFC defines the names of offices in the OC network. This table is also used by traditional OC, and the OC-IP application does not change the way it is used. OC-IP may use office numbers in the range 1 to 31.

The following table shows the datafill specific to TOPS-IP for table OCOFC.

**Table 44 Datafilling table OCOFC**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| VALUE | | 1 to 31 | Value. Enter the office number. No two office names can be associated with the same number and no two numbers can be associated with the same office name. |
| SYMBOL | | Alphanumeric up to 32 characters | Symbol. Enter the office name. |

### OCOFC example

The following example shows datafill for OC-IP. The datafill includes three distant offices that have IP data and voice connectivity with the office named HOME. (HOME also datafills itself in table OCOFC, because it uses HRNQT to route some calls to itself.)

**Figure 131 MAP display example for table OCOFC**

```
VALUE   SYMBOL
--------------------------------------------
1       HOME
2       HOST1
3       HOST2
5       REMOTE1
```

## OCGRP

Table OCGRP identifies each distant office referenced in table OCOFC as a host or a remote. The datafill also associates an OC-IP voice trunk group with each office, and specifies IP data connectivity.

***Note 1:*** IP data connectivity for an office must be specified in table OCGRP *before* data links can be added for that office in table OCIPDL.

***Note 2:*** When the office uses HRNQT, a distant switch may function as both a host and a remote for some other office. In this case, the distant switch must have two different entries in both table OCOFC and table OCGRP. One OCGRP entry identifies it as a host and the other entry identifies it as a remote. Also, a distant switch needs two entries in OCOFC and OCGRP if some of the OC traffic uses OC-IP and some of it uses traditional OC.

The following table shows the datafill specific to TOPS-IP for table OCGRP.

**Table 45 Datafilling table OCGRP**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| OFFICE | | Office name from table OCOFC | Office. Enter the office name. |
| OFCTYPE | | HOST, REMOTE | Office type. Enter the office type. |
| VLGRP | | Voice link group from table TRKOPTS | Voice link group. Enter the voice link group name. Table OCGRP enforces the following restrictions on the direction of the voice link:<br>- OG direction when the OFCTYPE is HOST<br>- 2W direction when the OFCTYPE is REMOTE |
| DLOVRLAY | | IP | Data link overlay. Enter IP.<br>***Note:*** IP data connectivity can be used only if IP voice connectivity is used and vice versa. |
| BCSLEVEL | | 50 (or greater) | Batch change supplement level. Enter the BCS level of the distant office or of the office in which the datafill resides, whichever is lower.<br>***Note:*** Table control enforces a BCS level of 48 or higher for tuples in OCGRP that have IP voice and data entries. However, both the host switch and remote switch must upgrade to LET0015 or higher before using the TOPS OC-IP application. Therefore, all OC-IP offices should be datafilled as BCS 50 or higher. |

## OCGRP example

The following example shows datafill for the two offices that have IP data and voice connectivity with the switch.

**Figure 132 MAP display example for table OCGRP**

```
OFFICE    OFCTYPE   VLGRP          DLOVRLAY  BCSLEVEL
-----------------------------------------------------------------
REMOTE1   REMOTE    OCIPTOREMOTE   IP        52
HOST1     HOST      OCIPTOHOST     IP        54
HOST2     HOST      OCIPTOHOST     IP        53
```

## OCGRP error and warning messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 46 Error and warning messages for table OCGRP**

| Error message | Explanation |
|---|---|
| DIRECTION OF TRUNK MUST BE OG | The user tries to add a host office (OFCTYPE set to HOST) with a voice trunk CLLI whose direction is not OG. |
| DIRECTION OF TRUNK MUST BE 2W | The user tries to add a remote office (OFCTYPE set to REMOTE) with a voice trunk CLLI whose direction is not 2W. |
| TRUNK MUST BE ASSIGNED DYNAMIC OC OPTION IN TABLE TRKOPTS | The user tries to set DLOVRLY to IP for a voice trunk CLLI that is not datafilled as DYNAMIC OC in table TRKOPTS. |
| TRUNK IS ASSIGNED DYNAMIC OPTION IN TABLE TRKOPTS | The user tries to set DLOVRLY to LAPD or HDLC for a voice trunk CLLI that is datafilled as DYNAMIC OC in table TRKOPTS. |
| BCS LEVEL CANNOT BE LESS THAN 48 FOR OC-IP OFFICES | The user changes the value for BCSLEVEL to less than 48.<br>***Note:*** Although table control allows BCS levels of 48 and 49, both the host switch and remote switch must upgrade to LET0015 or higher before using the TOPS OC-IP application. Therefore, all OC-IP offices should be datafilled as BCS 50 or higher. |
| WARNING: VOICE LINK CLLI HAS BEEN CHANGED. OC TRAFFIC TO THIS OFFICE WILL NOW USE THE UPDATED VOICE LINK CLLI. | The user changes the value of the VLGRP CLLI. (This is only allowed for OC-IP, not for TDM OC.) |
| WARNING: NO TRUNK MEMBERS EXIST FOR THIS GROUP. DATAFILL TABLE IPINV TO DEFINE TRUNK MEMBERS. | The user adds a CLLI that is datafilled in table TRKGRP, but does not have a Gateway card associated with it in table IPINV. |

## OCIPDL

Table OCIPDL defines the OC-IP data links that are used to communicate with each distant office. It also provides local and distant endpoint information about each link. Up to eight data links can be datafilled against each distant office. The distant office name must already be defined in table OCGRP with an IP data selector.

The COMID identifies a tuple in table IPCOMID, which indirectly specifies the port, transport protocol, and IP-XPM used for the *local* end of the data link. The IP address and port number fields directly specify the socket that the *distant* office uses for its end of the data link. This IP address is the active unit IP address of the SX05DA that supports the distant office's end of the data link.

***Note:*** Datafill for the local and far-end OC-IP data link connectivity must be parallel between OC switches in the network. A data link cannot be brought into service unless the datafill is consistent at both ends. For a discussion of parallel datafill, refer to "Parallel datafill for OC-IP data links" on page 91.

The following table shows the datafill specific to TOPS-IP for table OCIPDL.

**Table 47 Datafilling table OCIPDL**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| IPDLKEY | | See subfields | IP data link key. This field consists of subfields OFFICE and DLNUM. |
| | OFFICE | Office name from table OCGRP | Office. Enter the distant office name. |
| | DLNUM | 0 to 7 | Data link number. Enter the data link number for the distant office. |
| COMID | | COMID from table IPCOMID | Enter the COMID associated with local data connectivity. |
| IPADDR | | IP address of 4 octets from 0 to 255 | IP address. Enter the IP address associated with far-end data connectivity. |
| PORT | | 1024 to 65535 | Port. Enter the port associated with far-end data connectivity.<br>***Note:*** Refer to Chapter 7: "TOPS-IP engineering guidelines" for the recommended port range. |

## OCIPDL example

The following example shows two data links datafilled for each of three distant offices.

**Figure 133 MAP display example for table OCIPDL**

```
OCDLKEY      COMID   IPADDR              PORT
-----------------------------------------------------------
REMOTE1 0    1       47 192 201 112      8601
REMOTE1 1    2       47 192 201 110      8601
HOST1 0      8       47 192 218 140      8644
HOST1 1      9       47 192 218 150      8644
HOST2 0      12      47 192 63 100       8606
HOST2 1      13      47 192 63 100       8607
```

## OCIPDL error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 48 Error messages for table OCIPDL**

| Error message | Explanation |
|---|---|
| ERROR: CHANGES NOT ALLOWED, PLEASE DELETE AND RE-ADD. | Changes to table OCIPDL are not allowed. The user must delete the tuple and re-enter it to implement a change. |
| ERROR: LINK STATE NOT OFFLINE. | The user tries to delete a data link that is not in the OFFL state. |
| ERROR: THIS OFFICE IS NOT DATAFILLED AS IP IN TABLE OCGRP. | The user tries to add an office whose DLOVRLAY is not IP in table OCGRP. |
| ERROR: THIS OFFICE IS NOT DATAFILLED IN OCGRP. | The user tries to add an office name that is not datafilled in table OCGRP. |
| ERROR: THIS COMID IS ALREADY BOUND. | The user tries to add a COMID that is datafilled for this or another application. |
| ERROR: PROTOCOL FOR THIS COMID IS NOT DATAFILLED AS UDP IN TABLE IPSVCS. | The user tries to add a COMID whose protocol is not UDP in table IPSVCS. |
| ERROR: THE PORT FOR THIS COMID IS DATAFILLED AS 0 IN TABLE IPSVCS. | The user tries to add a COMID whose associated port is 0 in table IPSVCS. |
| ERROR: THIS COMID IS NOT DATAFILLED IN TABLE IPCOMID. | The user tries to add a COMID that is not in table IPCOMID. |
| ERROR: DUPLICATE IPADDR AND PORT FIELDS NOT ALLOWED FOR THIS TABLE. | The user tries to add a tuple whose IPADDR and PORT field are already datafilled against a tuple in table OCIPDL. |

**Table 48 Error messages for table OCIPDL**

| Error message | Explanation |
|---|---|
| ERROR: THE SERVICE ASSOCIATED WITH THIS COMID IS ALREADY BOUND TO A DIFFERENT APPLICATION. | A COMID associated with the same service name (in table IPCOMID) has been bound to a different application. |
| ERROR: IP COMID BIND ERROR.<br>INTERNAL ERROR #2 | Contact Nortel Networks technical support. |
| ERROR: INVALID APPLICATION ID.<br>INTERAL ERROR #4. | Contact Nortel Networks technical support. |
| ERROR: UNABLE TO VALIDATE COMID.<br>INTERNAL ERROR #5 | Contact Nortel Networks technical support. |
| ERROR: UNREGISTERED APPLICATION.<br>INTERNAL ERROR #6 | Contact Nortel Networks technical support. |
| ERROR: MISC IP COMID BIND ERROR.<br>INTERNAL ERROR #7. | Contact Nortel Networks technical support. |

## OFCVAR

Table OFCVAR contains office-wide parameters. For TOPS offices that use certain third-party Personal Audio Response System (PARS) devices, a parameter in OFCVAR controls the duration of the DTMF tone used to activate the PARS announcement. With OC-IP, this parameter must be datafilled in the *OC host switch*. The following table shows datafill relevant to TOPS-IP for table OFCVAR.

**Table 49 Datafilling table OFCVAR**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| TOPS_PARS_TONE_LENGTH | 0 to 255 | 10 | This parameter specifies the DTMF tone length for the PARS device. The value represents 10 ms increments. For example, a setting of 5 equals a tone length of 50 ms. |

***Note:*** This particular PARS functionality is only supported with TDM positions.

### OFCVAR example

The following example shows datafill for the OFCVAR parameter TOPS_PARS_TONE_LENGTH.

**Figure 134 MAP display example for table OFCVAR**

```
PARMNAME                    PARMVAL
------------------------------------------------------------
TOPS_PARS_TONE_LENGTH       10
```

## TOPSPARM

Table TOPSPARM contains TOPS-specific office parameters. The following table shows the datafill specific to OC-IP for table TOPSPARM.

**Table 50 Datafilling table TOPSPARM**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| OCIPDL_AUDIT_THRESHOLD | 2 to 10 failures | 3 | This parameter specifies how many consecutive audit failures are allowed before the system changes the state of an OC-IP data link from INSV to SYSB. |

### TOPSPARM example

The following example shows datafill specific to OC-IP for table TOPSPARM.

**Figure 135 MAP display example for table TOPSPARM**

```
PARMNAME                PARMVAL
------------------------------------------------------------------
OCIPDL_AUDIT_THRESHOLD  3
```

# IP position datafill

Datafill in the IP position tables specifies IP data and voice connectivity for IP positions. The operator positions have IP data connectivity with the managed IP network and are datafilled and maintained at the standalone/OC host switch.

***Note:*** The IP position application depends on the IP infrastructure, so datafill is *first* required in all the tables described in "IP infrastructure datafill" beginning on page 219.

## Table datafill dependencies

The following application-specific tables also require datafill for IP positions. There are no dependencies among these tables. However, table TOPSPOS depends on the infrastructure tables.

**Table 51 IP position datafill**

| Table name | Definition |
|---|---|
| TOPSPOS | TOPS Positions. This table provisions the data and voice connectivity for operator positions at a standalone or OC host switch. |
| TOPSPARM | TOPS Parameters. This table contains office parameters that are specific to TOPS applications. |
| MTCFAIL | Maintenance Failure Messages. This table contains text strings which, if datafilled, are includes in log reports when IP positions remove themselves from service. |
| MTCTEST | Maintenance Test Failure Messages. This table contains text strings which, if datafilled, are displayed to MAP users who issue a test command for an IP position that reports test failure. |

***Note:*** Table TQCQINFO is another IP position application table. However, because it is also used by the OC-IP application, it is described with the infrastructure tables (see page 263).

## TOPSPOS

Table TOPSPOS contains provisioning datafill for operator positions supported by the TOPS switch. Each tuple defines voice and data link information for a single position. Table TOPSPOS allows the voice and data paths to be provisioned as IP.

***Note:*** TOPS-IP does not change the datafill for TDM-based operator positions.

The following table shows the datafill specific to TOPS-IP for table TOPSPOS. For a description of the other fields, refer to *Customer Data Schema Reference Manual*.

**Table 52 Datafilling table TOPSPOS**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| VLPATH | | See subfields | Voice link path. For IP positions, this field consists of subfields VLTYPE and VLCLLI. |
| | VLTYPE | PKTV | Voice link type. Enter PKTV for packetized voice communication. |
| | VLCLLI | CLLI name from table TRKOPTS | Voice link CLLI. Enter the CLLI used for the packetized voice link (dynamic trunk). |
| DATAPATH | | See subfields | Data path. For IP positions, this field consists of subfields DATATYPE, IPCOMID, and URESOK. |
| | DATATYPE | IP | Datatype. Enter IP. |
| | IPCOMID | COMID from table IPCOMID | IPCOMID. Enter the COMID used for data communication. |
| | URESOK | Y, N | Unrestricted Idle OK. Enter Y to indicate that the position remains in the URES state indefinitely until a maintenance action forces a transition. Enter N to indicate that the position transitions to the SYSB state if the switch does not receive a request from the position to go into service within approximately15 seconds. |

## TOPSPOS example

The following example shows datafill for three IP positions.

**Figure 136 MAP display example for table TOPSPOS**

```
POSN0    VLPATH            DATAPATH      POSAREA
-------------------------------------------------------------------
411      PKTV POSIPVL      IP 20 N       OPR 6 17
412      PKTV POSIPVL      IP 20 N       OPR 6 24
413      PKTV POSIPVL      IP 21 N       OPR 6 17
```

## TOPSPOS error and warning messages

The following table lists possible error messages related to adding, changing, or deleting tuples. Only the error messages specific to TOPS-IP are shown. See *Customer Data Schema Reference Manual* for more information.

**Table 53 Error and warning messages for table TOPSPOS**

| Error message | Explanation |
|---|---|
| POSITION WITH IP DATATYPE MUST USE PKTV VLTYPE. | User tries to add a tuple with TDM voice link type and IP datatype. The IP datatype requires the packetized voice link type. |
| TRUNK MUST BE ASSIGNED DYNAMIC POS OPTION IN TABLE TRKOPTS. | User tries to datafill a tuple with a voice link CLLI that is not defined as DYNAMIC POS in table TRKOPTS. |
| SPECIFIED COMID IS NOT DATAFILLED IN IPCOMID | User tries to datafill a tuple with a COMID that is not datafilled in table IPCOMID. |
| COMID ALREADY BOUND BY ANOTHER APPLN. | User tries to datafill a tuple with a COMID that is already used by another application, such as OC-IP or QMS MIS-IP. |
| PROTOCOL FOR THIS COMID IS NOT DATAFILLED AS UDP IN IPSVCS | User tries to datafill a tuple with a COMID whose associated protocol (from table IPSVCS) is not UDP. UDP is the only protocol supported for IP positions data connectivity. |
| TOO MANY IP POS COMIDS ON THIS DTC, RE-USE AN EXISTING COMID | TOPSPOS already has tuples that use eight different COMIDs on this IP-XPM. Eight is the maximum allowed. |
| WARNING: POSITION VOICE CLLI IS NOT DATAFILLED IN IPINV OR TRUNK TABLES. THE POSITION CANNOT SUPPORT STANDALONE OR TDM-OC TOPS CALLS, BOOKED CALLS, OR DELAY CALLS. | User adds a placeholder CLLI, which does not allow the IP position to support any of the listed call types. In this context, “delay calls” refers to any call that the operator initiates. Refer to “Operator-originated calls” on page 149 for more information. |
| WARNING: NO TRUNK MEMBERS EXIST FOR THIS TRUNK GROUP. DATAFILL TABLE IPINV TO DEFINE TRUNK MEMBERS. | User adds a CLLI that is datafilled in table TRKGRP, but does not have a Gateway card associated with it in table IPINV. |

## TOPSPARM

Table TOPSPARM contains TOPS-specific office parameters. The following table shows the datafill specific to IP positions for table TOPSPARM.

**Table 54 Datafilling table TOPSPARM**

| Parameter name | Range of values | Default value | Explanation |
|---|---|---|---|
| IPPOS_AUDIT_INTERVAL | 5 to 15 seconds | 5 | This parameter is reserved for future use. Its value does not affect any functionality. |
| IPPOS_AUDIT_THRESHOLD | 2 to 5 | 3 | This parameter is reserved for future use. Its value does not affect any functionality. |

### TOPSPARM example

The following example shows datafill specific to TOPS-IP for table TOPSPARM.

**Figure 137 MAP display example for table TOPSPARM**

```
PARMNAME                PARMVAL
------------------------------------------------------------------
IPPOS_AUDIT_INTERVAL    5
IPPOS_AUDIT_THRESHOLD   3
```

## MTCFAIL

Table MTCFAIL associates text strings with numeric failure codes that operator positions may send to the switch. If a failure code is datafilled in table MTCFAIL, the switch includes the associated text string when it reports the failure.

The following table shows the fields in table MTCFAIL that are relevant to TOPS-IP.

**Table 55 Datafilling table MTCFAIL**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| ERRCODE | | 50 to 255 | Error code. A numeric error code that an IP position can send to the DMS in an out-of-service notification message. |
| ERRTEXT | | Alphanumeric up to 63 characters | Error text. Text that describes the error condition. |

### MTCFAIL example

The following example shows a tuple for one error code.

**Figure 138 MAP display example for table MTCFAIL**

```
ERRCODE                                              ERRTEXT
-----------------------------------------------------------
156                      POSITION_MAINTENANCE_IN_PROGRESS
```

***Note:*** Refer to *TOPS IWS Base Platform User's Guide* for explanation of the error codes that IP positions can return.

### MTCFAIL error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 56 Error messages for table MTCFAIL**

| Error message | Explanation |
|---|---|
| `ERRCODE VALUES LESS THAN 50 ARE RESERVED FOR NORTHERN TELECOM AND ARE UNCHANGEABLE.` | The user tries to modify or delete a tuple with a error code in the 0 to 50 range. These tuples are present by default and may not be changed. |

## MTCTEST

Table MTCTEST associates text strings with numeric failure codes that operator positions may send to the switch when a MAP user enters the TST command for a posted position, and the test fails. If a failure code is datafilled in table MTCTEST, the switch includes the associated text string when it reports the failure.

The following table shows the fields in table MTCTEST that are relevant to TOPS-IP.

**Table 57 Datafilling table MTCTEST**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| ERRCODE | | 1 to 511, excluding 101, 201 to 306, and 401 to 411 | Error code. A numeric error code that an IP position can send to the DMS when a test fails. |
| ERRTEXT | | Alphanumeric up to 63 characters | Error text. Text that describes the error condition. |

### MTCTEST example

The following example shows a tuple for one error code.

**Figure 139 MAP display example for table MTCTEST**

```
ERRCODE                                                ERRTEXT
-------------------------------------------------------------
153                              INITIALIZATION_IN_PROGRESS
```

***Note:*** Refer to *TOPS IWS Base Platform User's Guide* for explanation of the error codes that IP positions can return.

### MTCTEST error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

**Table 58 Error messages for table MTCTEST**

| Error message | Explanation |
|---|---|
| `ERRCODE VALUES 101, 201-306, AND 401-411 ARE RESERVED FOR NORTHERN TELECOM AND ARE UNCHANGEABLE.` | The user tries to modify or delete a tuple with a error code in one of the listed ranges. These tuples are present by default and may not be changed. |

## QMS MIS-IP datafill

Datafill in the QMS MIS-IP tables allows the TOPS switch to send MIS data to a vendor node on the managed IP network. The QMS MIS-IP application runs as a separate process in the TOPS switch. The application receives operator call and position event messages, buffers the messages, and sends them to the external MIS node.

### Table datafill dependencies

The QMS MIS-IP application depends on the IP data infrastructure, so datafill is first required in the following tables:

- LTCINV
- XPMIPGWY
- XPMIPMAP
- IPSVCS
- IPCOMID

Refer to "IP infrastructure datafill" beginning on page 219 in this chapter for examples of QMS MIS-IP datafill in these tables.

***Note:*** Table TQMISOPT (TOPS QMS MIS Options) contains parameters used by the QMS MIS application. For example, QMS_MIS_CAM_ON must be set to Y before the MIS application starts to buffer messages, raise alarms, and generate logs. Before provisioning MIS-IP, users should review the datafill for TQMISOPT. For details, refer to *Customer Data Schema Reference Manual*.

The following QMS MIS table also requires datafill, but has no dependencies other than the IP infrastructure.

**Table 59 QMS MIS datafill**

| Table name | Definition |
|---|---|
| QMSMIS | QMS MIS. This table provisions the QMS MIS data links, including the IP addresses of up to two IP connections. |

## QMSMIS

Table QMSMIS specifies provisioning information for the TOPS QMS MIS application on the switch. It supports up to two IP connections for transmitting the same MIS data stream.

***Note 1:*** The second MIS-IP data link may be provisioned for redundancy or for communication to a second MIS node. For engineering information, refer to Chapter 6: "TOPS-IP engineering guidelines."

***Note 2:*** To minimize TCP re-establishment delays, it is recommended that table IPSVCS be datafilled with a PORT value of 0 for the QMS MIS-IP service tuple. A value of 0 is used to request the XPM to randomly assign a port number.

The following table shows the datafill specific to TOPS-IP for table QMSMIS.

**Table 60 Datafilling table QMSMIS**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| INDEX | | TOPS | Index. Enter TOPS. |
| DATALINK | | See subfields | Datalink. This field consists of subfield DATALINK and refinements specific to the type of data link. |
| | DATALINK | IP | Datalink type. Enter IP.<br>***Note:*** During a change of interface, any MIS buffers that have not been sent out are lost. |
| | BUFXTIME | 1 to 59 seconds | Buffer transmit interval. Enter the maximum period before an MIS IP buffer is sent to the MIS node. |
| | CONNLIST | See subfields | Connection list. This field consists of the following refinements: DESTADDR, DESTPORT, DESSTAT, and COMID. Datafill up to 2 connections.<br>***Note:*** Although table control allows datafill for up to 4 IP connections, TOPS-IP supports only 2 connections. |
| | DESTADDR | IP address of 4 octets from 0 to 255 | Destination address. Enter the destination IP address of the MIS node. |
| | DESTPORT | 1024 to 32767 | Destination port. Enter the destination port of the MIS node. |

**Table 60 Datafilling table QMSMIS**

| Field | Subfield or refinement | Entry | Explanation and action |
|---|---|---|---|
| | DESSTAT | INACTIVE, ACTIVE | Destination status. Enter the desired destination status.<br>***Note 1:*** When the destination status of the node is set to INACTIVE, the switch does not send MIS message buffers to this node.<br>***Note 2:*** When the DESSTAT field is changed from ACTIVE to INACTIVE, messages may be lost.<br>***Note 3:*** If two IP connections both are set to INACTIVE, it is recommended that TQMISOPT parameter QMS_MIS_CAM_ON be set to N to conserve switch resources. |
| | COMID | COMID from table IPCOMID | COMID. Enter the COMID associated with local data connectivity. |

## QMSMIS example

The following example shows datafill for the TOPS QMS MIS-IP application.

**Figure 140 MAP display example for table QMSMIS**

```
INDEX        DATALINK
-------------------------------------------------------------
TOPS         IP  10 (123 15 3 5    2003     ACTIVE     30) $
```

## QMSMIS error messages

The following table lists possible error messages.

**Table 61 Error messages for table QMSMIS**

| Error message | Explanation |
|---|---|
| `You must set DATALINK to IP or MPC for TOPS MIS facility.`<br>`You must set DATALINK to ETHERNET for OSSAIN MIS nodes.` | The user tries to datafill a datalink name that does not match the index. |
| `Invalid COMID. Make sure COMID exists in table IPCOMID.` | The user tries to datafill a COMID that is not in table IPCOMID. |
| `Error! COMID already in use by another application.` | The user tries to datafill a COMID that is already used. |
| `ERROR ALLOCATING MEMORY FOR NEW IP TUPLE.` | The CM cannot allocate memory when the user tries to add an IP tuple. |

**Table 61 Error messages for table QMSMIS**

| Error message | Explanation |
|---|---|
| COMID IS NOT PRESENT IN TABLE IPCOMID. | The user tries to add IP connection information to the IP tuple using a COMID that is not in table IPCOMID. |
| COMID IS ALREADY IN USE BY ANOTHER APPLICATION. | The user tries to add IP connection information to the IP tuple using a COMID that is already used. |
| PROBLEM WITH THE SERVICE BOUND TO THIS COMID. | The user tries to add IP connection information to the IP tuple using a COMID associated with the wrong service. |
| COMID FAIL TO BIND TO IP LAYER. | The user tries to add IP connection information to the IP tuple which fails to bind the COMID. |
| EMPTY IP VECTOR IS NOT ALLOWED. | The user tries to add the IP interface with an empty IP connection vector. At least one IP connection must be datafilled. |
| DUPLICATE COMIDs ARE NOT ALLOWED.USE ONE COMID PER IP CONNECTION. | The user tries to add IP connection information to the IP tuple using a duplicate COMID. |
| ERROR - ONLY COMIDS DATAFILLED TO USE TCP PROTOCOL ARE ALLOWED IN TABLE QMSMIS. | The user tries to add IP connection information to the IP tuple using a COMID that is not associated with TCP in table IPSVCS. |
| FAIL TO ALLOCATE MEMORY FOR IP BUFFERS. | The CM cannot allocate memory the first time the user tries to add the IP interface to the table. |
| YOU MUST SET THE DESSTAT FIELD(S) TO INACTIVE BEFORE DELETING THE TUPLE. | The user tries to delete an IP tuple when a DESSTAT field (or fields) is active. |
| YOU MUST SET THE DESSTAT FIELD(S) TO INACTIVE BEFORE CHANGING THE TUPLE. | The user tries to change an IP tuple when a DESSTAT field (or fields) is active. |
| WARNING!! DATAFILLING A COMID WITH A NON-ZERO PORT IN TABLE IPSVCS FOR TCP, WILL RESULT IN TCP/IP CONNECTION RE-ESTABLISHMENT DELAYS. IT IS HIGHLY RECOMMENDED TO DATAFILL ZERO AS THE PORT NUMBER IN TABLE IPSVCS FOR THE QMS MIS IP APPLICATION. | The user tries to add IP connection information to the IP tuple using a COMID that is not associated with a port value of zero in table IPSVCS. |

## XIPVER datafill

The XIPVER CI test tool allows users to test IP data communication to the IP-XPM. The tool is provisioned in the IP data infrastructure, so datafill is first required in the following tables:

- LTCINV
- XPMIPGWY
- XPMIPMAP
- IPSVCS
- IPCOMID

Refer to "IP infrastructure datafill" beginning on page 219 in this chapter for examples of XIPVER datafill in these tables.

***Note:*** For information on how to use the XIPVER CI tool, refer to Chapter 11: "TOPS-IP CI tools."

# Chapter 9: TOPS-IP software ordering

This chapter provides information on ordering PCL (product computing module load) and NCL (non-CM) software loads, and on IP network warranty service options.

## PCL software loads

All functionality in a PCL is categorized as either base or optional. Base functionality is available for use immediately. Optional functionality is grouped into commercial units called software optionality control (SOC) options. All TOPS functionality is optional and is controlled by at least the Basic Operator Services order code, OSB00101. Some TOPS functionality requires additional order codes.

***Note1:*** SOC provides an interface at the MAP terminal. Users can enable or disable functionality controlled by SOC, track the state of SOC options, and generate reports about SOC options. For detailed information on how to use the SOC tool, please refer to *Software Optionality Control User's Manual*, 297-8991-901.

***Note2:*** Each PCL that supports TOPS includes a specific release of the TOPS software. This book discusses the required TOPS software releases, and not the PCL names. Please contact your Nortel Networks representative for information about the PCL names.

### TOPS-IP infrastructure—OSB00101

The TOPS-IP infrastructure is supported in North American and non-North American PCLs that support TOPS and that contain TOPS15 or higher.

The TOPS-IP infrastructure is provided as part of the Basic Operator Services SOC, OSB00101. All TOPS-IP application functionality also requires C-side 14 extended messaging, which is available with order code TEL00011. Certain TOPS-IP applications are available only in North American PCLs.

### C-side 14 Extended Messaging—TEL00011

C-side 14 extended messaging is required for all TOPS-IP applications. It is supported in all PCLs that support the TOPS-IP infrastructure.

The SOC code for C-side 14 extended messaging is TEL00011. This is a state SOC which controls the ability to provision extended messaging links in table LTCINV, both directly and through the CONVERTCSLINKS CI tool.

### OC-IP application—ENSV0107

The OC-IP application is supported in North American PCLs that support TOPS and contain TOPS15 or higher. OC-IP is not supported in non-North American loads.

The SOC code for OC-IP is ENSV0107, TOPS IP OC. This option must be in the ON state before OC-IP data links can be brought into service. Before SOC ENSV0107 can transition to the IDLE state, every OC-IP data link defined in table OCIPDL must be UNEQ, OFFL, or MANB.

### IP Position application—OSB00102

The IP Position application is supported in North American and non-North American PCLs that support TOPS and contain TOPS17 or higher. The TOPS17 requirement is for standalone and OC host switches. OC remote switches at TOPS15 and higher can process calls that are served by IP positions in the OC host.

The SOC code for IP Position functionality is OSB00102, OPP Over IP. This is a usage SOC. It controls the number of IP positions that can transition from the OFFL maintenance state to MANB in a TOPS standalone or OC host switch.

### QMS MIS-IP application—OSB00101

The QMS MIS-IP application is not currently supported. Customers with an interest in this application should discuss it with TOPS Marketing and with their MIS vendors.

## NCL software loads

7X07 Gateway loads have NCL names such as TGWY00xx and TGWYM0xx. The TGWY00xx software only works in conjunction with the TOPS-IP DHCP server. TGWYM0xx orders are maintenance releases and are provided by Nortel Networks as required. For example, TGWYM003 refers to the latest maintenance release for the TGWY0003 order.

The following table shows the supported NCL software releases for the 7X07AA Gateway and IP-XPM, for each TOPS release that supports TOPS-IP applications.

***Note:*** The IP Position application requires IWS17.1 or higher.

**Table 62 Compatibility between TOPS releases and NCL loads for TOPS-IP**

| TOPS release | Supported 7X07AA NCLs | Supported IP-XPM software loads |
|---|---|---|
| TOPS15 | TGWY0004/TGWYM004<br>***Note:*** Customers with TOPS15 should place any new orders for TGWY0004, and should have the latest TGWYM004 NCL. | QD716, QTP18<br>***Caution:*** The QD715 and QD717 loads are not supported for TOPS-IP. |
| TOPS17/SN04 | TGWY0004/TGWYM004<br>***Note:*** The TGWY0004 NCL is required for invoicing purposes. Customers should use the latest TGWYM004 NCL. | QTP19<br>***Caution:*** The QD717 load is not supported for TOPS-IP. |
| TOPS18/SN05 | TGWY0004/TGWYM004<br>***Note:*** The TGWY0004 NCL is required for invoicing purposes. Customers should use the latest TGWYM004 NCL. | QTP19 |
| TOPS19/SN06 | TGWY0004/TGWYM004<br>***Note:*** The TGWY0004 NCL is required for invoicing purposes. Customers should use the latest TGWYM004 NCL. | QTP19 |
| TOPS20/SN07 | TGWY0004/TGWYM004<br>***Note:*** The TGWY0004 NCL is required for invoicing purposes. Customers should use the latest TGWYM004 NCL. | QTP20 |
| TOPS21/SN08 | TGWY0004/TGWYM004<br>***Note:*** The TGWY0004 NCL is required for invoicing purposes. Customers should use the latest TGWYM004 NCL. | QTP21 |
| TOPS22/SN09 | TGWY0004/TGWYM004<br>***Note:*** The TGWY0004 NCL is required for invoicing purposes. Customers should use the latest TGWYM004 NCL. | QTP22 |

## IP network warranty service options

The TOPS-IP managed IP network includes components from several Nortel Networks product groups, and it may also consist of components from third-party vendors. Each Nortel Networks product, as well as each vendor product, has its own warranty policy. For more details, contact your Nortel Networks representative.

TOPS-IP service providers may choose from three options for receiving their warranty services:

- Independent option—Service providers work with each Nortel Networks group and with each third-party vendor for servicing.
- Operator Services (TOPS) blanket warranty agreement option—Service providers work with one contact for servicing.
- Switch-only option—Nortel Network provides support for the DMS switch only.

# Part 6: Billing

The TOPS-IP product does not affect or change billing.

# Part 7: OA&M

Part 7: Operation, administration, and maintenance includes the following chapters:

# Chapter 10: TOPS-IP maintenance activities

This chapter discusses maintenance activities for the following TOPS-IP areas:

- IP Gateway (IPGW) maintenance (page 293)
- IP-XPM maintenance, diagnostics, and troubleshooting (page 322)
- TOPSIP MAP (maintenance and administration position) level (page 323)
- OC-IP data link maintenance (page 324)
- IP position maintenance (page 340)
- TOPS QMS MIS-IP maintenance (page 369)

***Note:*** For information on using switch CI tools, refer to Chapter 11: "TOPS-IP CI tools."

## IP Gateway maintenance

The 7X07 Gateway cards provide IP voice communication in the TOPS-IP network. Installed in the IP-XPM, each card represents an integrated P-side node that has characteristics of both a P-side interface card and a subtending node.

This section discusses maintenance functions for the 7X07 Gateways, focusing on the following areas:

- Installing the 7X07AA Gateway cards (page 294)
- Datafilling the Gateway cards (page 295)
- Using the MAP commands at the IPGW level (page 299)
- Bringing a Gateway card into service (page 302)
- Troubleshooting the Gateway (page 308)
- Maintaining dynamic voice trunks (page 317)

***Note:*** Before performing any maintenance on the Gateway cards, users should review the limitations and restrictions listed in Chapter 6: "TOPS-IP feature impact."

## Installing the 7X07AA Gateway cards

Figure 141 shows the slot positions and related port numbering for up to 10 Gateway cards in the IP-XPM shelf (front view).

**Figure 141 7X07AA Gateway card slot position and port numbering in the IP-XPM**

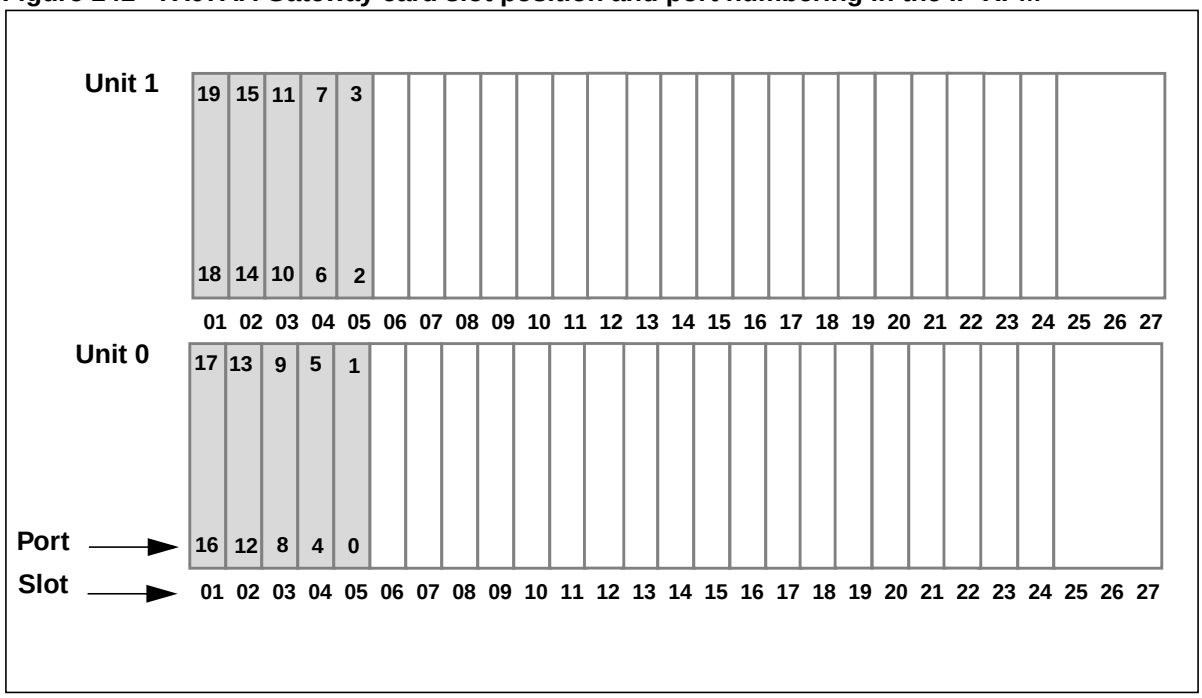



Table 63 lists the correct port mapping that is defined through datafill in tables LTCPSINV and IPINV.

***Note:*** Until the correct port datafill is present, the switch will generate PM777 log reports.

**Table 63 LTCPSINV-to-IPINV port mapping**

| LTCPSINV field PSLINK | IPINV field PORT |
|---|---|
| 0,1 | 0 |
| 2, 3 | 2 |
| 4, 5 | 4 |
| 6, 7 | 6 |
| 8, 9 | 8 |
| 10, 11 | 10 |
| 12, 13 | 12 |
| 14, 15 | 14 |
| 16, 17 | 16 |
| 18, 19 | 18 |

## Datafilling the Gateway cards

The Gateway cards are provisioned through datafill in the following tables:

- CARRMTC (Carrier Maintenance)
- LTCPSINV (LTC P-side Inventory)
- SITE (Site)
- IPINV (IP Inventory)

***Note 1:*** For the trunk groups supported by the Gateway cards, datafill is required in all the voice provisioning tables. This trunk group datafill must be done before datafilling table IPINV. Refer to Chapter 8: "TOPS-IP data schema" for datafill sequence and details on fields and valid values.

***Note 2:*** For Gateway engineering information, refer to Chapter 7: "TOPS-IP engineering guidelines."

### CARRMTC

Table CARRMTC specifies a set of carrier attributes for P-side links that are defined in table LTCPSINV. CARRMTC also provides maintenance control information for peripheral modules (PM), such as the DTC. The value in field TMPLTNM is referenced by table LTCPSINV.

The following example shows datafill for the DTC used by the Gateways for voice over IP communication.

**Figure 142 MAP display example for table CARRMTC**

```
CSPMTYPE TMPLTNM  RTSML  RTSOL  ATTR
-------------------------------------------------------------------------------
DTC      TGWY     255    255    DS1 NT7X07AA  MU_LAW SF ZCS BPV NILDL N 250 1000
50 50 150 1000 3 6 864 100 17 511 4 255
```

### LTCPSINV

Table LTCPSINV specifies the P-side link assignments that are associated with voice over IP at the DTC. Tuples in this table use the same key as table LTCINV.

***Note 1:*** An entry in table LTCPSINV is added automatically when an XPM is datafilled in table LTCINV. All the P-side link types initially default to NILTYPE. P-side links that do not have hardware assigned must remain NILTYPE. Unequipped software-assigned P-side links generate service-affecting problems.

***Note 2:*** After the P-side links for a Gateway are added to table LTCPSINV, the corresponding datafill for the Gateway must be entered in table IPINV. Otherwise, the IP-XPM will have inconsistent information about its packfill and diagnostics may be affected. The switch also will generate PM777 logs (wrong P-side card). For details on the correct datafill for port mapping, refer to Table 63 on page 294.

The following example shows the P-side link assignments for DTC 10 and DTC 11. In both DTCs, DS-1 signaling and TGWY (template name from table CARRMTC) are datafilled for P-side links 6 through 13. The other P-side links are unassigned and so must be datafilled with a value of NILTYPE. In this example, each DTC shows datafill for four Gateways defined in table IPINV.

**Figure 143 MAP display example for table LTCPSINV**

```
LTCNAME   PSLINKTAB
-------------------------------------------------------------------------------
DTC 10    N (0 NILTYPE)(1 NILTYPE)(2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N) (8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 DS1 TGWY N) (13 DS1 TGWY N) (14 NILTYPE) (15
NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $

DTC 11    N (0 NILTYPE)(1 NILTYPE)(2 NILTYPE) (3 NILTYPE) (4 NILTYPE)
(5 NILTYPE) (6 DS1 TGWY N) (7 DS1 TGWY N) (8 DS1 TGWY N) (9 DS1 TGWY N)
(10 DS1 TGWY N) (11 DS1 TGWY N) (12 DS1 TGWY N) (13 DS1 TGWY N) (14 NILTYPE) (15
NILTYPE) (16 NILTYPE) (17 NILTYPE) (18 NILTYPE) (19 NILTYPE) $
```

## SITE

Table SITE identifies a site name associated with the Gateway cards datafilled at the switch. The value in field NAME is referenced by table IPINV as well as by application-specific tables.

The following example shows datafill for site name TGWY. Additional fields in SITE are unused and should be set to default values.

***Note:*** After table IPINV is datafilled, the system automatically updates the MODCOUNT field to reflect the number of Gateway cards on the site.

**Figure 144 MAP display example for table SITE**

```
NAME   LTDSN  MODCOUNT OPVRCLLI ALMDATA
-------------------------------------------------------
TGWY   0      0        VER90    $
```

### IPINV

Table IPINV defines the individual Gateway cards at the switch. The following example shows eight Gateway cards identified by the site name TGWY. Four Gateway cards are located in DTC 10 and four are located in DTC 11. Associated with the Gateway cards are the TOPS application, the OCIPTOREMOTE and OCIPTOHOST trunk groups which support 144 members each, and the POSIPVL trunk group which supports 94 members.

***Note 1:*** The PORT value datafilled (even number) corresponds to the P-side link assignments (port, port+1) in table LTCPSINV. In this example, port 6 is for P-side ports 6 and 7, port 8 is for P-side ports 8 and 9, and so on. Refer to Table 63 on page 294.

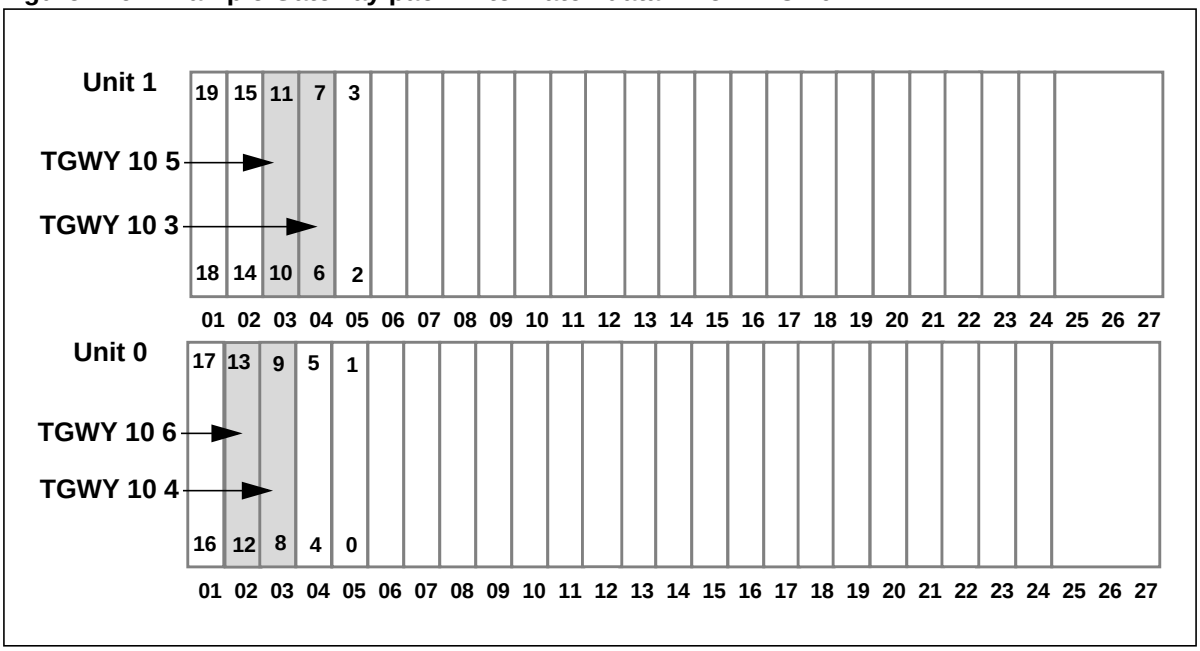
***Note 2:*** TOPS Gateways require the correct IP address in the IPZONE field. The primary IP address must match the one assigned to the Gateway by the DHCP server. Any mismatch between DHCP datafill and CM datafill for a Gateway will not allow the Gateway to come into service.

**Figure 145 MAP display example for table IPINV**

```
IPNO       PMTYPE  PMNO IPPEC  LOAD PORT  IPZONE               GWTYPE
-------------------------------------------------------------------------------
TGWY 10 3  DTC     10   7X07AA  $    6    47 174 68 7 0 0 0 0   TOPS OCIPTOREMOTE 0
TGWY 10 4  DTC     10   7X07AA  $    8    47 174 68 8 0 0 0 0   TOPS OCIPTOHOST 0
TGWY 10 5  DTC     10   7X07AA  $    10   47 174 68 9 0 0 0 0   TOPS OCIPTOREMOTE 48
TGWY 10 6  DTC     10   7X07AA  $    12   47 174 68 10 0 0 0 0  TOPS POSIPVL 0
TGWY 11 3  DTC     11   7X07AA  $    6    47 174 69 7 0 0 0 0   TOPS OCIPTOHOST 48
TGWY 11 4  DTC     11   7X07AA  $    8    47 174 69 8 0 0 0 0   TOPS OCIPTOREMOTE 96
TGWY 11 5  DTC     11   7X07AA  $    10   47 174 69 9 0 0 0 0   TOPS OCIPTOHOST 96
TGWY 11 6  DTC     11   7X07AA  $    12   47 174 69 10 0 0 0 0  TOPS POSIPVL 144
```

Figure 146 shows an example of the Gateway packfill for DTC 10.

**Figure 146 Example Gateway packfill to match datafill for DTC 10**



## Updating static data

Static data for the SX05DA card should be updated after users change the GWINDEX field in table XPMIPMAP (CM configuration method).

To update static data, perform a cold SWACT on the IP-XPM. Any in-service Gateways on the XPM will go SYSB and recover automatically after the cold SWACT completes.

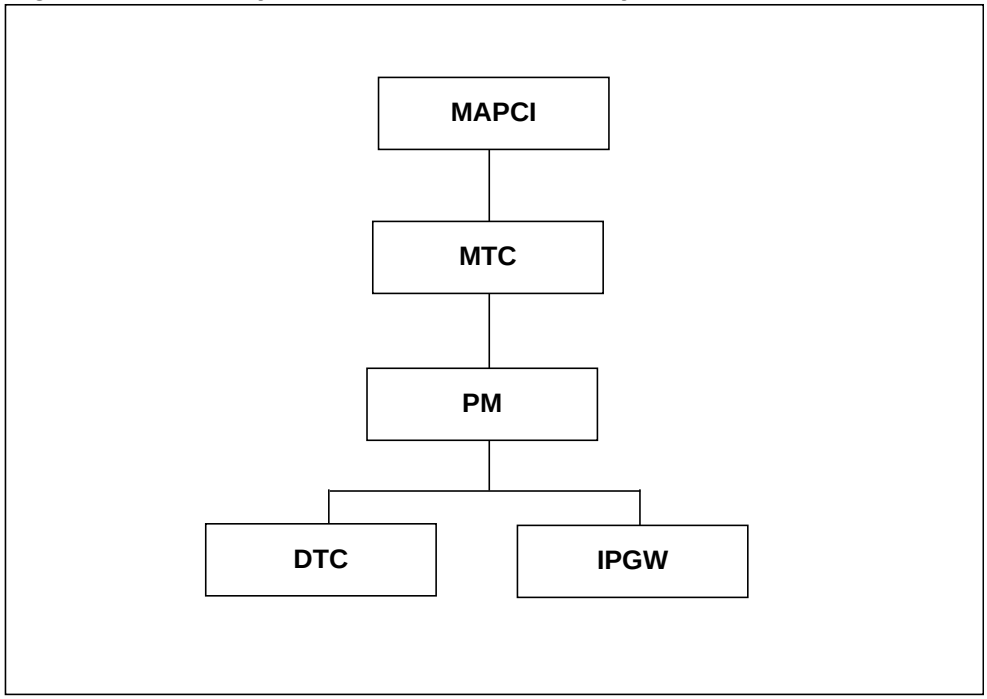
The automatic recovery takes three to four minutes. To recover the Gateways faster, they can be posted at the MAPCI;MTC;PM;IPGW level and manually busied and returned to service (with the FORCE option). This should be done after the Gateway's state is updated to SYSB by the system.

## Using the MAP commands at the IPGW level

The PM level of the MAP allows users to post the DTC and display the P-side links associated with the Gateway card. The DTC commands are accessed from the MAPCI;MTC;PM level menu. Likewise, the PM level allows users to post a provisioned Gateway (IPGW) or group of Gateways. The IPGW commands are also accessed from the MAPCI;MTC;PM level menu.

Figure 147 shows the MAP menu hierarchy.

**Figure 147 Gateway maintenance MAP hierarchy**



### IPGW MAP level

Figure 148 shows an example of the IPGW MAP display. To post a TOPS-IP Gateway, users type POST IPGW and specify the IPNO value from table IPINV, or the status, or ALL. For example, POST IPGW TGWY 10 3.

**Figure 148 MAP display example of IPGW level**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

IPGW                        SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit              PM      0       5        1     0     11     22
2  Post_             IPGW    0       3        1     0      0      9
3
4                    IPGW TGWY 10 3 OffL  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy
8  RTS
9  OffL
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

The following list briefly describes the IPGW commands in the order in which they appear at the MAP:

- QUIT exits the user from the IPGW MAP level. Control is returned to the level specified by the user.
- POST displays a specific Gateway or group of Gateways for maintenance purposes. Users can post Gateways by IPNO as datafilled in table IPINV (site name, frame, and Gateway unit), state, or all the Gateways.
- TRNSL displays the C-side links to the posted Gateway, along with its DTC number and state.
- TST runs diagnostics on the posted Gateway.
- BSY manually busies the posted Gateway and sets its state to MANB. For TOPS-IP Gateways, users can issue the BSY DRAIN option to provide a controlled method of taking a Gateway out of service. DRAIN allows calls in progress on a Gateway to remain up until completion, while preventing future call originations.

  ***Note:*** After the BSY DRAIN command is issued on an INSV Gateway, all IDL trunks are marked CFL. CPD trunks are marked as deloading. When the call associated with a deloading trunk completes, the trunk is marked CFL. When all trunks associated with a Gateway are CFL, the Gateway transitions to MANB.
- RTS returns a Gateway to service. The RTS command invokes the out-of-service (OOS) set of diagnostic tests to determine the general capability of the Gateway. RTS FORCE bypasses the OOS tests.
- OFFL off-lines the Gateway.
- LOADPMQ displays the current load status of the Gateway.
- NEXT posts the next Gateway in the post set.
- QUERYPM displays node status and configuration of the Gateway.
- PMRESET reloads and restarts the Gateway.
- SPARES is not supported for TOPS-IP Gateway maintenance.

***Note:*** For details on the IPGW command parameters, refer to *Command Interface Reference Manual*, 297-8991-824.

## Bringing a Gateway card into service

This procedure shows the steps to bring a Gateway card into service.

***Note:*** This procedure assumes that the Gateway cards have been properly installed in the IP-XPM, and datafilled in the switch provisioning tables (listed on page 295). The DHCP server, which provides configuration information for the Gateway cards, also must be properly installed and configured with Nortel Networks Optivity NetID (NetID) software (see Appendix A: “DHCP server guidelines”).

### Procedure: Bringing a Gateway card into service

***At the MAP terminal***

**1** Access the PM level of the MAP display and post the DTC. Type

```
>MAPCI;MTC;PM;POST DTC <DTC#>
```

and press the Enter key.

**Figure 149 MAP display example of DTC level—POST**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

DTC                        SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                    PM       0       5       1     0     11     22
2  Post_                   DTC      0       3       1     0      2      9
3  ListSet
4                          DTC 10   InSv   Links_OOS: CSide 0, PSide 6
5  Trnsl_                  Unit0: Act      InSv
6  Tst_                    Unit1: Inact    InSv
7  Bsy_                    MTC:
8  RTS_                    PM:
9  OffL                    POST:
10 LoadPM_
11 Disp_
12 Next
13 SwAct
14 QueryPM
15
16
17 Perform
18
```

**2** Display the P-side links associated with the Gateway cards. Type

```
>TRNSL P
```

and press the Enter key. The P-side links transition from off-line to manual busy (MBSY) automatically during the datafill processing for table IPINV

**Figure 150 MAP display example of DTC level—TRNSL**

```
    CM     MS     IOD   Net     PM     CCS   Lns   Trks  Ext   APPL
     .      .       .     .      .       .     .     .     .     .

DTC                          SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                PM      0       5       1      0     11     22
2  Post_               DTC     0       3       1      0      2      9
3  ListSet
4                     DTC 10   InSv   Links_OOS: CSide 0, PSide 6
5  Trnsl_             Unit0: Act      InSv
6  Tst_               Unit1: Inact    InSv
7  Bsy_               >trnsl p
8  RTS                Link 6:  IPGW TGWY 10 3  0;Cap MS;Status:MBSY
9  OffL               Link 7:  IPGW TGWY 10 3  1;Cap  S;Status:MBSY
10 LoadPM             Link 8:  IPGW TGWY 10 4  0;Cap MS;Status:MBSY
11 Disp_              Link 9:  IPGW TGWY 10 4  1;Cap  S;Status:MBSY
12 Next               Link 10: IPGW TGWY 10 5  0;Cap MS;Status:MBSY
13 SwAct              Link 11: IPGW TGWY 10 5  1;Cap  S;Status:MBSY
14 QueryPM
15
16
17 Perform
18
```

**3** RTS the P-side links. Type

```
>RTS LINK <link#>
```

and press the Enter key. (Repeat the RTS command for each link.)

**4** Display the P-side links again. The P-side links transition from MBSY to OK (in service).

**Figure 151 MAP display example of DTC level—TRNSL**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

DTC                          SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                PM      0       5       1     0     11     22
2  Post_               DTC     0       3       1     0      2      9
3  ListSet
4                     DTC 10   InSv   Links_OOS: CSide 0, PSide 0
5  Trnsl_             Unit0: Act      InSv
6  Tst_               Unit1: Inact    InSv
7  Bsy_               >trnsl p
8  RTS                Link 6:  IPGW TGWY 10 3  0;Cap MS;Status:OK
9  OffL               Link 7:  IPGW TGWY 10 3  1;Cap  S;Status:OK
10 LoadPM             Link 8:  IPGW TGWY 10 4  0;Cap MS;Status:OK
11 Disp_              Link 9:  IPGW TGWY 10 4  1;Cap  S;Status:OK
12 Next               Link 10: IPGW TGWY 10 5  0;Cap MS;Status:OK
13 SwAct              Link 11: IPGW TGWY 10 5  1;Cap  S;Status:OK
14 QueryPM
15
16
17 Perform
18
```

**5** Access the PM level of the MAP display and post the Gateway card. Type
`>MAPCI;MTC;PM;POST IPGW TGWY <Gateway frame# and unit#>`
and press the Enter key.

**6** Busy the Gateway card. Type
`>BSY`
and press the Enter key.

**Figure 152 MAP display example of IPGW level—POST**

```
    CM     MS     IOD   Net     PM     CCS   Lns   Trks  Ext   APPL
     .      .       .     .      .       .     .     .     .     .

IPGW                        SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                      PM      0       5       1     0     11     22
2  Post_                     IPGW    0       4       0     0      0      8
3
4                           IPGW TGWY 10 3 OffL Mtce Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                      POST:
8  RTS
9  OffL
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

**7** Determine if the Gateway card has a valid load. Type

```
>LOADPMQ
```

and press the Enter key.

***Note 1:*** After issuing the LOADPMQ command, ensure that the MTCE flag reappears at the MAP with the Who Am I status (MTCE: WAI/STATUS) before proceeding to the RTS step.

***Note 2:*** If LOADPMQ is not successful, refer to “Troubleshooting the Gateway” on page 308 for information on error messages and user actions.

**Figure 153 MAP display example of IPGW level—LOADPMQ**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

IPGW                          SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                 PM      0       5       1     0     11     22
2  Post_                IPGW    0       4       0     0      0      8
3
4                       IPGW TGWY 10 3 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                  >LOADPMQ
8  RTS                  LOAD QUERY HAS BEEN SUBMITTED...
9  OffL                 IPGW TGWY 10 3 PMReset/LoadPMQ Passed
10 LoadPMQ              THE IPGW CONTAINS A VALID LOAD.
11                      LOAD NAME: TOPS IP Gateway Release 3.1 AE
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

**8** Bring the Gateway card into service. Type

```
>RTS
```

and press the Enter key.

***Note:*** If RTS is not successful, refer to “Troubleshooting the Gateway” on page 308.

**Figure 154 MAP display example of IPGW level—RTS**

```
    CM     MS     IOD   Net     PM     CCS   Lns   Trks  Ext   APPL
     .      .       .     .      .       .     .     .     .     .


IPGW                          SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                PM      0       5        1     0     11     22
2  Post_               IPGW    0       3        0     0      0     9
3
4                     IPGW TGWY 10 3 InSv  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                >RTS
8  RTS                IPGW TGWY 10 3 Rts Passed
9  OffL
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

**9** You have completed this procedure. The Gateway card is in service.

## Troubleshooting the Gateway

This section provides troubleshooting information about the TOPS-IP Gateway (IPGW).

### LOADPMQ error

If the system displays the following error message in response to the LOADPMQ command, users should issue the PMRESET command (see page 312). PMRESET reloads the Gateway card. If PMRESET is not successful, refer to "PMRESET error" on page 311.

**Figure 155 MAP display example of IPGW level—LOADPMQ error message**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

IPGW                        SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                PM      0       2       1     0     11     22
2  Post_               IPGW    0       3       0     0      0      9
3
4                      IPGW TGWY 10 3 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                 >LOADPMQ
8  RTS                 LOAD QUERY HAS BEEN SUBMITTED...
9  OffL                IPGW TGWY 10 3 PMReset/LoadPMQ Failed
10 LoadPMQ             No Acknowledgement from PM
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

### RTS error

If the system displays the following error message in response to the RTS command, users should first issue the LOADPMQ command. If LOADPMQ is not successful, then issue the PMRESET command. If PMRESET is not successful, refer to “PMRESET error” on page 311.

**Figure 156 MAP display example of IPGW level—RTS error message**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

IPGW                        SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                     PM       0       5       1     0     11     22
2  Post_                    IPGW     0       3       0     0      0      9
3
4                           IPGW TGWY 10 3 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                      >RTS
8  RTS                       ** WARNING **
9  OffL                     IPGW HAS INVALID LOAD OR IS NOT YET LOADED.
10 LoadPMQ                  YOU MAY ISSUE THE LOADPMQ COMMAND TO QUERY
11                          THE IPGW FOR LOAD STATUS, OR YOU MAY ISSUE
12 Next                     THE PMRESET COMMAND TO FORCE THE IPGW TO
13                          INITIATE AUTOLOADING FROM THE LAN.
14 QueryPM
15 PMReset
16 Spares
17
18
```

### IP address mismatch error

A TOPS IPGW will not come into service if the IP address downloaded to it from table IPINV does not match the IP address assigned by the DHCP server. If the system displays the following error message in response to the RTS command, users should perform these checks:

- Verify that the DHCP server has the correct IP/MAC address association for the Gateway.
- Verify that the IP address for the Gateway is datafilled correctly in the IPZONE field in table IPINV.
- Verify that the Gateway card is installed in the correct physical location.

**Figure 157 MAP display example of IPGW level—IP address mismatch error message**

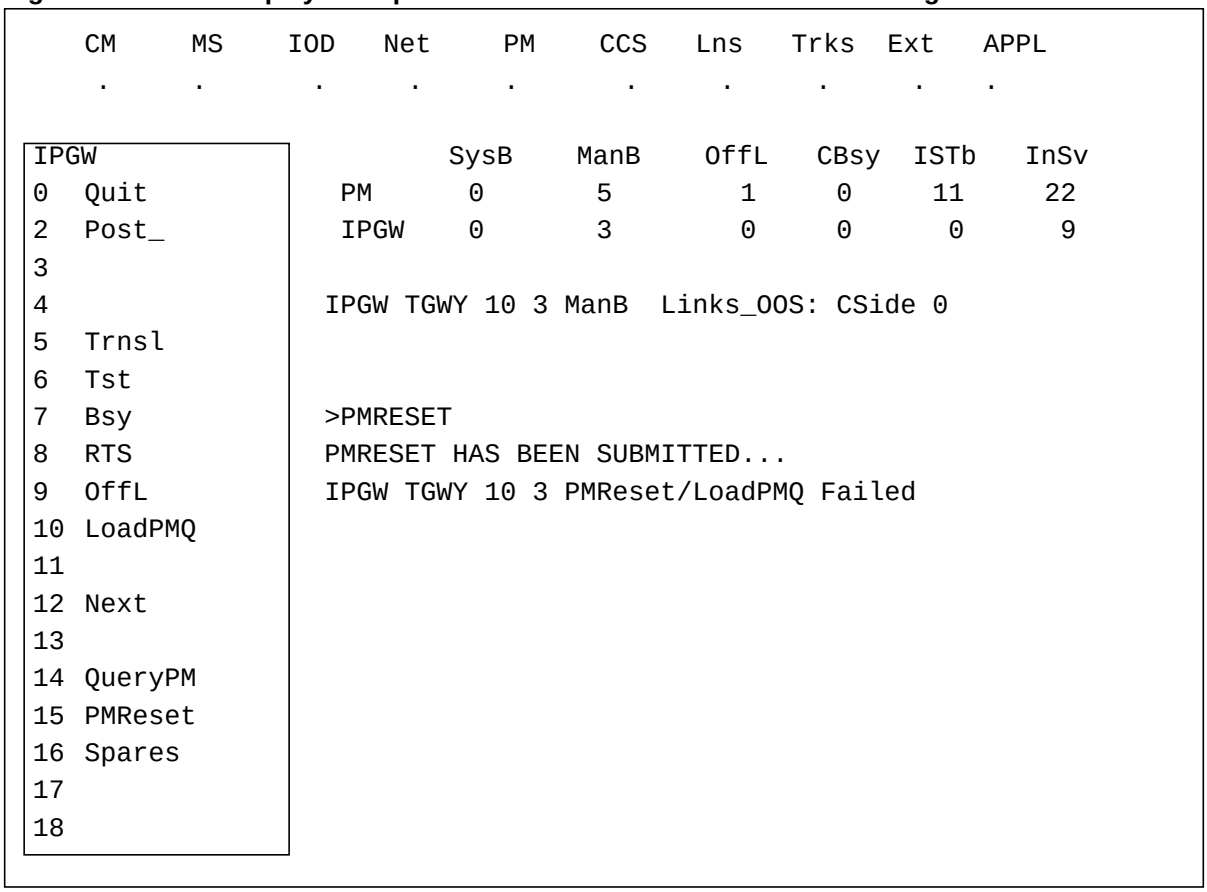
```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

IPGW                        SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                PM     0       5       1     0     11     22
2  Post_               IPGW   0       3       0     0      0      9
3
4                      IPGW TGWY 10 3 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                 >RTS
8  RTS
9  OffL                Static Data Xfer Failed
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

### PMRESET error

If the system displays the following error message in response to the PMRESET command, users should perform these checks:

- Verify that all DHCP data for the Gateway card is correct in NetID (at the DHCP server), such as the MAC address, default gateway router IP addresses, load name, and load server.
- Verify that BOOTP/DHCP relay is active on routers between the Gateway and the DHCP server.

**Figure 158 MAP display example of IPGW level—PMRESET error message**



### PMRESET success

After receiving the following success response from the PMRESET command, users should continue with the RTS step (Step 8 on page 307) of "Procedure: Bringing a Gateway card into service."

**Figure 159 MAP display example of IPGW level—PMRESET success message**

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

IPGW                          SysB    ManB    OffL   CBsy  ISTb   InSv
0  Quit                PM      0       5       1      0     11     22
2  Post_               IPGW    0       2       0      0      0     10
3
4                      IPGW TGWY 10 3 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                 >PMRESET
8  RTS                 PMRESET HAS BEEN SUBMITTED...
9  OffL                IPGW TGWY 10 3 PMReset/LoadPMQ Passed
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

***Note:*** After issuing the PMRESET command, ensure that the MTCE flag reappears at the MAP with the Who Am I status (MTCE: WAI/STATUS) before proceeding to the RTS step.

### Gateway card diagnostics

Gateway card diagnostics consist of test utilities that reside in the Gateway firmware. The diagnostics are controlled by the IP-XPM and invoked at the IPGW level. IP-XPM maintenance uses the diagnostics in a manner consistent with existing CM and XPM maintenance interfaces.

Gateway card diagnostics provide the IP-XPM maintenance system with the following capabilities:

- detect and isolate faults at the card level
- establish card sanity during in-service and out-of-service state transitions
- run audits at specific time intervals

The following diagnostics are available:

- Activity test—checks the activity of the unit in which the diagnostic is running.
- Port range test—checks the port of the Gateway card against datafill to ensure correct provisioning of the card and the validity of the port number.
- Hardware presence test—verifies that the Gateway card is present in the shelf and that the messaging and time switch cards are present and functional.
- Out-of-service (OOS) tests—check the integrity of the DS60 channels to the XPM interface of the Gateway card and verify messaging paths to the Gateway card. Out-of-service tests also execute the diagnostic set on-board the Gateway card by a maintenance request message (for example, RAM test, ROM test, address test, communication test, loopback test, and so on).
- In-service tests—test all accessible communication paths without impact to call processing and run a subset of the on-board diagnostics.

### Guidelines for troubleshooting

The following tables provide user actions for Gateway errors:

- Use Table 64 when a Gateway fails to load.
- Use Table 65 when a Gateway fails to RTS.
- Use Table 66 when a Gateway goes SYSB.
- Use Table 67 when the active LED is off.
- Use Table 68 when the active LED is blinking.
- Use Table 69 for miscellaneous error conditions.

**Table 64 Gateway fails to load**

| Error condition | User action |
|---|---|
| Gateway datafill in the CM. | Verify that Gateway datafill is correct. |
| The DHCP server is not running. | Verify that NetID application is running. |
| The DHCP server is not configured correctly. | Verify that NetID is configured for the correct load server. For example, verify that the DHCP server is on the correct subnet; verify that the MAC address is correct in NetID; and verify LAN connectivity. |
| The FTP server is not running. | Verify that the FTP application is running. |
| The Gateway load file is missing from the load server. | Place the correct load file in the load server. |

**Table 65 Gateway fails to RTS**

| Error condition | User action |
|---|---|
| There is no response from the XPM | 1. Post the Gateway at the MAP and issue the PMRESET command.<br>2. Perform an out-of-service test if RTS fails again.<br>3. Verify that Gateway datafill and hardware slots correspond. |
| The BOOTP/DHCP relay agent is not working or is incorrectly configured. | Reconfigure the router. |
| The diagnostic test fails with reason “Tst No Resources.” | Retry the RTS command. If it fails again, there may be a hardware fault. |

**Table 66 Gateway goes SYSB**

| Error condition | User action |
|---|---|
| The 7X07 self-test failed. | 1. Post the Gateway at the MAP and issue the PMRESET command.<br>2. Perform an out-of-service test. |
| The 7X07 diagnostic test failed. | There may be a hardware fault. Issue the PMRESET command and perform an out-of-service test.<br>***Note:*** For more information on Gateway diagnostics, refer to “Gateway card diagnostics” on page 313. |

**Table 67 Active LED on Gateway off**

| Error condition | User action |
|---|---|
| The Gateway did not get its load from the DHCP server. | Check that all DHCP data for the Gateway card is correct in NetID, such as the MAC address, default gateway router IP addresses, load name, and load server. |
| Gateway has no power. | Verify that the -48V fuse is in the frame supervisory panel (FSP) for the slot and shelf where the Gateway is installed. |

**Table 68 Active LED on Gateway blinking**

| Error condition | User action |
|---|---|
| Gateway is loaded or loading, but the Gateway is MANB, SYSB, or OFFL. | If MANB, return to service the posted Gateway card.<br>If SYSB, busy the posted Gateway card, issue the LOADPMQ command, and return to service the Gateway.<br>If OFFL, then busy the posted Gateway card, issue the LOADPMQ command, and return to service the Gateway. |

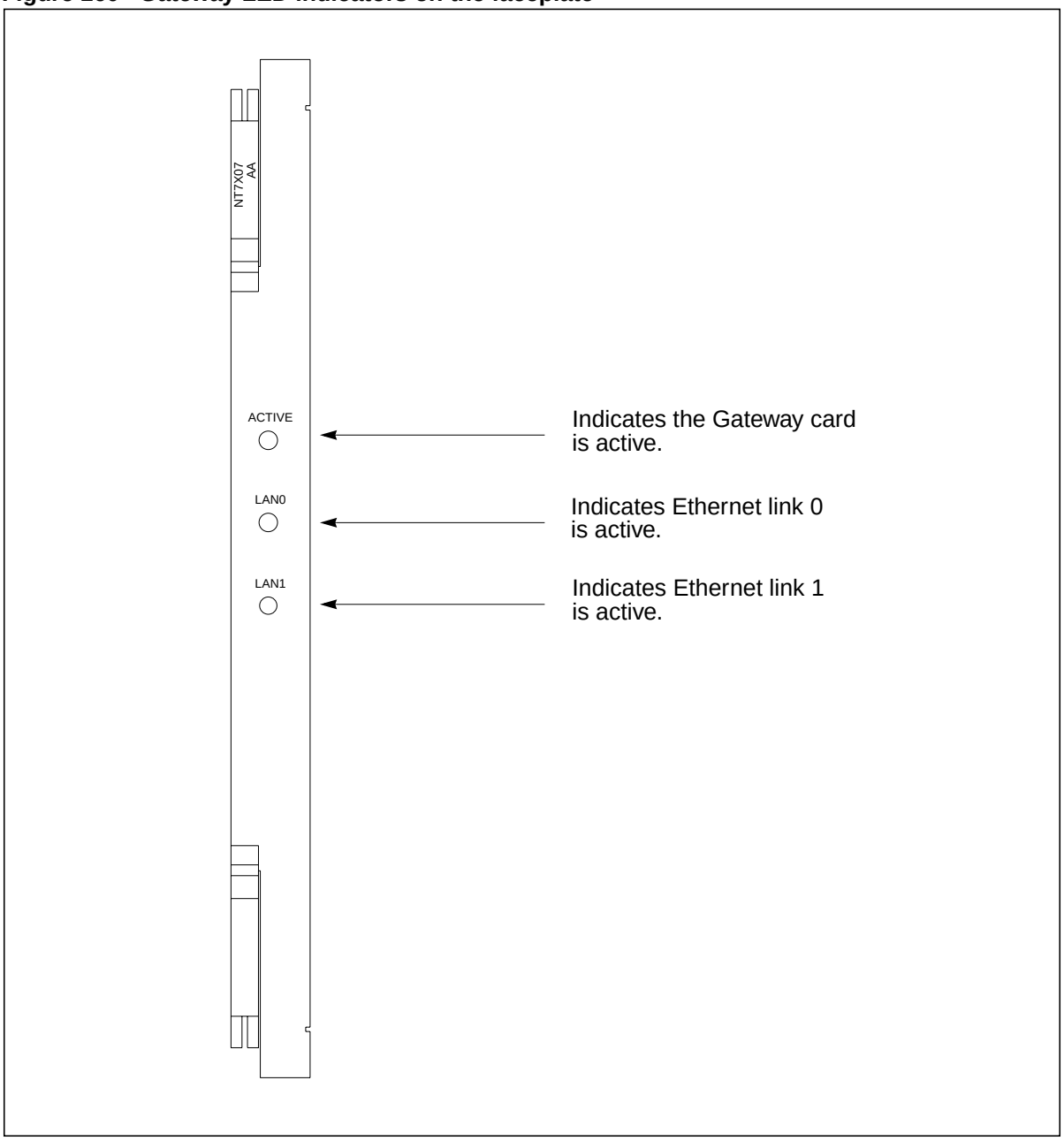
**Table 69 Miscellaneous error conditions**

| Error condition | User action |
|---|---|
| The in-service test fails. | Verify LAN connectivity by checking the Gateway LEDs. |
| LAN 0 or LAN 1 LED is off or blinking. | Verify connectivity of Gateway card, cables, and LAN switch. |
| No LEDs are lit and no power is to the Gateway. | Replace the -48V fuse in the FSP for the slot and shelf where the Gateway is installed. |

## Gateway card LED indicators

The Gateway faceplate has three LED indicators, which can be lit or blinking. Figure 160 shows the LED indicators on the faceplate.

**Figure 160 Gateway LED indicators on the faceplate**



The following table describes the possible Gateway or link states that correspond to the LED states.

**Table 70 Gateway LED indicators**

| LED | State | Explanation |
|---|---|---|
| Active | On | The Gateway card is in service. |
| Active | Off | The Gateway card did not get its load from the DHCP server. |
| Active | Blinking slowly | The Gateway card has its load but is off-line. |
| Active | Blinking fast | The Gateway card is MANB or SYSB. |
| LAN 0 | On | Ethernet 0 is getting link beat from the hub. |
| LAN 0 | Off | Ethernet 0 is not getting link beat from the hub. |
| LAN 0 | Blinking | There is a Gateway, cable, or hub hardware failure. |
| LAN 1 | On | Ethernet 1 is getting link beat from the hub. |
| LAN 1 | Off | Ethernet 1 is not getting link beat from the hub. |
| LAN 1 | Blinking | There is a Gateway, cable, or hub hardware failure. |

## Dynamic voice trunk maintenance

Two TOP-IP applications use dynamic voice trunks: OC-IP and IP positions. The maintenance strategy for dynamic trunking is based on the operation of the 7X07 Gateway cards (nodes) in the IP-XPM. Since a Gateway does not maintain any trunk information, dynamic trunks must mimic the state of the Gateway node.

This section gives an overview of the maintenance states and supported commands for dynamic trunk members and for carriers. It also discusses a method for restricting the number of available voice links.

### Supported trunk member states

The state of a trunk member depends on the state of its associated Gateway card. For example, when a user takes a Gateway out of service, all trunk members automatically update their states. So the state of the trunk members can be manipulated only through maintenance of the Gateway. Consequently, manual maintenance commands from the MTC;TRKS;TTP level of the MAP are blocked.

After bringing the Gateway card into service, its corresponding dynamic voice trunk members transition to the IDL state. Table 71 compares the Gateway states to the trunk states.

**Table 71 Gateway states and trunk states**

| Gateway | Trunk |
|---|---|
| OFFL | INB |
| MANB | CFL |
| SYSB | CFL |
| INSV | IDL (not currently call processing) |
| INSV | CPB (currently call processing) |

The following states are supported for TOPS-IP dynamic trunks:

- INB is the trunk state when the Gateway card is off-line. The Gateway card is off-line when initially datafilled, or when manually assigned to OFFL from the IPGW MAP level.
- CPD indicates the trunk is deloading because the associated Gateway card is draining.
- IDL, CPB, and UNEQ have the same meaning as they do for TDM trunks.
- RES indicates the trunk is restricted idle. TOPS-IP trunks are assigned to the RES state by the MAXCONNS (maximum connections) function. Datafill in table TOPSTOPT controls the MAXCONNS function, which limits the number of available members in a trunk group, and assigns the rest to the RES state. (For more information about the MAXCONNS function, refer to “Limiting the use of dynamic voice links” on page 200. For details on the TOPSTOPT datafill, refer to “TOPSTOPT” on page 255.)
- LO (lockout) indicates the IP-XPM has reported problems with the trunk member, and the member will not be selected by the switch. The IP-XPM attempts to resolve the lockout condition automatically. If the condition persists, it may be resolved by manually busying the Gateway card and returning it to service.
- CFL indicates that trunks are unavailable due to problems with the Gateway. The trunks will be set to CFL when the Gateway card is manually busied from the IPGW MAP level, or when the Gateway experiences problems and the switch assigns it to the SYSB state.
- INI is the default state following a restart. During system recovery of a Gateway, the INI trunks are set to IDL, after which the trunks can be used for call processing.

- MB indicates that the FRLS command has been used on the trunk to prevent it from being selected by call processing. After a FRLS command is performed on a trunk, the trunk will remain in the MB state until its associated Gateway card is busied and returned to service. This Gateway maintenance action removes 48 members from service temporarily. To avoid this service outage, the operating company should use the MAXCONNS function in table TOPSTOPT if there is a reason to limit member usage within a trunk group. (For details, refer to "Limiting the use of dynamic voice links" on page 200.)
- PMB indicates that the associated IP-XPM is out of service.

### Supported TTP commands

The following TTP commands are allowed for dynamic trunks, and have the same functions as they do for TDM trunks:

- QUIT
- POST

  ***Note:*** Posted dynamic trunks display "DYN" at the TTP MAP level.
- CKTINFO
- CKTLOC
- HOLD
- NEXT
- FRLS

  ***Note:*** FRLS ends the trunk's call and places the trunk member in the manual busy (MB) state. RTS is not supported for dynamic trunks, so the only way to return the trunk member to service is to busy and RTS the *entire Gateway card* associated with the trunk member. This action, done at the PM level, briefly removes 48 trunk members from service. A message displayed at the MAP warns users who attempt to issue the FRLS command on a TOPS-IP dynamic trunk.

### Unsupported TTP commands

The following TTP commands are *not* supported for dynamic trunks:

- SEIZE
- BSY
- RTS
- TST
- RLS
- CKT
- TRNSLVF
- STKSDR

- PADS
- LOADFW
- ROUTE

At the TTP level, sets of trunks can be posted in various ways: A for post by state; D for post by peripheral; and G for post by trunk group. If a posted set includes dynamic trunks, and the user issues the BSY ALL or RTS ALL command, the command is performed only on the TDM trunks in the set (if any).

Commands at other sublevels, such as C7TTP, are not allowed by existing checks because dynamic trunks do not meet the trunk group or signaling requirements for these levels.

The following additional commands from the MANUAL sublevel of TTP are *not* supported for dynamic trunks:

- LOSS
- TGEN
- NOISE
- OP
- TDET
- HSET
- JACK
- SGNL
- CALLTRF
- TBI

The following additional commands from the MONITOR sublevel of TTP are *not* supported for dynamic trunks:

- MONPOST
- MONLINK
- MONTALK
- CKTMON
- CPOS

The following additional commands from the DATATTP sublevel of TTP are *not* supported for dynamic trunks:

- BERT
- BTERM

### Supported CARRIER states

Gateway maintenance is interworked with carrier maintenance so that when the Gateway is out of service, the trunk carrier is taken out of service.

The following CARRIER states are supported:

- PBSY
- INSV
- MANB
- SYSB
- UNEQ
- OFFL

### Unsupported CARRIER states

The following CARRIER states are not supported:

- CBSY
- ALARM
- OS
- ML

### Supported CARRIER commands

The Gateway is treated as a remote carrier, so the commands and functions that may be used at the MTC;TRKS;CARRIER level correspond to those of a standard remote carrier.

***Note:*** Transitions to and from the off-line state must be done at the CARRIER level, not at the PM level. Other commands (for example, busying from a state other than off-line) are done at the PM level.

## IP-XPM maintenance, diagnostics, and troubleshooting

The SX05DA processor card on the IP-XPM provides IP connectivity for data messaging by TOPS-IP applications. TOPS-IP data link maintenance is performed at the various MAP levels under APPL;TOPSIP (see page 323), but standard DTC maintenance commands at the PM MAP level apply to the IP-XPM itself, as do standard DTC diagnostics.

In addition to the standard DTC maintenance and diagnostics, the IP-XPM includes software to support the SX05DA's IP functionality. Unless trouble arises, manual action is not required to enable or maintain the SX05DA's IP functionality.

The IP-XPM has a diagnostic that checks whether the SX05DA has communication with any of its default routers. This diagnostic runs automatically as part of the RTS sequence, and periodically on each unit after the unit is in service. If the active unit loses connectivity to all of its default routers, and the inactive unit does have connectivity to a default router, the XPM will auto-swact and the formerly active unit will drop to SYSB. It will recover automatically when network connectivity to the router is restored.

As with other XPMs, all CM logs should be examined if trouble occurs. A PM189 log with text "IP Net Conn Lost" indicates that the unit cannot communicate with its default router. If this log is seen together with indications that the SX05DA card is faulty (other PM logs or MAP response to QUERYPM FLT), the problem is more likely in the IP network (cabling, hub/switch, or router) than in the SX05DA itself.

***Note:*** Use of the FORCE option with the RTS command should be avoided because it causes diagnostics to be skipped and can result in a call processing outage.

## TOPSIP MAP level

The TOPSIP level of the MAP is accessed from the MAPCI;MTC;APPL level menu. It allows users to perform the following maintenance:

- The TOPSDEV command accesses the TOPSDEV MAP level used to maintain TCP/IP device application connections. For more information, refer to *TOPS and TMS Maintenance Manual*, 297-8341-550.
- The TOPSPOS command accesses the TOPSPOS MAP level used to maintain IP positions (see "IP position maintenance" on page 340).
- The OCDL command accesses the OCDL MAP level used to maintain OC-IP data links (see "OC-IP data link maintenance" on page 324).

Figure 161 shows an example of the TOPSIP MAP display.

**Figure 161 MAP display example of TOPSIP level**

```
  XAC      MS     IOD     Net     PM     CCS    Lns    Trks    Ext    APPL
   .       .       .       .       .       .     .       .      .      .

TOPSIP            OAMAP   ATMFW  SDM  SPMCP  SWMTC  SDMBIL     TOPSIP
 0 Quit             .       .     .     .      .      .          .
 2
 3 TOPSDEV
 4 TOPSPOS   OCDL   :   .     TOPSDEV:  .     TOPSPOS:  .    IPDB   :  .
 5 OCDL
 6           TOPSIP:
 7
 8
 9
10
11
12
13
14
15
16
17
18
   USER1
 Time  15:13  >
```

## OC-IP data link maintenance

The TOPS OC-IP application uses the common IP infrastructure to provide IP data and voice communication between an OC host switch and an OC remote switch. OC-IP maintenance focuses on the following areas:

- Data link connectivity (page 324)
- Maintenance states and transitions (page 326)
- Data link recovery (page 328)
- Data link end-to-end connectivity (page 328)
- OCDL level MAP commands (page 329)
- Related alarms (page 338)
- Related logs (page 339)

***Note:*** OC-IP voice communication relies on dynamic trunking and thus the maintenance strategy for voice links is based on the operation of the 7X07 Gateway cards in the IP-XPM. For more information, refer to "IP Gateway maintenance" on page 293.

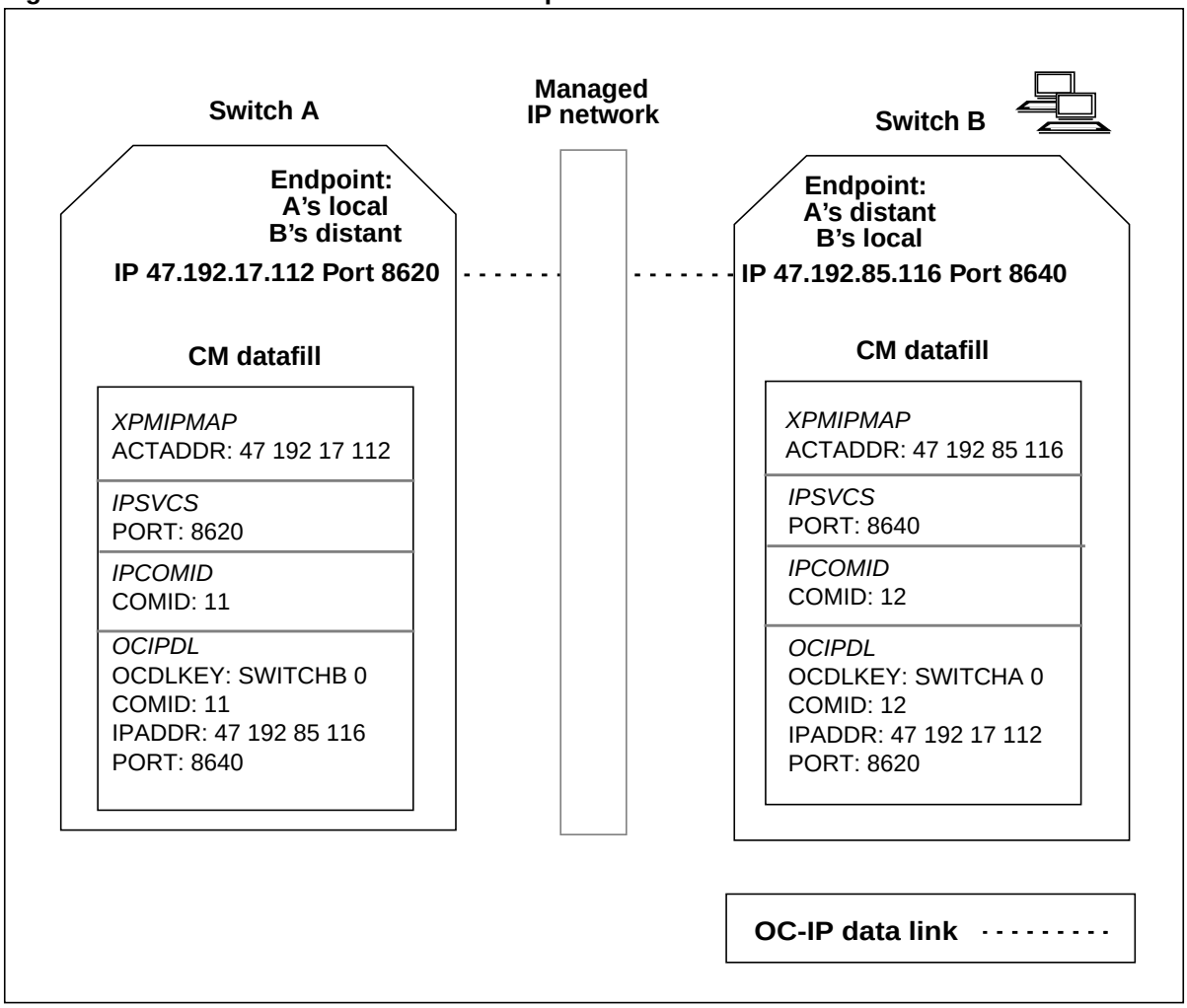
### Data link connectivity

OC-IP data links are used for OC messaging over the managed IP network to a distant switch. Multiple data links between any OC host-remote pair are provisioned for redundancy or for increased throughput capacity (or both).

An OC-IP data link does not represent any particular physical path to the distant switch. Depending on how the managed IP network is configured and managed, it is possible for messages sent on a single data link to take different routes through the network. But while the path can vary, the two endpoints are fixed. An OC switch must have datafill (using the DHCP method or the CM method) for both of the connection endpoints—the local end and the distant end—of each data link it uses.

Figure 162 shows how two OC switches (A and B) are aware of both connection endpoints through CM datafill. At either switch, the local data link connectivity information is contained in table XPMIPMAP in the ACTADDR field, and in table IPSVCS in the PORT field. The distant data link connectivity information is contained in table OCIPDL in the IPADDR and PORT fields.

**Figure 162 OC-IP data link connection endpoints and related datafill**




***Note:*** Datafill shown in Figure 162 assumes that both switches receive their IP configuration information using the CM method. When the DHCP method is used to configure the IP-XPM, the active IP address is obtained from a server in the network instead of from table XPMIPMAP. For more information, refer to "Parallel datafill for OC-IP data links" on page 91.

## Maintenance states and transitions

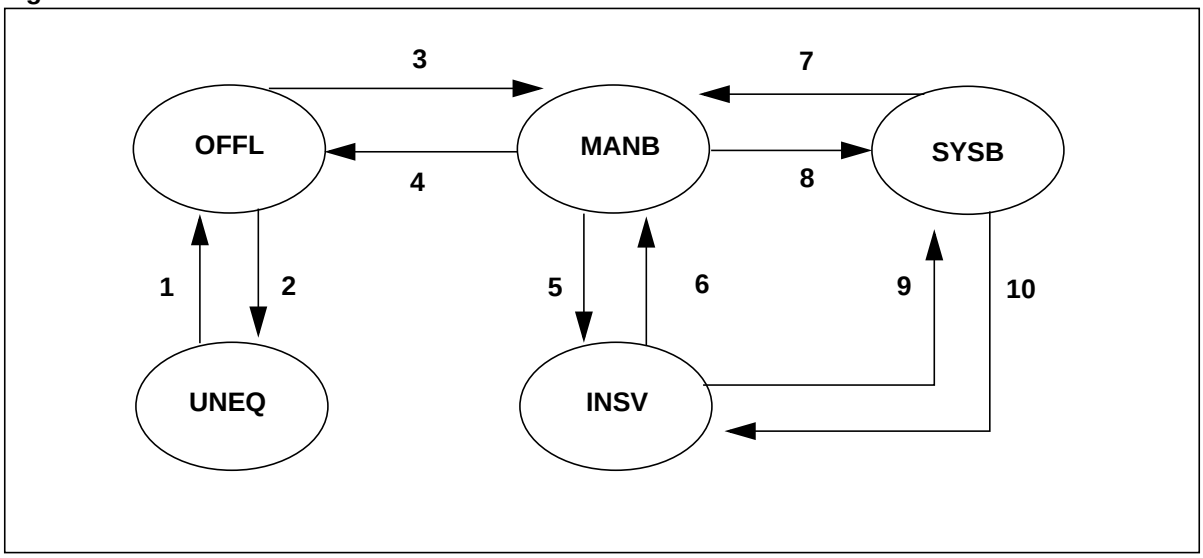
Table 72 describes the maintenance states for OC-IP data links.

**Table 72 OC-IP data link maintenance states**

| State | Description |
|---|---|
| UNEQ | Unequipped indicates the absence of datafill for the OC-IP data link in table OCIPDL. An OC-IP data link transitions to the UNEQ state when it is removed from datafill. |
| OFFL | Off-line indicates the OC-IP data link has been datafilled in table OCIPDL. Data links are initially OFFL after datafill, and must be in this state before being removed from datafill. |
| MANB | Manual busy indicates the OC-IP data link has been manually taken out of service. |
| SYSB | System busy indicates the OC-IP data link has been removed from service by the system because a fault was detected. While in the SYSB state, the data link is unavailable for call processing. Removal of all failures for the associated data link allows it to transition to the INSV state. |
| INSV | In service indicates the OC-IP data link is functioning without fault, and is ready for call processing. The following conditions must be met before the data link transitions to INSV:<br>- The SX05 (on the IP-XPM) associated with the COMID is in service.<br>- The COMID associated with the data link must be active, which means that a socket has been created and set up properly for that COMID.<br>- The local endpoint of the data link must have connectivity with the distant endpoint.<br>A failure with an INSV data link causes it to transition to the SYSB state. It takes a finite interval for the fault to be detected. |

The state transitions for OC-IP data links are shown in Figure 163. Each transition number is described following the figure. (MAP commands are described beginning on page 329.)

**Figure 163 OC-IP data link state transitions**




1 UNEQ to OFFL—The data link is datafilled in table OCIPDL.

2 OFFL to UNEQ—The data link is removed from datafill in table OCIPDL.

3 OFFL to MANB—The data link is manually busied at the MAP using the BSY command.

4 MANB to OFFL—The data link is off-lined at the MAP using the OFFL command.

5 MANB to INSV—The data link is returned to service from the MAP using the RTS command.

6 INSV to MANB—The data link is manually busied at the MAP using the BSY command.

7 SYSB to MANB—The data link is manually busied at the MAP using the BSY command.

8 MANB to SYSB—The data link fails to return to service using the RTS command.

9 INSV to SYSB—The data link has one or more faults detected.

10 SYSB to INSV—The system automatically returns the data link to service after faults are removed.

## Data link recovery

The switch performs a periodic recovery audit that attempts to bring OC-IP data links that are SYSB to the INSV state. The recovery audit interval is typically 30 seconds; however, after restarts and SWACTs the recovery audit runs every 10 seconds. The recovery audit runs in this mode for a maximum of five minutes, or until the link transitions out of the SYSB state.

The switch also attempts recovery of data links after a warm restart, cold restart, reload restart, or CM SWACT (switch of activity). The before and after state mapping is shown in Table 73.

**Table 73 State mapping**

| Before state | After state | | | |
|---|---|---|---|---|
| | **Warm restart** | **Cold restart** | **Reload restart** | **CM SWACT** |
| UNEQ | UNEQ | UNEQ | UNEQ | UNEQ |
| OFFL | OFFL | OFFL | OFFL | OFFL |
| MANB | MANB | MANB | SYSB | See Note |
| SYSB | SYSB | SYSB | SYSB | See Note |
| INSV | INSV | SYSB | SYSB | SYSB |
| ***Note:*** Before a SWACT, the switch performs status checks to ensure that all OC-IP data links on the active (old) side are in a valid state. A SWACT is prevented when a link is in the MANB or SYSB state. | | | | |

Following restarts and SWACTs, SYSB links attempt to be recovered by the periodic recovery audit.

## Data link end-to-end connectivity

While an OC-IP data link is in the INSV state, end-to-end connectivity is verified periodically through maintenance audits. When the switch audits the far-end, it waits a maximum of five seconds for a response from the far-end switch. If the auditing switch does not receive a response, this is considered an audit failure for the link. If an INSV link experiences three consecutive audit failures, the link is taken out of service and marked SYSB. (Three is the default value for parameter OCIPDL_AUDIT_THRESHOLD in table TOPSPARM, which controls the number of consecutive audit failures that will cause the system to remove a link from service.)

Whenever the switch marks a data link SYSB, it attempts to notify the switch at the distant end. When notified, the distant end of the data link goes out of service.

***Note:*** There are reasons other than audits that may cause an OC-IP data link to go SYSB. For more information refer to log report “TOPS304” on page 469.

## OCDL level MAP commands

The OCDL maintenance directory of the MAP allows users to monitor and change the state of OC-IP data links. The OCDL level is accessed from the MAPCI;MTC;APPL;TOPSIP level menu.

Figure 164 shows an example of the OCDL MAP display. In the example, the status (INSV) of the currently posted data link (DAHOST 0) is displayed along with its COMID (12). The post set contains one data link.

**Figure 164 MAP display example of OCDL level**

```
  XAC      MS     IOD     Net     PM     CCS    Lns    Trks    Ext    APPL
   .       .       .       .       .       .     .       .      .       .

OCDL              OAMAP   ATMFW  SDM  SPMCP  SWMTC  SDMBIL     TOPSIP
 0 Quit             .       .     .     .      .      .           .
 2 Post_
 3 ListSet
 4                OCDL   :   .     TOPSDEV:  .     TOPSPOS:  .    IPDB   :  .
 5
 6                Status           OffL    ManB    SysB    InSv
 7 BSY_           OCDL                3       0       0       8
 8 RTS_
 9 OffL_          DAHOST      0 COMID   12 InSv
10                Size of Post set:    1
11
12 NEXT
13
14
15
16
17
18 QOCDL_
   USER1
 Time  15:39  >
```

The next subsections provide details on parameters and responses for the OCDL MAP commands:

- QUIT (page 330)
- POST (page 331)
- LISTSET (page 332)
- BSY (page 332)
- RTS (page 333)
- OFFL (page 334)
- NEXT (page 335)
- QOCDL (page 336)
- RECREATE (unlisted) (page 337)

## QUIT

Exits user from the OCDL MAP level. When QUIT is executed successfully, control is returned to the level specified by the user.

**Table 74 QUIT parameters**

| Parameter | Definition |
|---|---|
| <nlevels> | Specifies the number of MAP levels to quit. |
| <incrname> | Specifies the MAP level increment (TOPSIP, APPL, MTC, MAPCI) that precedes the current increment in nesting. |
| ALL | Specifies to quit all MAP levels and return to the CI level. |

The following table lists common error responses, explanations, and actions.

**Table 75 QUIT responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `QUIT–Unable to quit requested number of levels`<br>`QUIT–Increment not found` | User entered an invalid level number or increment. | Re-enter the QUIT command using the correct level number or increment. |

## POST

Posts an OC-IP data link or set of OC-IP data links for maintenance purposes. Users can post data links by distant office, state, COMID, or all the data links datafilled in table OCIPDL. When POST is executed successfully, the MAP displays the first data link in the post set along with its COMID and state. The size of the post set is also shown.

**Table 76 POST parameters**

| Parameter | Definition |
|---|---|
| O <distant office> | Posts all the data links to the specified distant office. |
| O <distant office> <data link number> | Posts an individual data link to the specified distant office. |
| C <comid> | Posts an individual data link associated with the specified COMID. |
| S <state> | Posts all OC-IP data links that are currently in the specified state. |
| ALL | Posts all OC-IP data links. |

The following table lists common error responses, explanations, and actions.

**Table 77 POST responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP POST to get more information. |
| `The office is not datafilled in OCOFC`<br>`Could Not Create Post Set` | User specified a distant office that is not provisioned in table OCOFC. | Check table OCOFC for valid distant office numbers. |
| `No data links for this office are datafilled in OCIPDL`<br>`Could Not Create Post Set` | User specified a data link that is not provisioned in table OCIPDL. | Check table OCIPDL for valid data links. |
| `The data link is not datafilled in OCIPDL`<br>`Could Not Create Post Set` | User specified an office and data link combination that is not provisioned in table OCIPDL. | Check table OCIPDL. |
| `The COMID is not datafilled in OCIPDL`<br>`Could Not Create Post Set` | User specified a COMID that is not provisioned in table table OCIPDL. | Check table OCIPDL. |

**Table 77 POST responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `There are no data links in the (OffL, ManB, SysB, InSv) state`<br>`Could Not Create Post Set` | No data links are in the specified maintenance state. | View the data link counts for each maintenance state at the OCDL MAP level. |

## LISTSET

Lists all the posted data links. No parameters are used with the LISTSET command. When LISTSET is executed successfully, the MAP displays the COMID and current state of all the posted data links.

***Note:*** Subsequent changes to the state of a data link are not reflected in the previously displayed output.

The following table lists common error responses, explanations, and actions.

**Table 78 LISTSET responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `No OCDL posted` | The post set is empty. | Post a data link and re-enter the LISTSET command. |
| `LISTSET does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the LISTSET command without any parameters. |

## BSY

Manually busies the posted data link and sets its state to MANB. The BSY command is valid when the data link is in the OFFL, INSV or SYSB state. All data links in the post set can be busied using the ALL parameter. A data link that is already in the MANB state cannot accept the BSY command. When BSY is executed successfully, the data link transitions to the MANB state.

**Table 79 BSY parameters**

| Parameter | Definition |
|---|---|
| ALL | Busies all posted data links. |

The following table lists common error responses, explanations, and actions.

**Table 80 BSY responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP BSY to get more information. |
| `No OCDL posted` | The post set is empty. | Post a data link and re-enter the BSY command. |
| `Request invalid: data link is ManB` | The data link is already in the MANB state. | Use HELP BSY to get more information. |
| `Request invalid: data link is unequipped` | The data link has been removed from OCIPDL datafill. | Use HELP BSY to get more information. |
| `Request invalid: MTC already in progress for data link` | The data link is already receiving a maintenance action. | Use HELP BSY to get more information. |

When using the ALL parameter, if there are any INSV data links in the post set, the MAP displays the following warning message and requests confirmation.

**Figure 165 BSY warning message**

```
Warning: This action will take OC-IP data links out of
service and will affect Operator Services and active
calls. Are you sure you wish to proceed (Y/N)?
```

## RTS

Returns to service the posted data link and sets the state to INSV if successfully executed. If a failure is encountered, the data link transitions to the SYSB state.

The RTS command is valid only when SOC option ENSV0107 is enabled and the data link is in the MANB state. RTS is successful if the data port (socket) associated with the data link's COMID can be opened. Also, the local endpoint must have data connectivity with the distant endpoint.

**Table 81 RTS parameters**

| Parameter | Definition |
|---|---|
| ALL | Returns to service all posted data links. |

The following table lists common error responses, explanations, and actions.

**Table 82 RTS responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP RTS to get more information. |
| `No OCDL posted` | The post set is empty. | Post a data link and re-enter the RTS command. |
| `Request Invalid: data link is InSv` | The data link is already in service. | None. |
| `Request Invalid: data link is (UnEq or OffL or SysB)` | The data link must be in the MANB state to use the RTS command. | If datafill exists for the data link, BSY the data link and re-enter the RTS command. |
| `RTS Failed: <SysB Reason>` | The return to service failed due to the reason specified in the reason text. | Refer to TOPS304 log on page 469 for possible reasons and user actions. |
| `SOC option ENSV0107 must be ON to RTS an OCDL` | The TOPS-IP Oper Central SOC option is not enabled. | Ensure that ENSV0107 is set to ON before using the RTS command on the OC-IP data link. |

## OFFL

Off-lines the posted data link and sets the state to OFFL. The OFFL command is valid only when the data link is in the MANB state. A data link must be OFFL to delete its datafill in table OCIPDL. When OFFL is executed successfully, the data link transitions to the OFFL state.

**Table 83 OFFL parameters**

| Parameter | Definition |
|---|---|
| ALL | Off-lines all posted data links. |

The following table lists common error responses, explanations, and actions.

**Table 84 OFFL responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP OFFL to get more information. |
| `No OCDL posted` | The post set is empty. | Post a data link and re-enter the OFFL command. |
| `Request Invalid: data link is (UnEq or OffL or SysB or InSv)` | The data link must be in the MANB state to use the OFFL command. | BSY the data link and re-enter the OFFL command. |
| `Request invalid: MTC already in progress for data link.` | The data link is already receiving a maintenance action. | Use HELP OFFL to get more information. |

### NEXT

Displays the next data link in the post set. No parameters are used with the NEXT command. When NEXT is executed successfully, the MAP displays the next data link in the post set, along with its COMID and state.

The following table lists common error responses, explanations, and actions.

**Table 85 NEXT responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `End of post set` | The post set is empty, or there are no data links left in the post set. | None. |
| `NEXT does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the NEXT command without any parameters. |

## QOCDL

Retrieves information on the posted data link. QODCL is used only for the currently posted data link, not for the entire post set. This command is invalid if the data link is in the UNEQ state. When QODCL is executed successfully, the MAP displays the following information for the posted data link:

- data link name and number
- data link state
- SYSB reason (no failure, CM child dead, CM resource failure, peripheral failure, network failure, end to end connectivity failure)
- COMID
- name and number of the XPM
- local IP address and port (see Note 1 in Table 86)
- distant IP address and port (see Note 2 in Table 86)

**Table 86 QOCDL parameters**

| Parameter | Definition |
|---|---|
| CNTRS | Counters. Retrieves the socket information (IP address and port) from the XPM using the RSI interface. If the CNTRS parameter is not entered, the QOCDL command retrieves information from CM datafill only.<br><br>***Note 1:*** When CNTRS is *not* specified, the local IP address may be unknown if the DHCP configuration method is used. When CNTRS *is* specified the local IP address may be unknown if the CM configuration method is used or if communication to the XPM fails.<br><br>***Note 2:*** When CNTRS is specified, the distant IP address and port are not displayed, because the XPM is not aware of them. The text shows: “Not kept by the XPM.” |

The following table lists common error responses, explanations, and actions.

**Table 87 QOCDL responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `No OCDL posted` | The post set is empty. | Post a data link and re-enter the QOCDL command. |
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP QOCDL to get more information. |
| `QODCL does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the QOCDL command without any parameters. |

**Table 87 QOCDL responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `Request invalid: data link is unequipped` | User entered the command in the UNEQ state. | Datafill the data link in table OCIPDL before entering the QOCDL command. |

Figure 166 shows an example of a successful QOCDL command response at the MAP.

**Figure 166 Example of successful QOCDL command response**

```
Data Link:                DAHOST 0
Data Link State:          InSv
SysB Reason:              No Failure
COMID:                    12
XPM:                      DTC 10
Local IP Address:         47.192.3.24
Local Port Number:        8612
Distant End IP Address:   47.192.63.100
Distant End Port Number: 8606
```

## RECREATE

Recreates data link child processes if needed. No parameters are used with the RECREATE command. RECREATE is an unlisted command. When RECREATE is executed successfully, the necessary data link child processes are restarted, and the MAP displays a success message along with the number of processes that were restarted.

The following table lists common error responses, explanations, and actions.

**Table 88 RECREATE responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `RECREATE does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the RECREATE command without any parameters. |

### Related alarms

The switch raises an OCSysB alarm when an OC-IP data link transitions to the SYSB state. The OCSysB alarm is lowered if there are no longer any SYSB data links. The severity of the alarm is associated with the following conditions:

- Critical alarm—When no OC-IP data links to a given distant office are in service and at least one data link to the same distant office is SYSB.
- Major alarm—When at least one OC-IP data link to any distant office is SYSB.

The switch raises an OCManB alarm when an OC-IP data link transitions to the MANB state. The OCManB alarm is lowered if there are no longer any MANB data links. The severity of the alarm is associated with the following conditions:

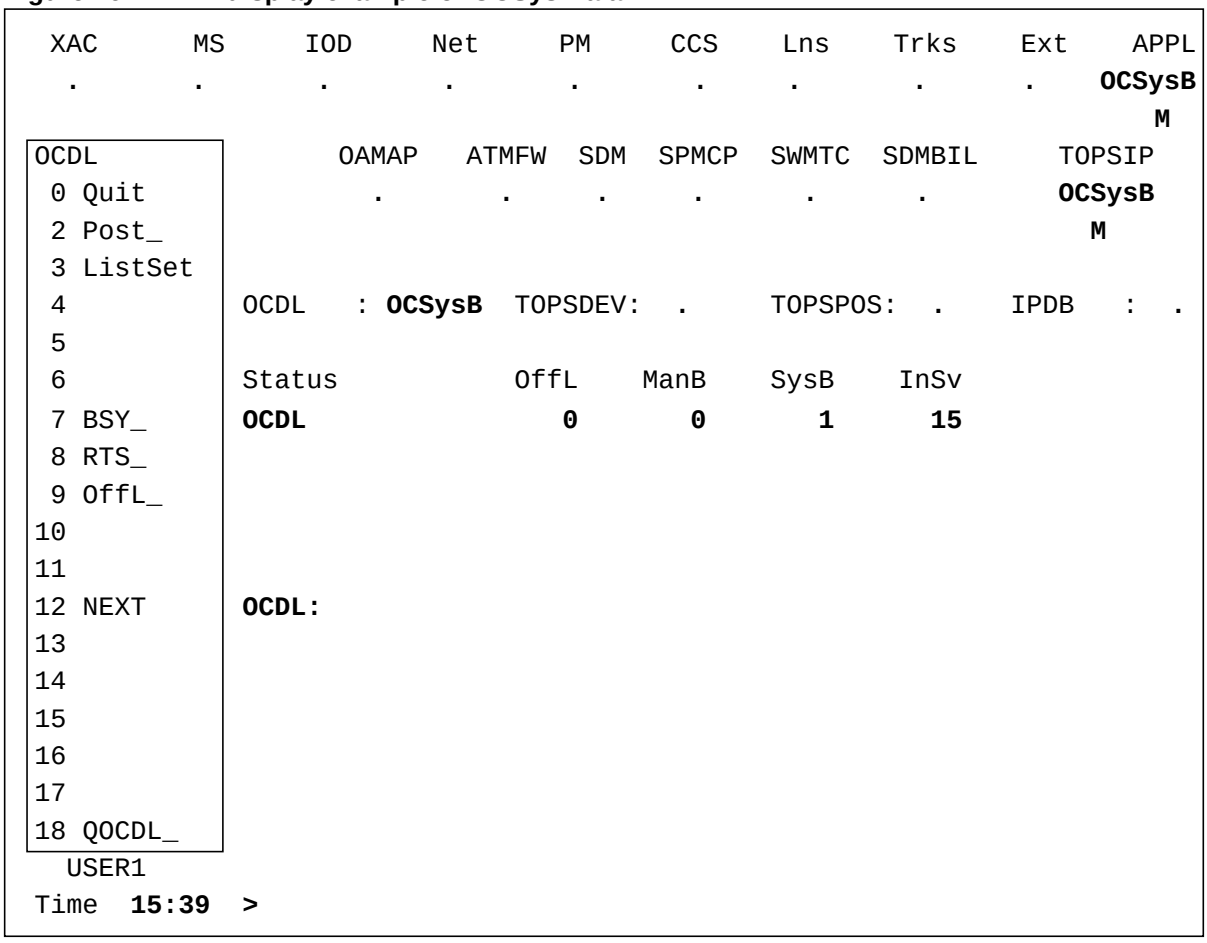
- Major alarm—When no OC-IP data links to a given distant office are in service and at least one data link to the same distant office is MANB.
- Minor alarm—When at least one OC-IP data link to any distant office is MANB.

### Display of OCSysB and OCManB alarms

The OCSysB alarm is visible at the MTC MAP level under APPL; at the APPL level under TOPSIP; and at the TOPSIP level and OCDL level beside OCDL. The OCManB alarm is visible at the same locations. The OCSysB alarm always has precedence, so the OCManB alarm is never displayed if one or more OC-IP data links are in the SYSB state.

Figure 167 shows an example of the OCSysB alarm at the MAP.

**Figure 167 MAP display example of OCSysB alarm**




***Note:*** Display of the OCSysB alarm assumes there are no other existing and more severe alarms already displayed in the maintenance and application alarm banners.

## Related logs

Three TOPS logs are related to OC-IP data link maintenance:

- A TOPS304 log is generated when an OC-IP data link enters or leaves the SYSB state.
- A TOPS504 log is generated when any OC-IP data link transitions to another state.
- A TOPS614 log is generated when the switch receives a message from an IP address or port that does not match the far-end IP address and port datafilled for the data link.

***Note:*** For examples of these logs, refer to Chapter 12: “TOPS-IP logs.”

## IP position maintenance

The IP position application uses the common IP infrastructure to provide IP data and voice communication between a DMS TOPS switch and operator positions. These positions are referred to as *IP positions*, and are datafilled and maintained at a TOPS standalone or OC host switch.

IP position maintenance includes the following areas:

- Introduction and concepts (page 340)
- Maintenance states and transitions (page 342)
- Position recovery (page 346)
- TOPSPOS level MAP commands (page 348)
- Related alarms (page 366)
- Related logs (page 368)

***Note:*** IP Position voice communication relies on dynamic trunking and thus the maintenance strategy for voice links is based on the operation of the 7X07 Gateway cards (nodes) in the IP-XPM. For more information, refer to "IP Gateway maintenance" on page 293.

### Introduction and concepts

This section provides an introduction to IP position maintenance and discusses several ways in which IP position maintenance differs from maintenance of traditional TDM-based TOPS positions.

#### Direct messaging between position and switch

Each IP position exchanges maintenance and call processing messages directly with the DMS TOPS switch over the managed IP network. This is unlike TDM positions, which use a virtual TPC and a gateway position with responsibility for providing group maintenance and for relaying messages between the position and the switch. IP positions use neither a virtual TPC nor a gateway position.

#### Maintenance state independent of voice connectivity

Whereas the maintenance state of a TDM position depends on the states of both its voice and data links, the state of an IP position depends only on the position's data connectivity to the switch. This is because an IP position has no voice connectivity to the switch when no active call is at the position. A dynamic voice link to the position is selected in the switch for each new call to the position.

#### Sockets for IP positions

Data communication between the switch and an IP position requires that a UDP socket be created and set up properly in the IP-XPM. The socket is associated with the COMID that is datafilled against the position in table TOPSPOS. The same COMID may be datafilled against many positions, so many positions can use the same socket.

***Note:*** For more information about datafilling the IP position application, refer to Chapter 4: "TOPS IP position application" and Chapter 8: "TOPS-IP data schema."

These sockets have no explicit appearance at the MAP, but they are automatically opened and closed as a result of position maintenance actions. When the first position datafilled to use a given COMID is returned to service, the corresponding socket is opened. When the last in-service position datafilled to use the COMID is manually busied, the socket is closed.

### Switch knowledge of position addresses

Whereas switch datafill specifies how to route a message to a TDM position, datafill does not specify how to route or address a message to an IP position. The switch learns the position's IP address and port from an in-service message that the position sends to the switch. An IP position cannot be brought into service at the switch until the switch has received an in-service message from the position. Positions can initiate both in-service and out-of-service state transitions at the switch, assuming their requests are compatible with the current maintenance state.

The following capabilities are possible:

- A position can use a different IP addresses for one session than it used for a previous session, without the need for a change in switch datafill.
- The service provider can use a server on the managed IP network to dynamically assign IP addresses to positions.
- A position can connect to different host switches at different times. Assuming the position is datafilled in table TOPSPOS at more than one host, it can send an in-service message to the host it wishes to connect to. Of course, the service provider can choose to datafill a position at only one host if this capability is not desired.

***Note 1:*** These capabilities have implications for system recovery, and should be used only with an understanding of those implications. Refer to "Position recovery" on page 346 for more information.

***Note 2:*** A position and its host switch must be on IP networks or subnetworks within the same IP address space. If IP positions are used with OC-IP, the OC remote switch must also be in the same address space. IP routes between these networks must exist. It is not possible to place IP positions, their host switch, or their OC-IP remote switch behind a server that performs network address translation.

Once a position has successfully come into service at a switch, the switch remembers the position's IP address until either the position is removed from datafill, or the position goes out of service and then sends a new in-service message with a different IP address. In the latter case, the switch remembers the new IP address.

### In-service and out-of-service messaging

The first time a MANB position is returned to service at the MAP, the switch ensures that the socket datafilled against the position's COMID is open, and then the switch waits for the position to send an in-service message. The switch does not learn the position's IP address and port until it receives this message, so the switch is unable to notify the position that a MAP user is attempting to bring it into service.

Once the switch has learned an IP address for a position, it attempts to notify the position whenever the position is returned to service at the MAP. The switch sends a message to the remembered IP address and port, prompting the position to send a new in-service message. Assuming the position is ready to come into service with that IP address and port, it responds with an in-service message to the switch and is quickly returned to service. However, if the position's IP address has changed while it was out of service, the position will not receive the notification that the switch sends, and the switch will have to wait until the position initiates a transition to in-service.

Similarly, the IP address that the switch has stored for each position is used in recovering the position following maintenance events such as CC warm SWACTs. For more information, refer to "Position recovery" on page 346.

Once an IP position is in service at a switch, either the switch or the position can initiate action to remove the position from service. The switch attempts to notify a position when it is manually removed from service at the MAP, so that the position can provide an appropriate display. If a position needs to remove itself from service, the position must attempt to notify the switch so that the switch can generate appropriate logs, alarms, and MAP updates.

***Note:*** Refer to *TOPS IWS Base Platform User's Guide* for the procedure for shutting down the base application in a way that ensures the position will be able to notify the switch.

## Maintenance states and transitions

The traditional RES (restricted idle) state, which means a TDM-based position is in service but not available for call processing, is not used for IP positions. Instead, IP positions introduce two new maintenance states: URES (unconnected restricted idle) and CRES (connected restricted idle). Datafill in field URESOK of table TOPSPOS affects maintenance transitions to and from the URES state.

### URES state

URES is an out-of-service state. It indicates that the socket corresponding to a position's COMID is open and the switch is ready to receive and process an in-service message from the position. When a position is in the URES state, the switch is not aware of any trouble related to the position.

A position transitions to the URES state when it is RTS'd at the MAP and the switch is waiting for the position to send an in-service message. In some cases a position can also transition to URES from an in-service state at its own request. This depends on URESOK datafill for the position, and is discussed in "Table TOPSPOS datafill for URES" on page 343.

### CRES state

CRES is an in-service state which resembles the RES state of TDM positions. It indicates that the IP position is in service but not accepting calls. When a position is in the CRES state, an operator may or may not be logged in. If an operator is logged in, either (a) the operator has chosen not to accept calls, or (b) the system has detected a problem in setting up or releasing a call at this position, and has forced the position to the CRES state.

### Table TOPSPOS datafill for URES

At the switch, table TOPSPOS contains a Y/N URESOK subfield in the DATAPATH field. At a high level, the value in URESOK indicates whether it is "OK" for the position to be in the URES state.

When URESOK=N, URES is a transient state, and the switch transitions the position to SYSB if it has been URES for more than about 15 seconds.

When URESOK=Y, a position can remain in the URES state indefinitely without transitioning to SYSB or raising alarms. This will occur if the position is RTS'd at the MAP, but does not send an in-service message to the switch.

Datafill for URESOK also affects switch handling of unsolicited out-of-service notifications from IP positions. If a position datafilled with URESOK=N sends an out-of-service notification to the switch, the switch always transitions the position to SYSB. If URESOK=Y, the position transitions to SYSB only if the notification indicates that position considers itself troubled. A position datafilled with URESOK=Y can send an out-of-service notification indicating it is not troubled, and the switch will transition the position to URES rather than to SYSB.

URESOK should be set to N if the service provider expects the position to be in-service at this switch at all times unless it has been manually removed from service at the MAP. Setting URESOK to Y may be useful for a position that connects to different switches at different times, or for a position that frequently has reason to remove itself from service and later return itself to service (perhaps with a different IP address) at the same switch.

***Note:*** Issues can arise if a position initiates a transition to or from an in-service state during a critical window of a CC warm SWACT or other major switch maintenance event. Refer to "Position recovery" on page 346 for more information.

## States and transitions

Table 89 lists and describes the maintenance states for IP positions.

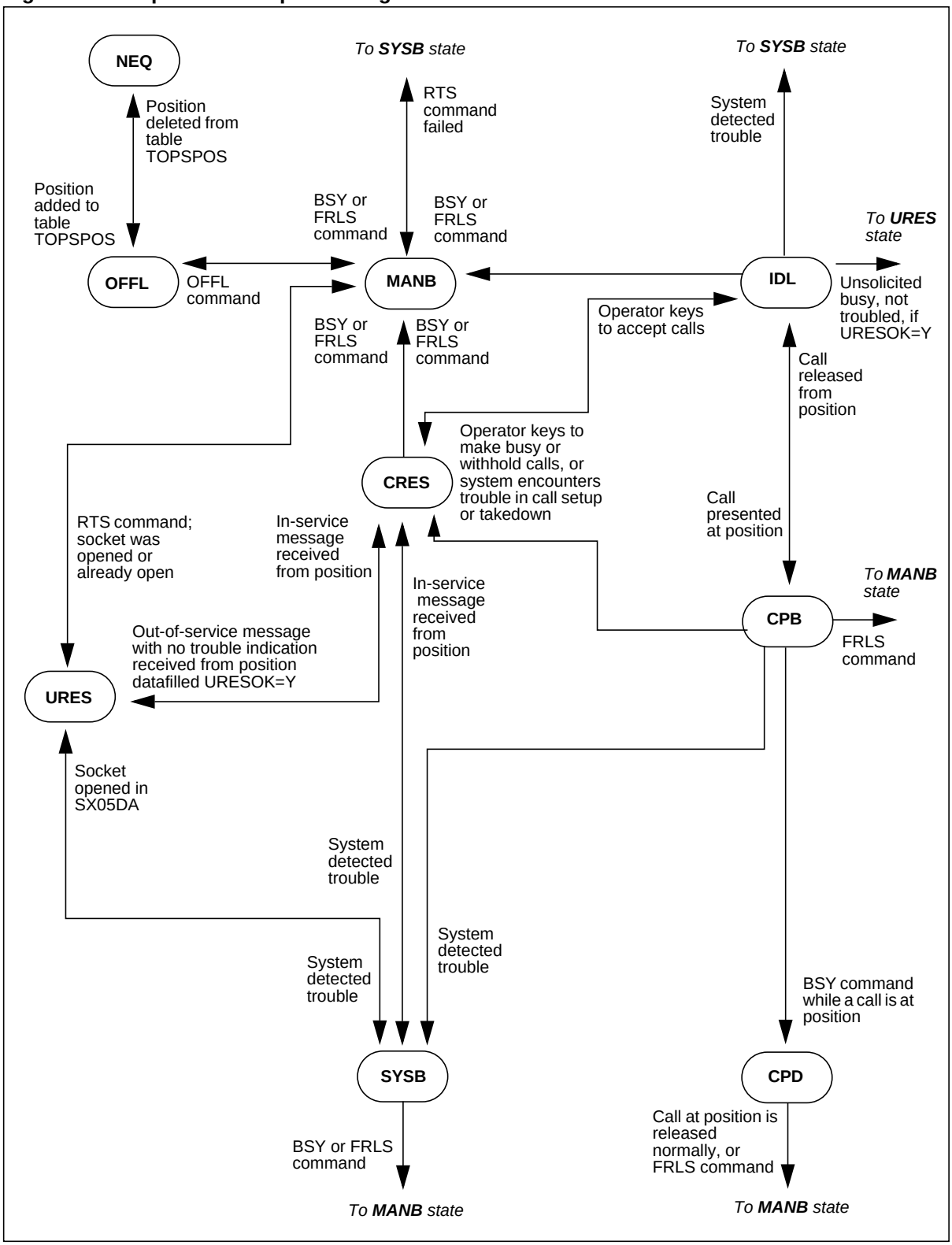
**Table 89 IP position maintenance states**

| State | Description |
|---|---|
| NEQ | Not equipped indicates the absence of datafill for the position in table TOPSPOS. This is not a true maintenance state, but it is displayed at the MAP when a position is removed from datafill while it is posted. |
| OFFL | Off-line indicates the position has been datafilled in table TOPSPOS. This state is equivalent to the INB state at the MP level of the MAP. The switch does not accept in-service requests sent by positions in this state. |
| MANB | Manual busy indicates the position has been manually taken out of service. This state is identical to the MANB state at the MP level of the MAP. The switch does not accept in-service requests sent by positions in this state. |
| URES | Unconnected restricted idle indicates the socket corresponding to the COMID datafilled against the position is open, the switch is ready to accept an in-service request message from the position, and the switch does not suspect any trouble with the position. |
| CRES | Connected restricted idle indicates the position is in service but is not accepting calls. An operator may or may not be logged into the position. |
| IDL | Idle indicates an operator is logged into the position and ready to accept a call. |
| CPB | Call processing busy indicates the position is processing a call. |
| CPD | Call processing deload indicates the position is waiting for a transition to the MANB state after completing the current call. |
| SYSB | System busy indicates the system has detected trouble with the position. For more information, refer to Table 107 on page 364. |

An overview of the state transitions for IP positions is shown in Figure 168 on page 345. In the figure, text describes each transition arrow. (MAP commands are described beginning on page 348, and various parts of this section include additional details about state transitions.)

The figure does not include some state transitions that occur over CC warm SWACTs and switch restarts in the active unit. These are described in "Position recovery" beginning on page 346. The figure also omits the transitions from IDL and CRES to CPD. These transitions occur only if the position is manually busied at the MAP when it has a held call and no active call.

**Figure 168 IP position call processing and maintenance states**



## Position recovery

This section describes how IP positions are handled over various switch recovery scenarios. This material has important implications for service providers who have positions that may be initiating actions to remove themselves from service.

### SWACT recovery

Before a CM SWACT, the switch performs status checks. These checks ensure that all IP positions on the active (old) side are in one of the following states: OFFL, URES (allowed only if URESOK=Y for the position in table TOPSPOS), CRES, IDL or CPB. A SWACT is prevented when a position is MANB, SYSB, CPD, or URES with URESOK=N in table TOPSPOS. Any such positions should be changed to OFFL.

Assuming that the status check passes, a restart on the inactive side will be done prior to the SWACT. During this restart, positions that are URES, CRES, IDL, or CPB on the active side are set to SYSB on the inactive side. (The OFFL state is preserved over SWACTs.) Each position's last known IP address is also transferred from the active to the inactive side.

Following the SWACT, the system recovery controller application for IP positions ensures that all the sockets for positions in the SYSB state are set up properly. After the sockets are set up, the SYSB positions are changed to URES and the switch attempts to notify each position that it should reset and send a new in-service request message. When the switch receives an in-service message from a position, it changes the position's state to CRES. An operator may now log into the position.

If the position is datafilled with URESOK=N in table TOPSPOS, an audit transitions it to SYSB if an in-service message is not received within 15 seconds (or longer). How frequently this audit runs depends on the availability of processor time, so it may be longer than 15 seconds before the audit detects that a position failed to send an in-service request.

### Active unit restart recovery

Operators logged into IP positions before a cold or reload restart in the active processor are automatically logged out. During the restart, IP positions that were not OFFL are changed to SYSB. Then the system recovery controller application for IP positions ensures that the sockets are set up. After that, the SYSB IP positions are changed to URES, the switch attempts to message each position at its last known IP address, and the scenario continues as it does after a CM SWACT.

### Recovery from XPM failure

This same overall strategy is used to recover IP positions in case of failure of an entire IP-XPM. The positions are made SYSB when the XPM failure occurs. Once the XPM has been recovered, the system automatically re-opens the sockets, changes the SYSB positions to URES, attempts to message each position at its last known IP address, and awaits an in-service message from each position.

### Recovery issues for positions that initiate state changes

DMS CC warm SWACT procedures were designed with the expectation that device statuses would not change during a critical window. For an ONP, the window begins with the STATUSUPDATE step of the PRESWACT and continues through the SWACT.

The expectation is the same for traditional and IP positions: with both kinds of positions, the STATUSCHECK step of PRESWACT and SWACT will report a problem with any position that does not have compatible status on the active (from) and inactive (to) processors, and the applicator must correct the problem—usually by off-lining the position on the active CPU—before the SWACT can continue.

To avoid status mismatches during ONPs and maintenance SWACTs, the service provider should ensure that positions do not initiate changes between in-service and out-of-service states during the critical maintenance window. For positions datafilled with URESOK=Y in table TOPSPOS, the safest way to avoid status mismatches may be to off-line them before the critical maintenance window begins.

## TOPSPOS level MAP commands

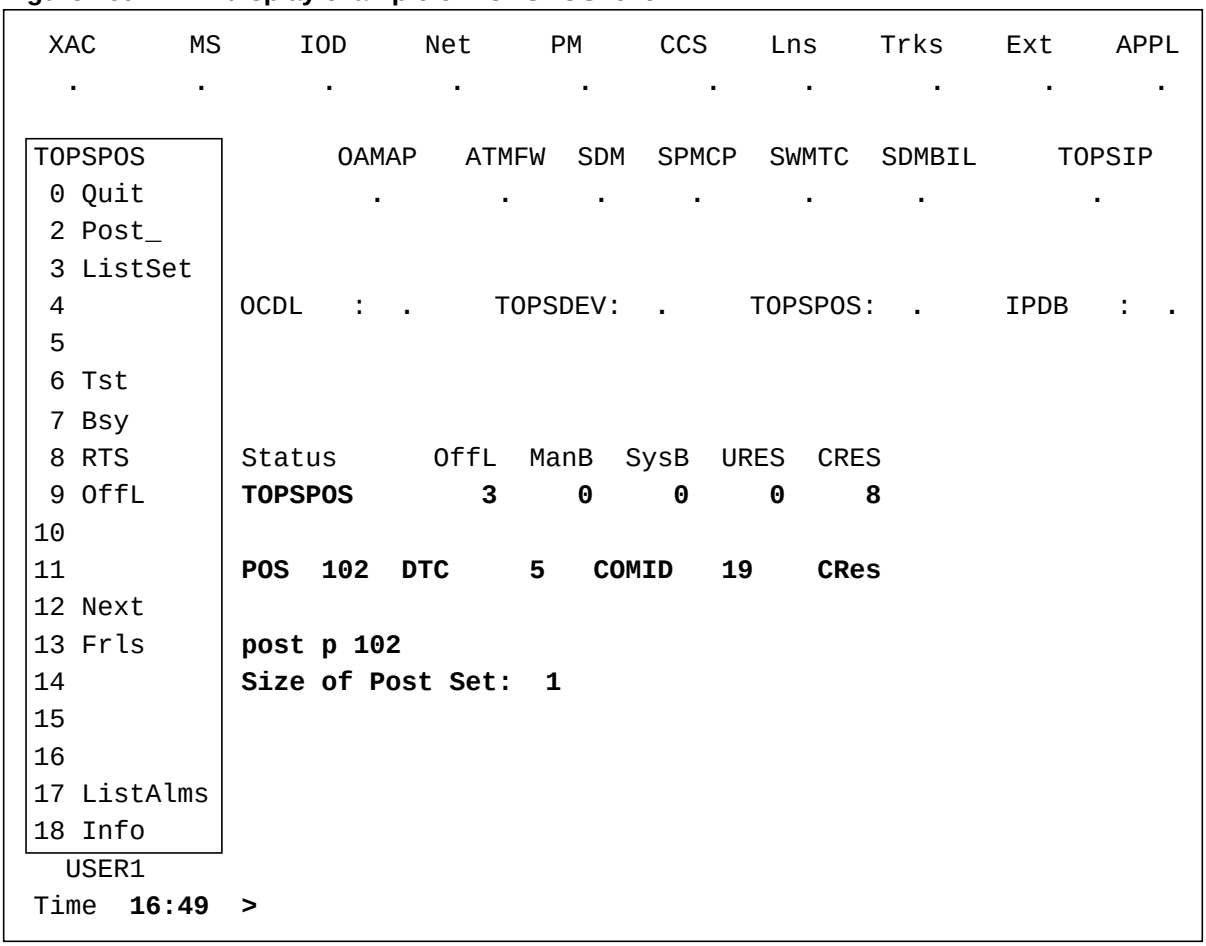
The TOPSPOS maintenance directory of the MAP allows users to monitor and change the state of IP positions. The TOPSPOS level is accessed from the MAPCI;MTC;APPL;TOPSIP level menu.

***Note:*** Only IP positions (not TDM positions) can be posted at the TOPSPOS MAP level.

Figure 169 shows an example of the TOPSPOS MAP display. In the example, the status banner about mid-screen shows the total number of IP positions in each state that is incompatible with call processing. Position 102 has been posted and is displayed along with its DTC number (5), its COMID (19), and its maintenance state (CRES). The post set contains one position.

***Note:*** This document refers to the one position that is displayed in the maintenance position as "the posted position," even if the post set contains multiple positions.

**Figure 169 MAP display example of TOPSPOS level**



The next subsections provide details on parameters and responses for the TOPSPOS MAP commands:



## QUIT

Exits user from the TOPSPOS MAP level. When QUIT is executed successfully, control is returned to the level specified by the user.

**Table 90 QUIT parameters**

| Parameter | Definition |
|---|---|
| <nlevels> | Specifies the number of MAP levels to quit. |
| <incrname> | Specifies which MAP level increment (TOPSIP, APPL, MTC, MAPCI) to quit out of. |
| ALL | Specifies to quit all MAP levels and return to the CI level. |

The following table lists common error responses, explanations, and actions.

**Table 91 QUIT error responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `QUIT -- Unable to quit requested number of levels`<br>`QUIT -- Increment not found` | User entered an invalid level number or increment. | Re-enter the QUIT command using a correct level number or increment. |

## POST

Creates a post set of IP positions for maintenance purposes, and posts the first position in the set. Users can create post sets by position number, position state, DTC number, or COMID; or all IP positions datafilled in table TOPSPOS can be included in the post set.

When POST is executed successfully, the MAP displays the posted position's associated DTC, COMID, and state. The display includes the mtce flag ("Mtce" following the other information about the position) if maintenance is in progress on the posted position. The MAP display also includes the number of positions in the post set. See Figure 169 on page 348 for an example.

**Table 92 POST parameters**

| Parameter | Definition |
|---|---|
| P <position number ...> | Posts the specified IP position or set of IP positions. |
| S <state> | Posts all IP positions that are currently in the specified state. |
| PM DTC <number> | Posts all IP positions whose data connectivity is through the specified DTC. |
| C <comid> | Posts all IP positions whose data connectivity is through the specified COMID. |
| ALL | Posts all IP positions datafilled in table TOPSPOS. |

The following table lists common error responses, explanations, and actions.

**Table 93 POST error responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters`<br>`Could not create post set` | User entered incorrect parameters. | Use HELP POST to get more information. |
| `POS <position number> not datafilled in TOPSPOS`<br>`Could not create post set` | User entered a position number that is not datafilled in table TOPSPOS. | Check table TOPSPOS for valid position numbers. |
| `POS <position number> not configured for IP in TOPSPOS`<br>`Could not create post set` | User entered a position number that is datafilled in table TOPSPOS, but not as an IP position. | Check table TOPSPOS for IP position numbers. |
| `There are no IP positions in the <state> state`<br>`Could not create post set` | User entered a valid state, but no IP positions are in that state. | None. |

**Table 93 POST error responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `No IP positions are datafilled to use DTC <number>`<br>`Could not create post set` | User entered a DTC that does not support any IP positions. | Check tables TOPSPOS and IPCOMID. |
| `No IP positions are datafilled to use COMID <comid>`<br>`Could not create post set` | User entered a COMID that is not datafilled in table TOPSPOS. | Check tables TOPSPOS and IPCOMID. |
| `No IP positions datafilled in table TOPSPOS`<br>`Could not create post set` | User entered the ALL parameter, but no IP positions are datafilled. | None. |

## LISTSET

Lists all the positions in the post set. No parameters are used with the LISTSET command. When LISTSET is executed successfully, the MAP displays the position number, DTC, COMID, and current state of each position in the post set.

***Note:*** Subsequent changes to the state of a position are not reflected in previously displayed output.

The following table lists common error responses, explanations, and actions.

**Table 94 LISTSET error responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `ListSet does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the LISTSET command without any parameters. |
| `No IP positions posted` | The post set is empty. | Post a position and re-enter the LISTSET command. |

Figure 170 shows an example of a successful LISTSET command response when the post set contains three CRES positions.

**Figure 170 Example of successful LISTSET command response**

```
POS  653 DTC    14 COMID   14 CRes
POS  900 DTC    13 COMID  133 CRes
POS 7805 DTC    14 COMID   14 CRes
```

### TST

Initiates a test on the posted position. The TST command can be successfully executed only when the position is in the CRES state. No parameters are used with the TST command.

When TST is executed successfully, the switch sends a test request to the position, displays the Mtce flag while it waits (no longer than 15 seconds) for a response, and then displays the result returned by the position.

If the position returns a failure result, it also returns a numeric failure code. The switch uses this code to index table MTCTEST and retrieve the text for the MAP response. If the code is not datafilled, the response includes the numeric code.

***Note:*** Refer to *TOPS IWS Base Platform User's Guide* for information about the failure codes IP positions can return in response to the TST command.

The following table lists common system responses, explanations, and actions.

**Table 95 TST responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `TST does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the TST command without any parameters. |
| `No position posted` | The post set is empty. | Post a position and re-enter the TST command. |
| `Request Invalid: Position must be CRES` | User issued the TST command on a position that is not in the CRES state. | If the position is in the MANB state, RTS it and re-enter the TST command after it transitions to CRES. |
| `No action taken - Mtce in progress` | Test could not be performed because other maintenance is already in progress on the posted position. | Retry after the other maintenance is completed. (The ABTK command may be used in an emergency.) |
| `Request Aborted` | The switch sent a test request to the position, but a higher-priority maintenance task preempted the task that was awaiting the response from the position. | Re-enter the TST command if the position is in the CRES state. |

**Table 95 TST responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `Request submitted`<br>`No Response, Timeout` | The switch timed out after waiting 15 seconds for the position to respond to the test request message. | Manually BSY and RTS the position. If it returns to the CRES state, re-enter the TST command. If it does not return to the CRES state, check switch and position logs, and check the position itself and net connectivity between the switch and the position. |
| `Request submitted`<br>`TST Passed` | The position indicated that the test passed. | No action is required unless a problem with the position is suspected. If a problem is suspected, other means of troubleshooting it must be found. |
| `Request submitted`<br>`<text from table MTCTEST,`<br>`for the failure code>` | The position returned a failure result, and the switch retrieved the text from the ERRTEXT field of table MTCTEST. | Action depends on the specific failure. |
| `Request submitted`<br>`No datafill for this`<br>`error code in MTCTEST.`<br>`Error code: <code>` | The position returned a failure result which is not datafilled in table MTCTEST. | Same as above. Also, consider datafilling appropriate text in switch table MTCTEST. |

## BSY

Manually busies the posted position, or all positions in the post set if the ALL parameter is used. The BSY command is valid for positions in all states except MANB and CPD.

Successful execution of the BSY command transitions a position to the MANB state and updates the MAP display accordingly. If the position is processing a call, it does not immediately transition to MANB. Instead, it transition to CPD until the call is released, and then it transitions to MANB. This applies to held calls as well as to active calls.

***Note:*** Usage SOC code OSB00102 (OPP over IP) controls the number of IP positions that can transition from OFFL to MANB.

**Table 96 BSY parameters**

| Parameter | Definition |
|---|---|
| ALL | Busies all positions in the post set. |

When the BSY command is entered with no parameters, the system response either indicates success or gives a failure reason. If the ALL parameter is used, the system first warns the user about the potential impact and asks whether the user is sure. If the user confirms, the system returns the prompt to the user while the command is still executing, and the response may not provide complete information about any failures.

The following table lists common system responses, explanations, and actions.

**Table 97 BSY responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP BSY to get more information. |
| `No position posted` | The post set is empty. | Post the position you want to busy, and re-enter the BSY command. |
| `Invalid Request, Position is MANB` | The position is already in the MANB state. | No further action is needed to BSY the position. |
| `Position is in an invalid state for the bsy command` | The position is in the CPD state, and will transition to MANB when there are no calls at the position. | The FRLS command may be used if there is an urgent need by busy the CPD position. |
| `BSY Failed:`<br>`SOC usage control exceeded` | The SOC code OSB00102 has reached its usage limit (the number of IP positions that may be used). | Increase the IP position usage limit in the SOC utility. |
| `No action taken - Mtce in progress` | Multiple users or tasks are attempting simultaneous maintenance on the posted position. This is not allowed. | Retry after the other maintenance is completed. (The ABTK command may be used in an emergency.) |
| `Improper use of this command could busy all the inservice positions in this office resulting in a severe service degradation`<br>`Are you sure you want to perform this command?`<br>`Please confirm ("YES", "Y", "NO", or "N"):` | The user has entered a BSY ALL command. If the user confirms, the system will attempt to busy all positions in the post set. | Enter Y or N depending on whether you want to proceed. |

**Table 97 BSY responses and actions**

| Response | Explanation | User action |
|---|---|---|
| <n1> requests submitted<br><n2> requests not submitted | The BSY command was entered with the ALL parameter, and the user confirmed. The MAP has submitted requests to the switch maintenance subsystem to bsy <n1> positions. There are <n2> positions in the post set for which the MAP did not submit a request to the maintenance subsystem.<br>(If either <n1> or <n2> is 0, the corresponding line is not displayed.) | If all requests were submitted, observe the banner to see whether the command succeeded, or use the LISTSET command to see the new states.<br>If any requests were not submitted, entering the BSY command with no parameters will give more information about the failure reason. |
| BSY Pending | A call is at position. The position has transitioned to the CPD state, and will transition to MANB when there are no calls at the position. | The FRLS command may be used if there is an urgent need by busy the CPD position. |
| BSY Passed | The position has transitioned to the MANB state. | None. This is a success response. |

***Note:*** When the last position datafilled to use a COMID transitions to MANB from SYSB, URES, CRES, or an in-service state, the system automatically closes the socket (in the SX05DA) that corresponds to that COMID.

### RTS

Attempts to return to service the posted position, or all positions in the post set if the ALL parameter is used. The RTS command is valid only for positions in the MANB state. The Mtce flag is displayed while execution of the RTS command is in progress for the posted position.

For positions datafilled in table TOPSPOS with field URESOK=N, successful execution of the RTS command transitions the position first to the URES state, and then to CRES. The transition to URES indicates that the system has opened the socket (in the SX05DA) corresponding to the position's COMID, or has verified that the socket is already open. Transition to CRES indicates that an in-service message from the position has been received and successfully processed. The system sets a 15-second timer when a position transitions to URES, and makes the position SYSB if an in-service message is not received before the timer expires.

For positions datafilled with URESOK=Y, successful execution of the RTS command transitions the position to the URES state. The system does not time for receipt of an in-service message or make the position SYSB if one is not received. However, the system does transition the position to CRES if an in-service message is received.

The ALL parameter can be used to return to service all positions in the post set. If the ALL parameter is used, the prompt is returned to the user while the system is waiting for any in-service messages from positions. The NOWAIT parameter causes the system to return the prompt while it is waiting for an in-service message even if the ALL parameter is not used. (NOWAIT has no effect if the ALL parameter is used, or if the position is datafilled with URESOK=Y.)

**Table 98 RTS parameters**

| Parameter | Definition |
|---|---|
| ALL | Returns to service all positions in the post set. |
| NOWAIT | Returns the prompt to the user while the system is waiting for the position to send an in-service request. |

When the RTS command is entered with no parameters, the system response either indicates success or gives a failure reason. Since using either parameter causes the prompt to be returned to the user before the command has finished executing, the system response does not provide complete information about most failures.

The following table lists common system responses, explanations, and actions.

**Table 99 RTS responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP RTS to get more information. |
| `No position posted` | The post set is empty. | Post the position you want to return to service, and re-enter the RTS command. |
| `Position must be in MANB state to RTS` | The position must be in the MANB state to use the RTS command. | If the position is OFFL, URES, or SYSB, busy it and then re-enter the RTS command. If the position is in any other state, no further action is needed to RTS the position. |

**Table 99 RTS responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `RTS Failed: XPM not Insv` | The return to service failed because the DTC on which this position's COMID is datafilled is not in service. | Check the DTC at the PM level of the MAP. |
| `RTS Failed: Failed to Open Socket` | The return to service failed because the system could not open a socket (on the SX05DA) for data communication with the position. | See "Peripheral Trouble" in Table 107 on page 364. |
| `RTS Failed: No InSv Request from Position` | A socket is open for the position, which is datafilled with URESOK=N in table TOPSPOS, and the 15-second timer expired without the DMS receiving an in-service message from the position. | Check the position itself. If the position is OK, check network connectivity between the DTC and the position. |
| `RTS Failed: Check Logs and Swers` | The return to service failed, and switch logs provide information about the failure. The INFO command may provide additional information about the failure. | Enter the INFO command, and see Table 107 on page 364.<br>Also, check DMS logs. Refer to Chapter 12: "TOPS-IP logs" for more information. |
| `RTS Failed: Request Aborted` | Execution of the RTS command was aborted, either because some higher-priority maintenance activity took precedence or because of a timeout waiting for a response from the maintenance subsystem. | Wait 15 seconds. Then if the position is still MANB, re-enter the RTS command. |
| `No action taken - Mtce in progress` | Multiple users or tasks are attempting simultaneous maintenance on the posted position. This is not allowed. | Same as above. |
| `Request submitted` | The RTS command was entered with the NOWAIT parameter, and a request has been made to the DMS maintenance subsystem. | Observe the MAP display to see whether the position transitions to the expected state. |

**Table 99 RTS responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `<n1> requests submitted`<br>`<n2> requests not submitted` | The RTS command was entered with the ALL parameter. The MAP has submitted requests to the switch maintenance subsystem to RTS <n1> positions. There are <n2> positions in the post set for which the MAP did not submit a request to the maintenance subsystem.<br>(If either <n1> or <n2> is 0, the corresponding line is not displayed.) | If all requests were submitted, observe the banner to see whether the command succeeded, or use the LISTSET command to see the new states.<br>If any requests were not submitted, entering the RTS command with no parameters will give more information about the failure reason. |
| `RTS Passed` | The RTS command was successfully entered with no parameters.<br>If the position is datafilled with URESOK=N, it is now in the CRES state, ready for an operator to log in.<br>If the position is datafilled with URESOK=Y, it is in the URES state and the system is ready to receive an in-service message from the position. | None. |

## OFFL

Off-lines the posted position, or all positions in the post set if the ALL parameter is used. The OFFL command is valid only when the position is in the MANB state. When OFFL is executed successfully, the position transitions to the OFFL state. A position must be OFFL to delete its datafill from table TOPSPOS.

**Table 100 OFFL parameters**

| Parameter | Definition |
|---|---|
| ALL | Off-lines all positions in the post set. |

When the OFFL command is entered with no parameters, the system response either indicates success or gives a failure reason. If the ALL parameter is used, the system returns the prompt to the user while the command is still executing, and the response may not provide complete information about any failures.

The following table lists common system responses, explanations, and actions.

**Table 101 OFFL responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `EITHER incorrect optional parameter(s) OR too many parameters` | User entered incorrect parameters. | Use HELP OFFL to get more information. |
| `No position posted` | The post set is empty. | Post the position you want to off-line, and re-enter the OFFL command. |
| `Request Invalid: Position must be MANB` | The position must be in the MANB state to use the OFFL command. | BSY the position and re-enter the OFFL command. |
| `No action taken - Mtce in progress` | Multiple users or tasks are attempting simultaneous maintenance on the posted position. This is not allowed. | Retry after the other maintenance is completed, if the position is still MANB. (The ABTK command may be used in an emergency.) |
| `<n1> requests submitted`<br>`<n2> requests not submitted` | The OFFL command was entered with the ALL parameter. The MAP has submitted requests to the switch maintenance subsystem to off-line <n1> positions. There are <n2> positions in the post set for which the MAP did not submit a request to the maintenance subsystem.<br>(If either <n1> or <n2> is 0, the corresponding line is not displayed.) | If all requests were submitted, observe the banner to see whether the command succeeded, or use the LISTSET command to see the new states.<br>If any requests were not submitted, entering the OFFL command with no parameters will give more information about the failure reason. |
| `OFFL Passed` | The position has been placed in the OFFL state. | None. |

### NEXT

Moves the next position in the post set to the maintenance position of the MAP display. No parameters are used with the NEXT command. When NEXT is executed successfully, the system displays the next position in the post set along with its associated DTC, COMID, and state. The system also displays the number of positions remaining in the post set.

The following table lists common error responses, explanations, and actions.

**Table 102 NEXT error responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `NEXT does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the NEXT command without any parameters. |
| `No IP positions posted` | A post set has not been created. | None. |
| `End of post set` | There are no more positions in the post set. | None. |

## FRLS

FRLS (force release) forces the posted position to the MANB state even if it processing a call. If it is, the call is taken down. No parameters are used with the FRLS command. This command is valid for positions in all states except MANB and OFFL. If the position is not processing a call, FRLS functions similarly to the BSY command.

When the FRLS command is successfully executed, the position transitions to the MANB state, and any call at the position is terminated.

The following table lists common system responses, explanations, and actions.

**Table 103 FRLS responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `FRLS does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the FRLS command without any parameters. |
| `No position posted` | The post set is empty. | Reconsider what you are trying to do. |
| `Invalid state for FRLS command` | The position is either MANB already, or OFFL. | None. |
| `No action taken - Mtce in progress` | Multiple users or tasks are attempting simultaneous maintenance on the posted position. This is not allowed. | Retry after the other maintenance is completed. (The ABTK command may be used in an emergency.) |
| `Request submitted` | The system has accepted the user's request and is in the process of forcing the position to the MANB state. | Observe the display to verify that the position transitions to the MANB state. |

## LISTALMS

Lists alarm conditions for IP positions. No parameters are used with the LISTALMS command. When LISTALMS is executed successfully, the MAP either indicates that no alarms were found, or displays a list of positions and their corresponding alarm conditions.

Alarm conditions indicate either that the position is system busy or that it has reported trouble with an external database. Refer to "Related alarms" on page 366 for more information about these alarms.

The following table lists common system responses, explanations, and actions.

**Table 104 LISTALMS responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `LISTALMS does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the LISTALMS command without any parameters. |
| `No TOPS IP position alarms found` | No IP positions are SYSB or reporting problems with an external database. | None. |
| `<pos1> <alarm1>`<br>`<pos2> <alarm2>`<br>`...`<br>(See Figure 171 for an example.) | Each listed position has the displayed alarm condition. | Table 107 on page 364 provides information about recovering SYSB positions.<br>"TPExDB alarm" on page 366 provides information about external database trouble. |

Figure 171 shows an example of a successful LISTALMS command response when positions have alarm conditions. In the example, "SysB" refers to the TPSysB alarm, and "ExDB" refers to the TPExDB alarm.

**Figure 171 Example of successful LISTALMS command response**

```
POS  670 SysB
POS  912 ExDB
POS  800 ExDB
```

### INFO

Retrieves and displays information about the posted IP position. No parameters are used with the INFO command.

The following table lists common error responses, explanations, and actions.

**Table 105 INFO error responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `INFO does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the INFO command without any parameters. |
| `No position posted` | The post set is empty. | Post the position about which you want information; then re-enter the INFO command. |

When INFO is executed successfully, the MAP displays the information shown in the table below, for the posted position.

***Note:*** Once information has been displayed by the INFO command, the display is not updated as the information changes. It is necessary to re-enter the INFO command to update the display.

**Table 106 Information displayed in response to INFO command**

| Item | Explanation |
|---|---|
| Position's current or last know IP address | The display for this item depends on context, as illustrated in the following examples.<br>If the position is in service:<br>**`Position IP Address:  95.92.20.53`**<br>If the position is out of service but has previously been in service, so that the switch "remembers" the last address:<br>**`Last Known Position IP Address:  95.92.20.53`**<br>If the position has never been in service at this switch:<br>**`Last Known Position IP Address: Unknown`** |
| IP address of the IP-XPM that supports the position | This information is available at the MAP only if the CM method is used for assigning SX05DA IP addresses, in which case it is displayed as in the following example:<br>**`XPM IP Address:  95.92.9.148`**<br>If the DHCP or BOOTP method is used, the display is as follows:<br>**`XPM IP Address: Use XIPVER/GETPMINFO for BOOTP/DHCP XPM IP COFIGs`**<br>`The XIPVER utility, which can be used to retrieve the IP configuration of an IP-XPM when the DHCP or BootP method is used, is documented in Chapter 11: "TOPS-IP CI tools." GETPMINFO is the command that retrieves the XPM's active IP address, and also other information. Before using GETPMINFO, it is necessary to bind to a COMID.` |

**Table 106 Information displayed in response to INFO command**

| Item | Explanation |
|---|---|
| Voice trunk of current active call at position | The display for this item depends on whether the position currently has a call, and if so, on whether the switch knows what voice trunk is in use for the current call. (On a host voice bypass call, the host will not know.) Following are examples:<br>Active standalone call at position, or OC host call when TDM OC is used:<br>**`Voice Trunk: CKT POSIPVL1 27`**<br>Call at position, but MAP subsystem does not know the voice trunk. (Typically this is a host voice bypass call. “Unknown” also displays when the position has a held call.)<br>**`Voice Trunk: Unknown`**<br>No call at position:<br>**`Voice Trunk: None`** |
| Operator currently logged into the position (see Note2) | The display depends on whether an operator is currently logged into the position. Following are examples.<br>If an operator is logged in:<br>**`Operator: 501`**<br>where 501 is operator number from table TQOPROF<br>If no operator is logged in:<br>**`Operator: None`** |
| Alarm conditions | Displays any alarm condition that is in effect for the position. Following are examples:<br>If the position is system busy:<br>**`Alarm Conditions: SysB`**<br>If the TPExDB alarm is in effect for the position:<br>**`Alarm Conditions: ExDB`**<br>Otherwise:<br>**`Alarm Conditions: None`** |
| SYSB reason | For positions not in the SYSB state, the display is:<br>**`SysB Reason: None`**<br>For a SYSB position, the display is:<br>**`SysB Reason: <reason>`**<br>Refer to Table 107 for a list of the possible SYSB reasons as displayed in response to the INFO command, with user actions. |

Figure 172 shows an example of a successful INFO command response at the MAP. The example is for a position that is processing a host voice bypass call on a switch that uses the CM method to assign SX05DA IP addresses.

**Figure 172 Example of successful INFO command response**

```
Position IP Address:   95.92.20.53
XPM IP Address:   95.92.9.100
Voice Trunk: Unknown
Operator: 653
Alarm Conditions:  None
SysB Reason: None
```

The following table lists the SYSB reasons that may be displayed in the response to the INFO command. Most of these reasons can also appear in the TOPS502 IP position state change log. For those that can, the following table references the documentation of the log for explanation and user actions.

**Table 107 SYSB reasons and actions**

| SysB Reason | Explanation | User action |
|---|---|---|
| Peripheral trouble | The system has not been able to open a socket for the position in the SX05DA card of the IP-XPM (DTC). | Check at the PM MAP level for any trouble with the position's DTC. After any trouble with the DTC has been resolved, return to the TOPSPOS level and BSY/RTS the position.<br>(SX05DA socket states are preserved over XPM SWACTs. So if the system has failed to open a socket, simply SWACTing the XPM will not cause the system to try again to open the socket. RTSing a position that is datafilled to use the socket will cause the system to attempt to open the socket if it is not already open.) |
| InSv request timeout | See Table 150 on page 472. | See Table 150 on page 472. |
| No response to audit | See Table 150 on page 472. | See Table 150 on page 472. |
| Unsupported BCS level | See Table 150 on page 472. | See Table 150 on page 472. |
| Unsolicited OOS notify received | See Table 150 on page 472. | See Table 150 on page 472. |
| CM-position state mismatch | See Table 150 on page 472. | See Table 150 on page 472. |
| CM-position datafill mismatch | See Table 150 on page 472. | See Table 150 on page 472. |

**Table 107 SYSB reasons and actions**

| SysB Reason | Explanation | User action |
|---|---|---|
| `Misc failure, check swers` | See Table 150 on page 472. | See Table 150 on page 472. |
| `CM restart` | This is normal for a short time following a CM SWACT or a cold or reload restart in the active unit. It is best not to manually interfere with the system recovery controller (SRC) unless the situation persists for long enough that it is clear that the SRC has failed. | Check SRC logs to determine the status of SRC recovery. Do not attempt manual maintenance while SRC recovery is in progress.<br>If the INFO command still shows this SYSB reason after the SRC has finished trying to recover the system, attempt to manually BSY and RTS the position. If that fails, the SYSB reason should change. Investigate based on the new SYSB reason. |

## ABTK

ABTK (abort task) is a hidden command that aborts any current maintenance task for posted position. No parameters are used with the ABTK command. ABTK can be executed for positions in any state.

When ABTK is successfully executed, any maintenance task that is executing for the posted position is terminated, and if the Mtce flag was displayed for the posted position, it is cleared.

The following table lists common error responses, explanations, and actions.

**Table 108 ABTK responses and actions**

| Response | Explanation | User action |
|---|---|---|
| `ABTK does NOT utilize any parameters` | User entered parameters, which are not used with this command. | Re-enter the ABTK command without any parameters. |
| `No position posted` | The post set is empty. | Reconsider what you are trying to do. |

## Related alarms

IP position alarms are associated with the following conditions:

- A TPSysB (TOPS position system busy) alarm is raised when an IP position transitions to the SYSB state.
- A TPExDB (TOPS position external database) alarm is raised when an IP position reports trouble with an external database (for example, a directory assistance database).

### TPSysB alarm

The severity level of the TPSysB alarm depends on the reason for the trouble. The alarm is major if any positions are SYSB due to peripheral trouble. Otherwise it is minor. The alarm is cleared when no IP positions are in the SYSB state.

Users can take the following steps to manually clear this alarm:

- At the TOPSPOS MAP level, enter POST S SYSB and then LISTSET to determine which positions are system busy. First attempt to manually BSY and RTS the SYSB positions. If positions remain SYSB, continue to the next step.
- For each SYSB position, the INFO command can be used to determine the SYSB reason. Also examine switch logs, especially TOPS135, TOPS 137, TOPS502, and PM logs if the SYSB reason is peripheral trouble. Investigate based on the SYSB reason and logs.

  ***Note:*** For more information about SYSB reasons, see Table 107 on page 364. For more information about the TOPS logs listed above, refer to Chapter 12: “TOPS-IP logs.”
- If the trouble cannot be corrected and the user wants to simply clear the alarm, issue the BSY command, which transitions the position state to MANB. This should be done only by experienced maintenance personnel who understand the implications.

### TPExDB alarm

The severity level of the TPExDB alarm takes into account the severities reported by all positions. For example, if position 100 reports major trouble and then position 200 reports minor trouble, the alarm will remain major. Then if position 100 either is removed from service or reports that the trouble is resolved, the alarm will drop to minor. The alarm is cleared when all positions that have reported trouble either report that the trouble is resolved or are removed from service.

Users can take the following steps to manually clear this alarm:

- At the TOPSPOS MAP level, use the LISTALMS command to determine which positions are reporting external database trouble.
- Determine the physical locations of these positions.

- Check and resolve any problems with the external database itself, and with network connectivity between the positions and the database.
- If the trouble cannot be corrected and the user wants to simply clear the alarm, all positions that are reporting external database trouble can be manually busied at the MAP. This should be done only by experienced maintenance personnel who understand the implications.

***Note 1:*** IWS datafill allows the service provider to specify whether a particular position will inform the switch if it detects a problem with connectivity to an external database. In IWS17.1, this applies to the DA database. If the service provider has other means of quickly detecting when this problem occurs, all positions should probably be datafilled to not inform the switch. Otherwise it is recommended that only a few representative positions be datafilled to inform the switch. If every position in a TOPS office were datafilled to notify the switch of external database trouble, many switch logs would be generated whenever an event occurred, and switch resources could be adversely affected.

***Note 2:*** Refer to *TOPS IWS Base Platform User's Guide* for information about datafilling positions to report, and not report, DA database connectivity problems to the switch.

### Display of alarms

The TPSysB alarm is visible at the MTC MAP level under APPL, at the APPL level under TOPSIP, and at the TOPSIP and TOPSPOS levels beside TOPSPOS.

The TPExDB alarm is visible at the MTC MAP level under APPL, at the APPL level under TOPSPOS, and at the TOPSIP and TOPSPOS levels beside IPDB.

Like all alarms, these are visible at a particular level only if no other, or more severe alarm condition is displayed in the same location. When conditions for two alarms of equal severity exist, and the alarm displays occupy the same location on the screen, the one that has been most recently detected is displayed. (The TPExDB alarm condition is considered to be detected every time a position sends a notification.)

Figure 167 shows an example of TPSysB and TPExDB alarms at the MAP. In the example, the TPExDB alarm is major, so it takes precedence under APPL and TOPSPOS.

**Figure 173 MAP display example of TPSysB and TPExDB alarms**

```
 XAC      MS     IOD     Net     PM     CCS    Lns    Trks    Ext    APPL
  .       .       .       .       .       .     .       .      .    TPExDB
                                                                        M

TOPSPOS          OAMAP   ATMFW  SDM  SPMCP  SWMTC  SDMBIL     TOPSIP
 0 Quit            .       .     .     .      .      .        TPExDB
 2 Post_                                                        M
 3 ListSet
 4           OCDL   :  .    TOPSDEV:  .    TOPSPOS: TPSysB  IPDB   : TPExDB
 5
 6 Tst
 7 Bsy
 8 RTS       Status      OffL  ManB  SysB  URES  CRES
 9 OffL      TOPSPOS       3     0     1     0     7
10
11
12 Next
13 Frls
14           TOPSPOS:
15
16
17 ListAlms
18 Info
  USER1
Time  16:50  >
```

***Note:*** The display of these alarms assumes that there are no other existing and more severe alarms already displayed in the alarm banner.

## Related logs

Four TOPS logs are directly related to IP position maintenance:

- A TOPS135 log is generated when the system attempts to open a socket for IP position data connectivity. It reports success or failure.
- A TOPS136 log is generated when an IP position reports trouble with an external database.
- The TOPS137 log provides various information that is useful in troubleshooting IP position maintenance problems.
- A TOPS502 log is generated when an IP position transitions to or from the SYSB state, unless the SYSB reason is peripheral failure.

***Note:*** For more information about these logs, refer to Chapter 12: “TOPS-IP logs.”

# TOPS QMS MIS-IP maintenance

The TOPS QMS MIS-IP application uses the managed IP network to send MIS messages from the switch to an external reporting facility (MIS server). Transmission Control Protocol (TCP) is used at the transport layer to send a 1450 byte-message.

Up to two IP connections can be provisioned in table QMSMIS. This capability allows the TOPS switch to send MIS data to more than one vendor or to increase the reliability of the MIS data sent to a single vendor.

The QMS MIS-IP application requires a dedicated IP-XPM. This IP-XPM cannot be used for other TOPS-IP applications, such as OC-IP and IP positions. It need not contain 7X07 Gateway cards (used only for voice over IP applications). For details on engineering, refer to Chapter 7: "TOPS-IP engineering guidelines."

This section summarizes possible MIS IP faults and corrections, and discusses related logs, OMs, and alarms.

***Note:*** If a switch of activity (SWACT) in the XPM occurs, QMS MIS alarms and logs are generated to indicate that the TCP connection was taken out of service. In this scenario, when the SWACT completes, the TCP connections are eventually re-established and the alarms are cleared.

## QMS MIS-IP fault detection and correction

Table 109 lists the problems that can occur while the QMS MIS application is sending messages and how the problems can be corrected. User actions are listed in the order in which to perform them.

**Table 109 QMS MIS-IP fault detection and correction**

| Fault | Detection | User action sequence |
|---|---|---|
| MIS IP child process dies and cannot be recreated | TQMS_MIS_PROCESS alarm is raised and the associated EXT108 log is generated | 1. Look for logs, software errors (swers), and traps to find the cause.<br>2. Use the MISCHILD command in the TQMIST tool to recreate the child process.<br>3. Perform a maintenance SWACT.<br>***Note:*** For details on using the TQMIST tool, refer to *Translations Guide*. |

**Table 109 QMS MIS-IP fault detection and correction**

| Fault | Detection | User action sequence |
|---|---|---|
| MIS IP interface cannot send a buffer<br>***Note:*** The MIS buffer is discarded and the MIS application keeps attempting to send subsequent buffers | QMIS102 log is generated (QMS_MIS_IP_SEND_FAIL) | 1. Ensure that the external MIS server and TCP connection are working.<br>2. Use the PING command in the XIPVER tool to determine if the MIS server is responding.<br>***Note:*** Refer to Chapter 11: TOPS-IP CI tools for details on the XIPVER tool. |
| MIS IP interface cannot close a socket | QMIS103 log is generated (QMS_MIS_CLOSESOCKET_FAIL) | Use the FORCECLOSE command in the XIPVER tool to close the open socket. |
| MIS server cannot be reached | TOPS QMS MIS alarm is raised and the associated log is generated (see Table 110 on page 370 for details) | 1. Use the PING command in the XIPVER tool to determine if the MIS server is responding.<br>2. Use the QUERYCOMID command in the XIPVER tool to query the state of the outgoing TCP port on the XPM. |
| Outgoing TCP port on the XPM is closed<br>***Note:*** The MIS application automatically tries to open the port every time a buffer is ready to be sent. | TOPS QMS MIS alarm is raised and the associated log is generated (see Table 110 on page 370 for details) | Use the QUERYCOMID command in the XIPVER tool to query the state of the outgoing TCP port on the XPM. |

## Related alarms

Four alarms are related to the TOPS QMS MIS interface (either X.25 or IP). The alarms are visible at the MAPCI;MTC;EXT level at the MAP.

Table 110 summarizes the alarms. Three alarms have associated log reports and threshold parameter settings in table TQMISOPT. When the threshold is reached, the alarm is raised and the log is generated. The alarm is cleared when the number of MIS IP connections increases above the threshold.

The fourth alarm is associated with the MIS child process. It is raised when the MIS child process dies and cannot be recreated automatically by the switch. The alarm is cleared when the child process is recreated.

**Table 110 QMS MIS alarms**

| Alarm | Associated log | Parameter in table TQMISOPT |
|---|---|---|
| TQMS_MIS_MINOR | EXT106 | QMS_MINOR_ALARM_THRESH |
| TQMS_MIS_MAJOR | EXT107 | QMS_MAJOR_ALARM_THRESH |

**Table 110 QMS MIS alarms**

| Alarm | Associated log | Parameter in table TQMISOPT |
|---|---|---|
| TQMS_MIS_CRITICAL | EXT108 | QMS_CRITICAL_ALARM_THRESH |
| TQMS_MIS_PROCESS | EXT108 | N/A |

## Related logs

In addition to the logs EXT106, EXT107, and EXT108, the following two QMIS logs are related to the QMS MIS-IP application:

- A QMIS102 log is generated the first time an IP connection is unable to transmit a TOPS QMS MIS buffer.
- A QMIS103 log is generated when a closesocket failure response is received by the TOPS QMS MIS-IP application.

***Note:*** For examples of these logs, refer to Chapter 12: “TOPS-IP logs.”

## Related OMs

The QMSMIS OM group contains eight registers related to the QMS MIS-IP application:

- BUFIP1SX
- BUFIP2SX
- BUFIP3SX
- BUFIP4SX
- BUFIP1TL
- BUFIP2TL
- BUFIP3TL
- BUFIP4TL

The first set of four registers counts the buffers that are successfully sent (SX) across the IP connection (up to four connections). The second set of four counts the total (TL) attempts to send buffers across the IP connection.

***Note:*** For details on OM groups, refer to Chapter 13: “TOPS-IP OMs.”

# Chapter 11: TOPS-IP CI tools

This chapter describes four utilities that users access at the CI (command interface) level of the MAP:

- The XIPVER tool is used to test IP-XPM data communication.
- The CONVERTCSLINKS tool is used to convert C-side 14 links.
- The IPGWSTAT tool displays information about TOPS-IP Gateways and their associated IP-XPMs, C-side links, and voice trunks.

  ***Note:*** This tool is intended to be used primarily by Nortel Networks field support.
- The TQMIST tool allows users to capture QMS MIS event messages based on specified call trace selection criteria.

## XIPVER

XIPVER is a multi-user tool that tests IP data communication through the SX05DA card on the IP-XPM. With XIPVER, users initiate User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) transactions through the IP-XPM. Up to ten sessions of the tool can be used simultaneously. XIPVER is not controlled by any SOC state. It uses non-menu commands.

***Note:*** Users should have a basic knowledge of TCP/IP internetworking before using the XIPVER tool.

This discussion focuses on the following XIPVER tool user tasks:

- datafilling the XIPVER tool at the switch
- understanding the purpose of each XIPVER command
- using the *parameter* commands to set values for the XIPVER tool parameters, such as the destination IP address and port, the outgoing data message, the packet size, timeouts, and options for route recording
- using the *connection* commands to bind and unbind the tool session, set up UDP sockets, set up TCP servers and clients, send ICMP echo requests (ping), and close connections and sockets
- using the *tracing* commands to create tracesets and enable message tracing

- using the *query* commands to query the IP-XPM or COMID (communication identifier)
- using the *miscellaneous* commands to get help, show or reset parameter values, and quit the tool session
- entering commands in a sample XIPVER session
- understanding possible error messages

## Datafilling the XIPVER tool

The XIPVER tool is provisioned in the IP data infrastructure, so datafill is required in the following tables:

- LTCINV
- XPMIPGWY
- XPMIPMAP
- IPSVCS
- IPCOMID

This section shows example XIPVER datafill in tables IPSVCS and IPCOMID. For details on the other tables, refer to Chapter 8: "TOPS-IP data schema."

### Table IPSVCS

To provision XIPVER, a service name for the tool must be present in table IPSVCS. This table specifies a port number and protocol used in data communication. The following example shows datafill for two XIPVER service names. The protocol value should be set to TCP_UDP to allow both TCP and UDP transactions.

**Figure 174 MAP display example for table IPSVCS**

```
SERVICE           PORT       PROTOCOL
-----------------------------------------------------------------
XIPVER            5000       TCP_UDP
XIPVER1           0          TCP_UDP
```

### Table IPCOMID

The XIPVER service name must be associated with a COMID in table IPCOMID. The COMID reserves a port on the IP-XPM to use for data communication. The following example shows datafill for XIPVER distributed across two DTCs.

**Figure 175 MAP display example for table IPCOMID**

```
COMID     SERVICE          XPMNAME
-----------------------------------------------------
40        XIPVER           DTC 10
41        XIPVER           DTC 11
50        XIPVER1          DTC 10
```

***Note:*** Two different COMIDs may be associated with the same service name only if they are on different XPMs, and two COMIDs may use the same XPM only if they are associated with different service names.

## Understanding the XIPVER commands

Users start an XIPVER tool session by typing “XIPVER” at the CI level of the maintenance and administration position (MAP). This section briefly describes the four groups of XIPVER commands.

### Parameter commands

The parameter commands allow the user to set specific values for the tool parameters.Table 111 lists each parameter command and the page where its description begins.

**Table 111 XIPVER parameter commands**

| Command | Purpose | Page |
|---|---|---|
| DIP | Sets the destination IP address parameter. | 378 |
| DP | Sets the destination application port number parameter. | 378 |
| MESSAGE | Sets the outgoing data message. | 379 |
| PACKETSIZE | Sets the size of packet for the PING command. | 380 |
| PINGTIMEOUT | Sets the timeout parameter for the PING command. | 381 |
| RR | Sets the record route option. | 381 |
| TIMEOUT | Sets the timeout parameter for the XIPVER commands (except CONNECT and PING, which is set using PINGTIMEOUT). | 382 |
| TTLIVE | Sets the time-to-live parameter. | 383 |

## Connection commands

The connection commands allow the user to initiate TCP and UDP transactions from the switch to a destination node in the managed IP network. Table 112 lists each connection command and the page where its description begins.

**Table 112 XIPVER connection commands**

| Command | Purpose | Page |
|---|---|---|
| CLOSE | Closes all the sockets, or the specified sockets, associated with the XIPVER tool session. | 384 |
| COMIDBIND | Binds the XIPVER tool session to a COMID datafilled in table IPCOMID. | 386 |
| COMIDUNBIND | Unbinds the COMID from the XIPVER tool session. | 387 |
| CONNECT | Establishes a TCP connection with a remote machine. | 387 |
| FORCECLOSE | Closes all the sockets, or the specified sockets, associated with a COMID. | 388 |
| PING | Sends an ICMP echo request message. | 389 |
| SEND | Sends a TCP or UDP message to a remote machine. | 391 |
| TCPSERVER | Sets up the tool as a TCP server. | 392 |
| UDPSOCKET | Sets up the tool as a UDP socket. | 392 |

## Tracing commands

The tracing commands allow the user to create tracesets and enable or disable message tracing. Table 113 lists each tracing command and the page where its description begins.

**Table 113 XIPVER tracing commands**

| Command | Purpose | Page |
|---|---|---|
| TRACESET | Sets the traceset options. | 393 |
| TRACE | Enables or disables message tracing. | 395 |

### Query commands

The query commands allow the user to query the IP-XPM and the COMID. Table 114 lists each query command and the page where its description begins.

**Table 114 XIPVER query commands**

| Command | Purpose | Page |
|---|---|---|
| GETPMINFO | Queries an Ethernet-based SX05DA XPM. | 397 |
| QUERYCOMID | Displays information about a COMID datafilled in table IPCOMID. | 398 |

### Miscellaneous commands

The miscellaneous commands allow the user to get information on the available commands, show or reset parameter values, and quit the XIPVER tool session. Table 115 lists each miscellaneous command and the page where its description begins.

**Table 115 XIPVER miscellaneous commands**

| Command | Purpose | Page |
|---|---|---|
| HELP | Displays available commands. | 400 |
| Q <command> | Displays detailed information on a specific command. | 402 |
| QUIT | Exits the XIPVER tool. | 402 |
| RESET | Resets the XIPVER tool parameters. | 403 |
| SHOW | Shows the current value of the XIPVER parameters. | 404 |
| SHOWUSERS | Shows the current users of the XIPVER tool | 404 |

## Using the parameter commands

The parameter commands (listed on page 375) allow the user to set specific values for the tool parameters. Users enter the command name followed by one or more arguments. The number of arguments depends on the parameter. Entering the command with no arguments or with incorrect arguments causes the system to respond with the current (unchanged) value of the parameter.

This section discusses the parameters (arguments) for each command and gives examples of the MAP display. In the examples, commands entered by the user appear in bold text; responses appear in plain text.

## DIP

The DIP command sets the destination IP address, which is used by the SEND, PING, and CONNECT commands. The IP address must be entered in the correct format: four integers separated by spaces; otherwise, the DIP value is not updated and the current value is output.

The DIP command has the following syntax:

```
DIP <destination IP address>
```

**Table 116 DIP parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <destination IP address> | 0 to 255 for each address part | NIL | Specifies a destination IP address. |

The following figure shows examples of the DIP command and system response.

**Figure 176 MAP display example for DIP command**

```
>DIP
DIP: NIL

>DIP 175 21 56 100
DIP: 175.21.56.100

>DIP 621
EITHER incorrect optional parameter(s) OR too many parameters.
DIP: 175.21.56.100
```

## DP

The DP command sets the destination application port number, which is used by the SEND and CONNECT commands. The port number must be a valid integer; otherwise, it is not updated and the current value is displayed.

The DP command has the following syntax:

```
DP <destination port number>
```

**Table 117 DP parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <destination port number> | 0 to 65535 | NIL | Destination port number. |

The following figure shows examples of the DP command and system response.

**Figure 177 MAP display example for DP command**

```
>DP 8078
DP: 8078

>DP
DP: 8078

>DP gvb
EITHER incorrect optional parameter(s) OR too many parameters.
DP: 8078
```

## MESSAGE

The MESSAGE command specifies the data message, which is used by the SEND command. To update the current message value, the following conditions apply:

- Users may enter the message bytes in either decimal or hexadecimal format, each byte separated by a space. Hexadecimal entries must be preceded by the # character. The system response always displays the message in hexadecimal (it converts decimal entries to hexadecimal).
- If the message entered has fewer bytes than the specified size, the tool fills up the message with FF bytes.

The MESSAGE command has the following syntax:

```
MESSAGE <message size> <data message>
```

**Table 118 MESSAGE parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <message size> | 1 to 250 bytes | NIL | Specifies the number of bytes of the message. |
| <data message> | Hex numbers | FF FF FF | The actual message in hex format with each byte separated by a space. |

The following figure shows examples of the MESSAGE command and system response.

**Figure 178 MAP display example for MESSAGE command**

```
>MESSAGE
Message unchanged
   FF FF FF

>MESSAGE 100 #43 43 53 32 #21
43 2B 35 20 21 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

>MESSAGE XXX
Message unchanged
43 2B 35 20 21 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

## PACKETSIZE

The PACKETSIZE command sets the size of the packet used by the PING command (ICMP echo request).

The PACKETSIZE command has the following syntax:

```
PACKETSIZE <size>
```

**Table 119 PACKETSIZE parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <size> | 8 to 4096 bytes | 64 | Specifies the number of bytes of the packet. |

The following figure shows examples of the PACKETSIZE command and system response.

**Figure 179 MAP display example for PACKETSIZE command**

```
>PACKETSIZE
PACKETSIZE:64

>PACKETSIZE 344
PACKETSIZE:344

>PACKETSIZE 5000
EITHER incorrect optional parameter(s) OR too many parameters.
PACKETSIZE:344
```

### PINGTIMEOUT

The PINGTIMEOUT command sets the value of the timer used by the PING command. If a response from the PING is not received before the timeout, control of the XIPVER tool returns to the user. The timeout value must be a valid integer; otherwise, the timer is not updated and the current value is displayed.

The PINGTIMEOUT command has the following syntax:

```
PINGTIMEOUT <seconds>
```

**Table 120 PINGTIMEOUT parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <seconds> | 1 to 10 | 3 | Specifies the number of seconds to wait for a response from the PING command. |

The following figure shows examples of the PINGTIMEOUT command and system response.

**Figure 180 MAP display example for PINGTIMEOUT command**

```
>PINGTIMEOUT
PINGTIMEOUT: 3

>PINGTIMEOUT 7
PINGTIMEOUT: 7

>PINGTIMEOUT 100
EITHER incorrect optional parameter(s) OR too many parameters.
PINGTIMEOUT: 7
```

### RR

The RR command sets the record route option, which is used by the PING command. When the record route option is set, the PING reply message displays the IP addresses of intermediate nodes. (For an example showing the routes in the reply message, see Figure 189 on page 390.)

***Note:*** Some routers in a path may not allow the record route (RR) option. In this case, the PING packet may be dropped by the router, which causes the command to fail.

The RR command has the following syntax:

```
RR <YES|NO|Y|N>
```

**Table 121 RR parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <YES \| NO \| Y \| N> | YES, NO, Y, N | NO | Specifies whether or not the record route option is requested when using the PING command. |

The following figure shows examples of the RR command and system response.

**Figure 181 MAP display example for RR command**

```
>RR
RR: NO

>RR Y
RR: YES

>RR T
EITHER incorrect optional parameter(s) OR too many parameters.
```

## TIMEOUT

The TIMEOUT command sets the value of the timer used by the following commands:

- CLOSE
- FORCECLOSE
- GETPMINFO
- QUERYCOMID
- SEND
- TCPSERVER
- UDPSOCKET

If a response from the command is not received by the timeout, control of the XIPVER tool returns to the user. The timeout value must be a valid integer; otherwise, the timeout value is not updated and the current value is displayed.

The TIMEOUT command has the following syntax:

```
TIMEOUT <seconds>
```

**Table 122 TIMEOUT parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <seconds> | 1 to 15 | 3 | Specifies the number of seconds to wait for a response from the XPM. |

The following figure shows examples of the TIMEOUT command and system response.

**Figure 182 MAP display example for TIMEOUT command**

```
>TIMEOUT
TIMEOUT: 3

>TIMEOUT 8
TIMEOUT: 8

>TIMEOUT 45
EITHER incorrect optional parameter(s) OR too many parameters.
TIMEOUT: 8
```

## TTLIVE

The TTLIVE command specifies the time to live parameter used by the PING command. Time to live refers to the maximum number of hops (to intermediate nodes) between the IP-XPM and the destination node.

The TTLIVE command has the following syntax:

```
TTLIVE <number of hops>
```

**Table 123 TTLIVE parameters**

| Parameter | Range of values | Default value | Explanation |
|---|---|---|---|
| <number of hops> | 1 to 10 hops | 4 | Specifies the maximum number of hops to the destination node. |

The following figure shows examples of the TTLIVE command and system response.

**Figure 183 MAP display example for TTLIVE command**

```
>TTLIVE
TTLIVE: 4

>TTLIVE 8
TTLIVE: 8

>TTLIVE C
EITHER incorrect optional parameter(s) OR too many parameters.
TTLIVE: 8
```

## Using the connection commands

The connection commands (listed on page 376) allow the user to initiate TCP and UDP transactions from the switch to a destination node in the managed IP network. This section discusses the parameters (arguments) for each command and gives examples of the MAP display.

### CLOSE

The CLOSE command disconnects all connections and closes all open sockets associated with the XIPVER session COMID. If a particular socket number is specified, CLOSE closes only that socket.

***Note 1:*** Closing the listening socket of a TCP server closes *all* sockets associated with the server.

***Note 2:*** CLOSE does not close sockets that are associated with other applications or other XIPVER sessions. However, FORCECLOSE (page 388) can be used for this purpose.

***Note 3:*** The CLOSE command is invalid if no connections or sockets are currently open.

The CLOSE command has the following syntax:

```
CLOSE
CLOSE <socket number>
```

**Table 124 CLOSE parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <socket number> | -1 to 32767 | Specifies the socket to close. A value of -1 closes all sockets associated with the COMID.<br>***Note 1:*** A value of -1 is recommended for users who want to close all resources associated with a COMID.<br>***Note 2:*** When no parameter is specified with the CLOSE command, all sockets are closed. |

The following figure shows examples of the CLOSE command and system response. In the example, the XIPVER tool is already set up as a TCP server.

***Note 1:*** The CLOSE command requires confirmation.

***Note 2:*** When closing a TCP client that has a fixed port (instead of 0), a delay occurs in closing the socket.

**Figure 184 MAP display example for CLOSE command**

```
>CLOSE
This command will close all connections and sockets associated with XIPVER tool
Are you sure you want to continue? (Yes/No)
Please confirm (“YES”, “Y”, “NO”, or “N”)
>Y
14:55:06.778 Closed all sockets and connections associated with COMID 100

>CLOSE 12
This command will close all connections and sockets associated with socket 12
Are you sure you want to continue?(Yes/No)
Please confirm (“YES”, “Y”, “NO”, or “N”)
>Y
12:56:06.986 Closed socket 12 and all connections associated with it.

>CLOSE
14:36:48:668 CLOSE request denied: the XIPVER tool does not have any
connections or sockets to close.
```

## COMIDBIND

To initiate TCP, UDP, and ICMP transactions using the XIPVER tool, the user must *bind* the tool session to a particular COMID. The COMID, datafilled first in table IPCOMID, associates an XPM port with an IP service.

The COMIDBIND command, when used with a COMID value, binds the XIPVER tool session to the specified COMID. To be valid, the COMID must be present in table IPCOMID and not in use by any other application.

***Note 1:*** Each XIPVER session can be bound to *only one unique* COMID. To change the COMID associated with the session, first issue the COMIDUNBIND (page 387) command. Then re-issue the COMIDBIND command with a different COMID.

***Note 2:*** No datafill changes (IPSVCS and IPCOMID) are allowed to the COMID after it is bound. Changes are allowed after using the COMIDUNBIND command or after quitting the XIPVER tool session.

The COMIDBIND command has the following syntax:

```
COMIDBIND
COMIDBIND <comid>
```

**Table 125 COMIDBIND parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <comid> | 0 to 1023 | Specifies the COMID to bind to the XIPVER tool session. |

The following figure shows examples of the COMIDBIND command and system response.

**Figure 185 MAP display example for COMIDBIND command**

```
>COMIDBIND
COMID: NIL

>COMIDBIND 40
COMID: 40

>COMIDBIND 8679
EITHER incorrect optional parameter(s) OR too many parameters.
COMID: 40

>COMIDBIND 47
21:22:10.392 COMIDBIND request denied: COMID 47 is already bound to
another application

>COMIDBIND 100
21:22:16.926 COMIDBIND request denied: COMID 100 is not datafilled in
table IPCOMID
```

### COMIDUNBIND

The COMIDUNBIND command unbinds the XIPVER session from its bound COMID. Unbinding also closes all connections and sockets that are associated with that COMID. This command has no parameters.

The COMIDUNBIND command has the following syntax:

```
COMIDUNBIND
```

The following figure shows examples of the COMIDUNBIND command and system response.

**Figure 186 MAP display example for COMIDUNBIND command**

```
>COMIDUNBIND
21:22:36.875 XIPVER tool unbound from COMID 40
COMID: NIL

>COMIDUNBIND E
The COMIDUNBIND command takes no arguments.
COMID: NIL
```

### CONNECT

The CONNECT command creates a TCP client by establishing a TCP connection with a destination node. It uses the current parameter values for destination IP address (set with the DIP command) and destination port (set with the DP command). The CONNECT command has no parameters.

***Note 1:*** The XIPVER tool should not already be set up as a TCP client, TCP server, or UDP socket before using the CONNECT command.

***Note 2:*** Before using the CONNECT command, ensure that values are set for the DIP and DP parameters.

***Note 3:*** The XIPVER tool always uses a timeout of 30 seconds to wait for a response from the CONNECT request before failing.

The CONNECT command has the following syntax:

```
CONNECT
```

The following figure shows examples of the CONNECT command and system response. The tool waits 30 seconds for a response from the XPM.

**Figure 187 MAP display example for CONNECT command**

```
>CONNECT
10:40:39.148 TCP Client created: Connected to 190.32.43.54:1044

>CONNECT
10:40:39.148 CONNECT request denied: XIPVER tool already setup as a UDP socket

>CONNECT
10:20:01.300 CONNECT request failed: No response received from XPM with in 30
seconds
```

## FORCECLOSE

The FORCECLOSE command closes all open sockets associated with a particular COMID, regardless of the application to which the COMID is bound. If a socket number is specified, FORCECLOSE closes only that socket.

***Note 1:*** Caution should be taken when issuing the FORCECLOSE command, because affected sockets may be in use by other applications.

***Note 2:*** Closing the listening socket of a TCP server closes *all* sockets associated with the server.

The FORCECLOSE command has the following syntax:

```
FORCECLOSE <comid> ALL
FORCECLOSE <comid> SOCKET <socket number>
```

**Table 126 FORCECLOSE parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <comid> | 0 to 1023 | Specifies the COMID to forceclose. |
| ALL | ALL | Specifies all sockets. |
| <socket number> | 0 to 32767 | Specifies the socket to forceclose. |

The following figure shows examples of the FORCECLOSE command and system response.

***Note:*** The FORCECLOSE command requires confirmation.

**Figure 188 MAP display example for FORCECLOSE command**

```
>FORCECLOSE 40 ALL
This command will close ALL sockets and connections associated with COMID 40
Are you sure you want to continue? (Yes/No)
Please confirm (“YES”, “Y”, “NO”, or “N”)
>Y
13:02:38.252 Force closed all sockets and connections associated with COMID 40

>FORCECLOSE 40 SOCKET 333
13:02:38.252 Force closed Socket 333 of COMID 40 and all connections associated
with it.
```

## PING

The PING command sends an ICMP echo request message to a destination node. PING uses the current parameter values set by the following commands:

- DIP (destination IP address)

  ***Note:*** The destination IP address may be specified as an argument to the PING command, which overrides the current value of DIP.

- PACKETSIZE (size of packet)
- PINGTIMEOUT (ping timer)
- RR (record route option)
- TTLIVE (time to live)

The PING command has the following syntax:

```
PING
PING IP <destination IP address>
PING DNS <DNS address>
```

**Table 127 PING parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| IP <destination IP address> | 0 to 255 for each address part | Specifies a destination IP address for the PING (overrides the IP address set with the DIP parameter). |
| DNS <DNS address> | Up to 100 ASCII characters | Specifies a DNS address for the PING. The address must be delimited by single quotes. |

The following figure shows examples of the PING command and system response. In the third example the RR option is set to Y, so the next system response shows the hops in the route.

***Note:*** When RR is ON, elapsed time is shown in 10 ms increments.

**Figure 189 MAP display example for PING command**

```
>PING
DIP: 47.129.13.40
10:44:18.860 ICMP Echo Request sent to machine 47.129.13.40
10:44:19.130 ICMP Echo Response from machine 47.129.13.40

>PING
DIP: 47.142.226.100
0:44:18.860 ICMP Echo Request sent to machine 47.142.226.100
PING request failed: No response received from XPM within 2 seconds

>RR Y
RR: YES

>PING IP 198.43.54.48
DIP: 198.43.54.48
10:44:18.860 ICMP Echo Request sent to machine 198.43.54.48
10:44:19.130 ICMP Echo Response from machine 198.43.54.48
Route:
176.24.68.102
176.24.53.102
198.43.54.48
176.24.53.102
176.24.68.102
Elapsed Time: 0

>RR N
RR: NO

>PING DNS 'WNC6724'
DNS: WNC6724
10:44:18.860 ICMP Echo Request sent to machine 47.129.13.48
10:44:19.130 ICMP Echo Response from machine 47.129.13.48
```

### SEND

The SEND command sends the data message to the destination node using either TCP or UDP. SEND uses the current parameter values set by the following commands:

- DIP (destination IP address)
- DP (destination port)
- MESSAGE (data message)

Before using SEND, the XIPVER tool must be set up in one of the following ways:

- as a TCP client with the CONNECT command (page 387)
- as a TCP server with the TCPSERVER command (page 392)

  ***Note:*** If the tool is set up as a TCP server, SEND requires the optional socket number parameter.
- as a UDP socket with the UDPSOCKET command (page 392)

The SEND command has the following syntax:

`SEND` (used for TCP client or UDP socket)
`SEND <socket number>` (used for TCP server)

**Table 128 SEND parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <socket number> | 0 to 32767 | Specifies the socket number. |

The following figure shows examples of the SEND command and system response. The first example is for a TCP server; the second example is for a TCP client or UDP socket.

**Figure 190 MAP display example for SEND command**

```
>SEND 99
10:48:14.332 Message of size 20 sent thru socket 99
79 02 11 00 2D 03 01 07 49 02 A0 00 02 00 15 14 02 02 01 04

>SEND
10:44:35.510 Message of size 50 sent to 210.90.56.11:9000
D2 A0 00 02 00 15 1C 01 04 0F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

### TCPSERVER

The TCPSERVER command sets up the XIPVER tool as a TCP server. After creating the TCP server, the XPM accepts connection requests (for up to ten clients) on behalf of the TCP server. The TCPSERVER command has no parameters.

***Note:*** The XIPVER tool should not already be set up as a TCP client, TCP server, or UDP socket before using this command.

The TCPSERVER command has the following syntax:

```
TCPSERVER
```

The following figure shows examples of the TCPSERVER command and system response.

**Figure 191 MAP display example for TCPSERVER command**

```
>TCPSERVER
15:10:03.280 TCP server created

>TCPSERVER
TCPSERVER request failed: ADDRESS IN USE
```

### UDPSOCKET

The UDPSOCKET command sets up the XIPVER tool as a UDP socket. The command has no parameters.

***Note:*** The XIPVER tool should not be set up as a TCP client, TCP server, or UDP socket before using this command.

The UDPSOCKET command has the following syntax:

```
UDPSOCKET
```

The following figure shows examples of the UDPSOCKET command and system response.

**Figure 192 MAP display example for UDPSOCKET command**

```
>UDPSOCKET
13:06:58.499 UDP socket created

>UDPSOCKET
UDPSOCKET request failed: XIPVER tool already setup as a UDP socket
```

## Using the tracing commands

The tracing commands (listed on page 376) allow the user to create tracesets and enable or disable message tracing. This section discusses the parameters (arguments) for each command and gives examples of the MAP display.

### TRACESET

The TRACESET command specifies options for tracesets that are used in message tracing. The user can specify up to 10 tracesets. Each traceset can be configured to trace messages based on COMID, destination IP address, or XPM. Message tracing can be further refined on direction (incoming, outgoing, or both). Tracesets also can be configured to trace packets.

***Note 1:*** When message tracing is enabled, XIP log reports display the information captured on the traced messages. Users can view these logs with the LOGUTIL command. Refer to page 396 for an example log report.

***Note 2:*** The values for the TRACESET parameter are shared among all open XIPVER tool sessions.

***Note 3:*** Large messages between the CM and XPM are broken into packets.

***Note 4:*** Tracing messages may affect real-time performance.

The TRACESET command has the following syntax:

```
TRACESET ALL CLEAR
TRACESET SET <set number> CLEAR
TRACESET SET <set number> MESSAGE COMID <comid> <direction>
TRACESET SET <set number> MESSAGE IP <IP address> <direction>
TRACESET SET <set number> MESSAGE XPM <type> <number> <direction>
TRACESET SET <set number> MESSAGE ALL <direction>
TRACESET SET <set number> PACKET ALL <direction>
```

**Table 129 TRACESET parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| ALL | ALL | Specifies all tracesets, all messages, or all packets. |
| SET <set number> | 0 to 9 | Specifies a particular traceset. |
| CLEAR | CLEAR | Clears all tracesets or the specified traceset. |
| MESSAGE | MESSAGE | Specifies tracing of messages. |
| PACKET | PACKET | Specifies tracing of packets. |
| COMID <comid> | 0 to 1023 | Specifies message tracing for a particular COMID. |

**Table 129 TRACESET parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| IP <IP address> | 0 to 255 for each address part | Specifies message tracing for a particular IP address.<br>***Note:*** This is the IP address of the remote node. |
| XPM <type> <number> | DTC, PDTC<br>0 to 255 | Specifies message tracing for a particular XPM. |
| Direction | IN, OUT, BOTH | Specifies the direction of tracing: incoming, outgoing, or both.<br>***Note:*** When used with the IP parameter, message tracing is supported only on the incoming (IN) direction. |

The following figure shows examples of the TRACESET command and system response. In the last example, the user tried to change a non-nil traceset.

***Note:*** When users change the traceset criteria after enabling message tracing, tracing is still enabled and the tool uses the new criteria.

**Figure 193 MAP display example for TRACESET command**

```
>TRACESET SET 0 MESSAGE COMID 12 IN
TRACESET 0: MESSAGES COMID 12 DIRECTION IN

>TRACESET SET 1 PACKET ALL BOTH
TRACESET 1: PACKETS ALL DIRECTION BOTH

>TRACESET SET 2 MESSAGE XPM DTC 20 OUT
TRACESET 2: MESSAGES XPM DTC 20 DIRECTION OUT

>TRACESET SET 4 MESSAGE IP 47 142 226 116 IN
TRACESET 4: MESSAGES IP 47.142.226.116 DIRECTION IN

>TRACESET SET 5 CLEAR
TRACESET 5: NIL

>TRACESET ALL CLEAR
ALL TRACESETS: CLEARED

>TRACESET SET 6 MESSAGE ALL DIRECTION IN
There is a criteria already specified for trace set 6
Are you sure you want to continue? (Yes/No)
Please confirm: (“YES”, “Y”, “NO”, or “N”):
>Y
TRACESET 6: MESSAGES ALL DIRECTION IN
```

## TRACE

The TRACE command enables or disables message tracing. TRACE is used with the TRACESET command (page 393), which sets the options for the tracesets.

***Note 1:*** The values for the TRACESET parameter are shared among all open XIPVER tool sessions.

***Note 2:*** Because message tracing may affect real-time performance, it is recommended that tracing be disabled after the tracing session is finished.

With message tracing enabled, an XIP log report displays message information:

- service name
- COMID
- XPM name and number
- message identifier
- destination or source IP address
- destination or source port
- operation code
- message data

The TRACE command has the following syntax:

```
TRACE <activation> SET <set number>
TRACE <activation> ALL
TRACE INFO
```

**Table 130 TRACE parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <activation> | ENABLE, DISABLE | Enables or disables tracesets.<br>***Note:*** The options for a traceset must be non-nil for tracing to be enabled (See the TRACESET command.) |
| SET <set number> | 0 to 9 | Specifies a particular traceset. |
| ALL | ALL | Specifies all tracesets. |
| INFO | INFO | Displays all traceset settings. |

The following figure shows examples of the TRACE command and system response.

**Figure 194 MAP display example for TRACE command**

```
>TRACE ENABLE SET 0
Enabled Trace Set: 0

>TRACE DISABLE ALL
Disabled ALL Trace Sets

>TRACE INFO
TRACESET 0: PACKETS ALL DIRECTION OUTGOING <DISABLED>
TRACESET 1: NIL
TRACESET 2: NIL
TRACESET 3: NIL
TRACESET 4: NIL
TRACESET 5: NIL
TRACESET 6: NIL
TRACESET 7: NIL
TRACESET 8: NIL
TRACESET 9: NIL
```

The LOGUTIL utility allows users to view the content of the log reports. The following figure shows examples of log report XIP891 generated for traced incoming messages.

***Note:*** For examples of XIP logs, refer to Chapter 12: "TOPS-IP logs."

**Figure 195 Example log report for XIP891**

```
XIP891 SEP08 14:59:57 1032 INFO Trace Incoming Message
          SERVICE   : REMOTE1_IPSVC        COMID      :     4
          PERIPHERAL: DTC       10         MSGID      :    49
          SRC IP    : 47 156 160 179       SRC PORT # :  5500
          DST IP    :                      DST PORT # :
          OP CODE   : 00001101 00001010
          MESSAGE DATA:
          00 30 01 7C 01 18 00 00 00 09 00 28 00 00 01 02 03 04 80 15
          FF FF 2F 9C A0 B3 15 7C 01 5E 48 65 6C 6C 6F 20 57 6F 72 6C
          64 0D 0A 48 65 6C 6C 6F 20 57
```

## Using the query commands

The query commands (listed on page 377) allow the user to query the IP-XPM or the COMID. This section discusses the parameters (arguments) for each command and gives examples of the MAP display.

### GETPMINFO

The GETPMINFO command displays information about a particular IP-XPM, such as the active and inactive IP addresses, route masks, routers, and any active COMIDs. The XPM (DTC) must be datafilled in table XPMIPMAP to be valid.

The GETPMINFO command has the following syntax:

```
GETPMINFO <XPM type> <XPM number>
```

**Table 131 GETPMINFO parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <XPM type> | DTC | Specifies the XPM type. |
| <XPM number> | 0 to 255 | Specifies the XPM number. |

The following figure shows examples of the GETPMINFO command and system response.

**Figure 196 MAP display example for GETPMINFO command**

```
>GETPMINFO DTC 10
14:52:44.162
Active Address: 95.64.10.100      Inactive Address: 95.64.10.101
Unit0 Address : 95.64.10.102      Unit1 Address   : 95.64.10.103

Ether Type:   100 BaseT
Device Type:  On board AMD card

Entry 0
         Destination Address      [0]:0.0.0.0
         Route Mask               [0]:0.0.0.0
         Gateway Address          [0]:95.64.10.1
         Metric                   [0]:1

Entry 1
         Destination Address      [1]:0.0.0.0
         Route Mask               [1]:0.0.0.0
         Gateway Address          [1]:95.64.10.2
         Metric                   [1]:1

Active COMIDs:
  10
  54
  40
```

## QUERYCOMID

The QUERYCOMID command displays information about a particular COMID. The COMID must be datafilled in table IPCOMID to be valid.

The QUERYCOMID command has the following syntax:

```
QUERYCOMID <comid>
```

**Table 132 QUERYCOMID parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <comid> | 0 to 1023 | Specifies the COMID to query. |

The following figure shows examples of the QUERYCOMID command and system response. The five examples show the following information:

- TCP server through socket 496
- TCP client
- UDP socket
- no TCP or UDP connections
- invalid COMID

**Figure 197 MAP display example for QUERYCOMID command**

```
>QUERYCOMID 24
COMID Status         :ACTIVE
Socket Port Type     :TCP
Local Socket ID      :495
Local Socket State   :LISTENING
Local IP Address     :95.64.10.100
Local Port           :11111

         Connected Socket ID        [0]:496
         Connected Socket State     [0]:ESTABLISHED
         Remote IP Address          [0]:95.64.10.116
         Remote Port                [0]:3000

>QUERYCOMID 24
COMID Status         :ACTIVE
Socket Port Type     :TCP
Local Socket ID      :495
Local Socket State   :ESTABLISHED
Local IP Address     :95.64.10.100
Local Port           :11111

         Connected Socket ID        [0]:496
         Connected Socket State     [0]:ESTABLISHED
         Remote IP Address          [0]:95.64.10.116
         Remote Port                [0]:3000

>QUERYCOMID 42
COMID Status         :ACTIVE
Socket Port Type     :UDP
Local Socket ID      :495
Local Socket State   :BOUND
Local IP Address     :95.64.10.120
Local Port           :5555

>QUERYCOMID 88
COMID Status: INACTIVE

>QUERYCOMID 1130
QUERYCOMID request failed: INVALID_COMID
```

## Using the miscellaneous commands

The miscellaneous commands (listed on page 377) allow the user to get help, query the available commands, show or reset parameter values, show information on the current users, and quit the XIPVER tool session. This section discusses the parameters (arguments) for each command and gives examples of the MAP display.

### HELP

The HELP command displays a brief definition for each command available with the XIPVER tool. The HELP command has no parameters.

The HELP command has the following syntax:

```
HELP
```

The following figure shows examples of the HELP command and system response.

**Figure 198 MAP display example for HELP command**

```
>HELP
XPM IP Verification Tool

Parameter Commands:
   DIP:            Sets the destination address parameter
   DP:             Sets the destination application port number
                   parameter
   MESSAGE:        Sets the outgoing message
   PACKETSIZE:     Sets the size of packet parm for PING command
   PINGTIMEOUT:    Sets the time out parameter for PING command
   RR:             Sets the record route option
   TIMEOUT:        Sets the time out parameter for XIPVER tool
                   commands (except for PING command)
   TTLIVE:         Sets time to live parameter for PING command

Connection Commands:
   CLOSE:          Closes specified sockets associated with XIPVER
                   tool COMID
   COMIDBIND:      Binds XIPVER tool session to a Communication ID
   COMIDUNBIND:    Unbinds the COMID from XIPVER tool session
   CONNECT:        Establishes a TCP connection with a remote machine
   FORCECLOSE:     Closes specified sockets associated with a COMID
   PING:           Sends an ICMP Echo Request
   SEND:           Sends a TCP/UDP message to a remote machine
   TCPSERVER:      Sets the XIPVER tool as a TCP server
   UDPSOCKET:      Sets up a UDP socket

Tracing Commands:
   TRACESET:       Sets the trace option sets
   TRACE:          Enables/Disables message tracing

Query Commands:
   GETPMINFO:      Queries an ethernet based SX05 XPM
   QUERYCOMID:     Displays information about a COMID datafilled in
                   IPCOMID table

Misc. Commands:
   HELP:           Displays available commands
   Q <command>:    Displays detailed information on <command>
   QUIT:           Exits XIPVER tool
   RESET:          Resets XIPVER tool parameters
   SHOW:           Shows all the XIPVER tool parameters
   SHOWUSERS:      Shows information about current XIPVER users
```

## Q

The Q command displays detailed information on the syntax and valid values of the specified command.

The Q command has the following syntax:

```
Q <command>
```

**Table 133 Q parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <command> | DIP, DP, MESSAGE, PACKETSIZE, PINGTIMEOUT, RR, TIMEOUT, TTLIVE, COMIDBIND, COMIDUNBIND, CONNECT, FORCECLOSE, PING, SEND, TCPSERVER, UDPSOCKET, TRACE, TRACESET, GETPMINFO, QUERYCOMID, QUIT, RESET, SHOW, SHOWUSERS | Displays the syntax and valid values for each command. |

The following figure shows an example of the Q command and system response.

**Figure 199 MAP display example for Q command**

```
>Q TIMEOUT
Set the time out XIPVER tool parameter

- The time is specified in seconds and the valid range is from 1 to 15

Parms:  [<Timeout> {1 TO 15}]
```

## QUIT

The QUIT command exits the user from the XIPVER tool. Quitting closes all sockets and connections associated with the current session of the XIPVER tool. All changes to private parameters also are lost upon quitting.

The QUIT command has the following syntax:

```
QUIT
QUIT <nlevels>
QUIT <incrname>
QUIT ALL
```

**Table 134 QUIT parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| <nlevels> | Numeric | Specifies the number of MAP levels to quit. |
| <incrname> | Alphanumeric | Specifies the name of the MAP level increment that precedes the current increment in nesting. |

**Table 134 QUIT parameters**

| Parameter | Range of values | Explanation |
|---|---|---|
| ALL | ALL | Specifies quitting all MAP levels and return to the CI level. |

The following figure shows examples of the QUIT command and system response.

**Figure 200 MAP display example for QUIT command**

```
>QUIT
Bye Bye
CI:
```

## RESET

The RESET command resets and displays the default values of the XIPVER parameters. This command has no parameters.

The RESET command has the following syntax:

```
RESET
```

***Note:*** The RESET command requires confirmation.

The following figure shows examples of the RESET command and system response.

**Figure 201 MAP display example for RESET command**

```
>RESET
This command will reset all XIPVER tool parameters.
Are you sure you want to continue? (Yes/No)
Please confirm (“YES”, “Y”, “NO, or “N”)

>Y
DIP                 : NIL
DP                  : NIL
PACKETSIZE          : 64
PINGTIMEOUT         : 3
TIMEOUT             : 3
RR                  : NO
TTLIVE              : 4
MESSAGE             :
   FF FF FF
```

### SHOW

The SHOW command displays the current values of the XIPVER parameters. This command has no parameters.

The SHOW command has the following syntax:

```
SHOW
```

The following figure shows examples of the SHOW command and system response.

**Figure 202 MAP display example for SHOW command**

```
>SHOW
DIP                 : 95.64.10.100
DP                  : 5000
PACKETSIZE          : 64
PINGTIMEOUT         : 5
TIMEOUT             : 4
RR                  : NO
TTLIVE              : 8
MESSAGE
   43 2B 35 20 21 FF FF FF FF FF
```

### SHOWUSERS

The SHOWUSERS command displays the current users of the XIPVER tool.

The SHOWUSERS command has the following syntax:

```
SHOWUSERS
```

The following figure shows examples of the SHOWUSERS command and system response.

**Figure 203 MAP display example for SHOWUSERS command**

```
>SHOWUSERS
<><><><><><><><><><><><><><><><><><><><>
USER#             : 0
USER NAME         : USER1
COMID             : 100
STATE             : XIPVER_TCPCLIENT
PROTOCOL          : TCP
<><><><><><><><><><><><><><><><><><><><>
USER#             : 1
USER NAME         : USER2
COMID             : 110
STATE             : XIPVER_BOUND
PROTOCOL          : UNKNOWN
<><><><><><><><><><><><><><><><><><><><>
```

## Sample XIPVER session

This section shows a series of typical tasks users perform in an XIPVER tool session. In the examples, commands entered by the user appear in bold text; responses appear in plain text. For details on the command syntax, refer to the previous sections on each command.

The following user tasks are described:

- Entering an XIPVER session (page 406)
- Setting up the tool parameters, including:
  - showing tool users (page 406)
  - changing tool parameters (page 406)
  - showing current tool parameters (page 407)
  - resetting tool parameters (page 407)
- Sending TCP and UDP messages, including:
  - binding and unbinding a COMID (page 407)
  - querying a COMID (page 408)
  - querying an XPM (page 408)
  - setting up a UDP socket (page 409)
  - setting up a TCP server (page 409)
  - setting up a TCP client (page 410)
  - sending messages as a UDP socket (page 410)
  - sending messages as a TCP server (page 411)
  - sending messages as a TCP client (page 412)
  - sending and receiving ping (ICMP echo) messages (page 413)
  - closing a UDP socket (page 414)
  - closing a TCP server (page 415)
  - closing a socket on a TCP server (page 416)
  - closing a listening socket on a TCP server (page 417)
  - closing a TCP client (page 418)
- Tracing messages, including:
  - setting up tracesets (page 419)
  - enabling and disabling tracesets (page 419)
  - displaying tracesets (page 419)
- Exiting an XIPVER session (page 420)

## Entering an XIPVER session

**Figure 204 Entering an XIPVER session**

```
>XIPVER
USER# :0
For a list of available commands type: HELP<cr>.
```

## Showing tool users

**Figure 205 Showing tool users**

```
>SHOWUSERS
<><><><><><><><><><><><><><><><><><><>
USER#             : 0
USER NAME         : USER1
COMID             : NIL
STATE             : XIPVER_NIL
PROTOCOL          : TCP
<><><><><><><><><><><><><><><><><><><>
```

## Changing tool parameters

**Figure 206 Changing tool parameters**

```
>DIP 47.142.226.100
DIP: 47.142.226.100

>DP 14000
DP:14000

>PACKETSIZE 334
PACKETSIZE:334

>PINGTIMEOUT 10
PINGTIMEOUT:10

>TIMEOUT 8
TIMEOUT:8

>RR YES
RR: YES

>TTLIVE 10
TTLIVE:10

>MESSAGE 10 #43 21 #29 #23 32 21 10 #A1 12 #DE
   43 15 29 23 20 15 0A A1 0C DE
```

## Showing current tool parameters

**Figure 207 Showing current tool parameters**

```
>SHOW
DIP                 : 47.142.226.100
DP                  : 14000
PACKETSIZE          : 334
PINGTIMEOUT         : 10
TIMEOUT             : 8
RR                  : YES
TTLIVE              : 10
MESSAGE             :
   43 15 29 23 20 15 0A A1 0C DE
```

## Resetting tool parameters

**Figure 208 Resetting tool parameters**

```
>RESET
This command will reset all XIPVER tool parameters.
Are you sure you want to continue? (Yes/No)
Please confirm ("YES", "Y", "NO", or "N"):
y
DIP            : NIL
DP             : NIL
PACKETSIZE     : 64
PINGTIMEOUT    : 1
TIMEOUT        : 3
RR             : NO
TTLIVE         : 4
MESSAGE        :
   FF FF FF
```

## Binding and unbinding a COMID

**Figure 209 Binding and unbinding a COMID**

```
>COMIDBIND 200
COMID: 200

>COMIDUNBIND
21:23:36.875 XIPVER tool unbound from COMID 200
COMID: NIL
```

## Querying a COMID

**Figure 210 Querying a COMID**

```
>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :495
Local Socket State :LISTENING
Local IP Address   :47.245.1.116
Local Port         :11111

         Connected Socket ID         [0]:495
         Connected Socket State      [0]:ESTABLISHED
         Remote IP Address           [0]:47.142.226.100
         Remote Port                 [0]:3000
```

## Querying an XPM

**Figure 211 Querying an XPM**

```
>GETPMINFO DTC 10
14:52:44.162
Active Address: 47.245.1.100       Inactive Address: 47.245.1.101
Unit0 Address : 47.245.1.102       Unit1 Address   : 47.245.1.103

Ether Type:   100 BaseT
Device Type:  On board AMD card

Entry 0
         Destination Address      [0]:0.0.0.0
         Route Mask               [0]:0.0.0.0
         Gateway Address          [0]:47.245.1.1
         Metric                   [0]:0

Entry 1
         Destination Address      [1]:0.0.0.0
         Route Mask               [1]:0.0.0.0
         Gateway Address          [1]:47.245.1.2
         Metric                   [1]:0

Active COMIDs:
         NONE
```

## Setting up a UDP socket

**Figure 212 Setting up a UDP socket**

```
>COMIDBIND 100
COMID: 100

>QUERYCOMID 100
COMID Status       :INACTIVE

>UDPSOCKET
4:19:36.003 UDP socket created

>QUERYCOMID 100
COMID Status         :ACTIVE
Socket Port Type     :UDP
Local Socket ID      :495
Local Socket State   :BOUND
Local IP Address     :47.24.1.116
Local Port           :5555
```

## Setting up a TCP server

**Figure 213 Setting up a TCP server**

```
>COMIDBIND 100
COMID: 100

>QUERYCOMID 100
COMID Status       :INACTIVE

>TCPSERVER
14:21:09.327 TCP server created

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :495
Local Socket State :LISTENING
Local IP Address   :47.245.1.116
Local Port         :11111
```

## Setting up a TCP client

**Figure 214 Setting up a TCP client**

```
>COMIDBIND 100
COMID: 100

>QUERYCOMID 100
COMID Status       :INACTIVE

>DIP 47 142 226 116
DIP: 47.142.226.116

>DP 14000
DP:14000

>CONNECT
10:40:39.148 TCP Client created: Connected to 47.142.226.116:14000

>QUERYCOMID 100
COMID Status         :ACTIVE
Socket Port Type     :TCP
Local Socket ID      :495
Local Socket State   :ESTABLISHED
Local IP Address     :47.24.1.20
Local Port           :11111

         Connected Socket ID        [0]:495
         Connected Socket State     [0]:ESTABLISHED
         Remote IP Address          [0]:47.142.226.116
         Remote Port                [0]:3000
```

## Sending messages as a UDP socket

**Figure 215 Sending messages as a UDP socket**

```
>UDPSOCKET
13:06:58.899 UDP socket created

>DIP 47 142 226 116
DIP: 47.142.226.116

>DP 10000
DP:10000

>MESSAGE 60 #34 #76 #84 23 190 #76
   34 76 84 17 BE 76 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF

>SEND
13:08:13.756 Message of size 60 sent to 47.142.226.116:10000
   34 76 84 17 BE 76 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF
```

## Sending messages as a TCP server

**Figure 216 Sending messages as a TCP server**

```
>TCPSERVER
15:10:17.061 TCP server created

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :495
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :11111

>
15:11:03.280 Connection made with 47.142.226.116:14000 thru 494 socket

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :495
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :11111

         Connected Socket ID         [0]:494
         Connected Socket State      [0]:ESTABLISHED
         Remote IP Address           [0]:47.142.226.116
         Remote Port                 [0]:14000

>MESSAGE 10 #43 22 12 #45 19 #43
   43 16 0C 45 13 43 FF FF FF FF

>SEND 494
15:12:06.294 Message of size 10 sent thru socket 494
   43 16 0C 45 13 43 FF FF FF FF
```

## Sending messages as a TCP client

**Figure 217 Sending messages as a TCP client**

```
>DIP
DIP: 47.142.226.116

>DP 14111
DP:14111

>CONNECT
13:17:36.811 TCP Client created: Connected to 47.142.226.116:14111

>MESSAGE 120 #43 54 65 67 87
   43 36 41 43 57 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

>SEND
13:17:54.756 Message of size 120 sent to 47.142.226.116:14111
   43 36 41 43 57 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

### Sending and receiving ping (ICMP echo) messages

***Note:*** Some routers in a path may not allow the record route (RR) option. In this case, the PING packet may be dropped by the router, which causes the command to fail.

**Figure 218 Sending and receiving ping messages**

```
>DIP
DIP: 47.142.226.116

>PING
DIP: 47.142.226.116
10:45:09.104 ICMP Echo Request sent to machine 47.142.226.116
10:45:09.440 ICMP Echo Response from machine 47.142.226.116

>PING IP  47 142 227 8
DIP: 47.142.227.8
10:48:48.727 ICMP Echo Request sent to machine 47.142.227.8
10:48:49.168 ICMP Echo Response from machine 47.142.227.8

>RR YES
RR: YES

>PING IP 47 245 0 1
DIP: 47.245.0.1
10:50:46.399 ICMP Echo Request sent to machine 47.245.0.1
10:50:46.791 ICMP Echo Response from machine 47.245.0.1
ROUTE:
47.245.0.21
47.245.0.1
47.245.0.1
47.245.1.19
Elapsed Time: 10

>RR N
RR: NO

>PING DNS 'WNC6724'
DNS: WNC6724
10:44:18.860 ICMP Echo Request sent to machine 47.129.13.45
10:44:19.130 ICMP Echo Response from machine 47.129.13.45
```

## Closing a UDP socket

**Figure 219 Closing a UDP socket**

```
>COMIDBIND 100
COMID: 100

>UDPSOCKET
4:19:36.003 UDP socket created

>QUERYCOMID 100
COMID Status         :ACTIVE
Socket Port Type     :UDP
Local Socket ID      :495
Local Socket State   :BOUND
Local IP Address     :47.24.1.20
Local Port           :5555

>CLOSE
This command will close all connections and sockets associated with
XIPVER tool
Are you sure you want to continue? (Yes/No)
Please confirm ("YES", "Y", "NO", or "N"):
>Y
13:03:59.655 Closed all sockets and connections associated with 100

>QUERYCOMID 100
COMID Status       :INACTIVE
```

## Closing a TCP server

**Figure 220 Closing a TCP server**

```
>COMIDBIND 100
COMID: 100

>TCPSERVER
14:21:09.327 TCP server created

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :495
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :11111

>CLOSE
This command will close all connections and sockets associated with
XIPVER tool
Are you sure you want to continue? (Yes/No)
Please confirm ("YES", "Y", "NO", or "N"):
>Y
13:03:59.655 Closed all sockets and connections associated with COMID
100

>QUERYCOMID 100
COMID Status       :INACTIVE
```

## Closing a particular socket on a TCP server

**Figure 221 Closing a particular socket on a TCP server**

```
>COMIDBIND 100
COMID: 100

>TCPSERVER
12:54:21.310 TCP server created

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :494
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :8888

12:55:59.304 Connection made with 47.245.1.20:8888 thru 493 socket

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :494
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :8888

         Connected Socket ID           [0]:493
         Connected Socket State        [0]:ESTABLISHED
         Remote IP Address             [0]:47.142.226.116
         Remote Port                   [0]:14000

>CLOSE 493
This command will close all connections associated with socket 493
Are you sure you want to continue? (Yes/No)
Please confirm ("YES", "Y", "NO", or "N"):
y
12:56:53.982 Closed Socket 493 and all connections associated with it.

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :494
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :8888
```

### Closing a listening socket on a TCP server

***Note:*** Closing a listening socket closes all sockets.

**Figure 222 Closing a listening socket on a TCP server**

```
>CLOSE
12:58:54.448 Connection made with 47.245.1.20:8888 thru 492 socket

>QUERYCOMID 100
COMID Status       :ACTIVE
Socket Port Type   :TCP
Local Socket ID    :494
Local Socket State :LISTENING
Local IP Address   :47.245.1.20
Local Port         :8888

         Connected Socket ID           [0]:492
         Connected Socket State        [0]:ESTABLISHED
         Remote IP Address             [0]:47.142.226.116
         Remote Port                   [0]:14000

>CLOSE 494
This command will close all connections associated with socket 494
Are you sure you want to continue? (Yes/No)
Please confirm ("YES", "Y", "NO", or "N"):
>Y
12:59:29.092 Closed Socket 494 and all connections associated with it.

>QUERYCOMID 100
COMID Status       :INACTIVE
```

## Closing a TCP client

**Figure 223 Closing a TCP client**

```
>COMIDBIND 100
COMID: 100

>DIP 47 142 226 116
DIP: 47.142.226.116

>DP 14000
DP:14000

>CONNECT
10:40:39.148 TCP Client created: Connected to 47.142.226.116:14000

>QUERYCOMID 100
COMID Status          :ACTIVE
Socket Port Type      :TCP
Local Socket ID       :495
Local Socket State    :ESTABLISHED
Local IP Address      :47.24.1.20
Local Port            :11111

          Connected Socket ID        [0]:495
          Connected Socket State     [0]:ESTABLISHED
          Remote IP Address          [0]:47.142.226.116
          Remote Port                [0]:3000

>CLOSE
This command will close all connections and sockets associated with
XIPVER tool
Are you sure you want to continue? (Yes/No)
Please confirm ("YES", "Y", "NO", or "N"):
>Y
13:03:59.655 Closed all sockets and connections associated with 100

>QUERYCOMID 100
COMID Status       :INACTIVE
```

## Setting up tracesets

**Figure 224 Setting up tracesets**

```
>TRACESET SET 0 MESSAGE ALL IN
TRACESET 0: MESSAGES ALL DIRECTION IN

>TRACESET SET 1 MESSAGE COMID 100 OUT
TRACESET 1: MESSAGES COMID 100 DIRECTION OUT

>TRACESET SET 2 MESSAGE XPM DTC 10 BOTH
TRACESET 2: MESSAGES XPM DTC 10 DIRECTION BOTH

>TRACESET SET 3 MESSAGE IP 47 142 226 116 IN
TRACESET 3: MESSAGES IP 47.142.226.116 DIRECTION IN

>TRACESET SET 4 PACKET ALL IN
TRACESET 4: PACKETS ALL DIRECTION IN
```

## Enabling and disabling tracesets

**Figure 225 Enabling and disabling tracesets**

```
>TRACESET ENABLE ALL
Enabled all Trace Sets

>TRACE DISABLE SET 1
Disabled Trace Set: 1

>TRACE DISABLE ALL
Disabled ALL Trace Sets

>TRACE ENABLE SET 0
Enabled Trace Set: 0
```

## Displaying tracesets

**Figure 226 Displaying tracesets**

```
>TRACE INFO
TRACESET 0: MESSAGES ALL DIRECTION INCOMING <ENABLED>
TRACESET 1: MESSAGES COMID 100 DIRECTION OUTGOING <DISABLED>
TRACESET 2: MESSAGES XPM DTC 10 DIRECTION BOTH <DISABLED>
TRACESET 3: MESSAGES IP 47.142.226.116 DIRECTION INCOMING <DISABLED>
TRACESET 4: PACKETS ALL DIRECTION INCOMING <DISABLED>
TRACESET 5: NIL
TRACESET 6: NIL
TRACESET 7: NIL
TRACESET 8: NIL
TRACESET 9: NIL
```

### Exiting an XIPVER session

**Figure 227 Exiting an XIPVER session**

```
>QUIT
Bye Bye
CI:
```

## Understanding possible error messages

Error messages may appear at the MAP during an XIPVER tool session to report denials or failures of certain command requests. The following table lists the error message, explanation, and action.

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| `CLOSE request denied: the xipver tool is not bound to a COMID` | The XIPVER tool was not bound to a COMID using the COMIDBIND command, so the CLOSE command cannot be used. | To close a COMID of another application use the FORCECLOSE command. |
| `CLOSE request denied: the xipver tool does not have any connections or sockets to close` | The XIPVER tool is bound to a COMID but there is no socket opened that can be closed. | To close a COMID of another application use the FORCECLOSE command. |
| `COMIDBIND request denied: COMID <comid> is not datafilled in table IPCOMID` | The COMID is not datafilled in table IPCOMID. | Datafill the COMID before using the COMIDBIND command. |
| `COMIDBIND request denied: COMID <comid> is already bound to another application` | The COMID is in use by another application. The same COMID cannot be shared by applications. | Wait for the COMID to become free, or use another COMID. |
| `COMIDBIND request denied: XIPVER tool is already bound to a COMID. Use COMIDUNBIND command to unbind the current comid.` | The XIPVER tool is already bound to another COMID. The XIPVER tool can only be bound to one COMID at a time. | Unbind the current COMID from the XIPVER tool to use a new COMID, or open another session of the XIPVER tool. |
| `CONNECT request denied: Please use DIP command to set a destination IP address before using this command` | The destination IP address was not specified. | Specify the destination IP address before using the CONNECT command. |

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| `CONNECT request denied: Please use DP command to set a destination port before using this command` | The destination port number was not specified. | Specify the destination port before using the CONNECT command. |
| `PING request denied: Destination IP address not provided` | The destination IP address was not specified. | Specify the destination IP address with the DIP command or with the PING command. |
| `SEND request denied: XIPVER tool not setup as a TCP client, TCP server, or UDP socket` | The XIPVER tool is not yet set up as a TCP client, TCP server, or UDP socket. | Set up the XIPVER tool as a TCP client, TCP server, or UDP socket before using the SEND command. |
| `SEND request denied: XIPVER tool is used as a TCP server. Please specify a socket ID.` | The XIPVER tool is set up as a TCP server. | Specify the socket ID through which to send the message. |
| `SEND request denied: A destination address is not specified. Please use DIP command to specify a destination address` | The XIPVER tool is set up as a UDP socket. | Specify the destination IP address before using the SEND command. |
| `SEND request denied: A destination port number is not specified. Please use DP command to specify a destination port number` | The XIPVER tool is set up as a UDP socket. | Specify the destination port before using the SEND command. |
| `<Command> request denied: XIPVER tool is not bound to a COMID` | The XIPVER tool is not bound to a COMID. | Bind the XIPVER tool to a COMID before using the specified command. (See Note 1.) |
| `<Command> request denied: XIPVER tool already setup as a TCP client` | The XIPVER tool is set up as a TCP client. | Close the TCP client and try the command again. (See Note 2.) |
| `<Command> request denied: XIPVER tool already setup as a TCP server` | The XIPVER tool is set up as a TCP server. | Close the TCP server and try the command again. (See Note 2.) |

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| `<Command> request denied: XIPVER tool already setup as a UDP socket` | The XIPVER tool is set up as a UDP socket. | Close the UDP socket and try the command again. (See Note 2.) |
| `<Command> request failed: No response received from XPM with in <#> seconds` | No response was received from the XPM within the specified number of seconds. | Change the value of the timeout with the PINGTIMEOUT command or with the TIMEOUT command. (See Note 1.) |
| `<Command> request failed: rsi_invalid_comid` | The COMID is invalid. | Specify a valid COMID. (See Note 1.) |
| `<Command> request failed: rsi_xpm_not_insv` | The XPM to which the COMID is bound is not in service. | Wait for the XPM to come into service and try the command again. (See Note 1.) |
| `<Command> request failed: rsi_invalid_appl_id` | The XIPVER tool application has a problem. | Quit the XIPVER tool and start a new session. Try the command again. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: rsi_appl_comid_mismatch` | The XIPVER tool application has a problem. | Quit the XIPVER tool and start a new session. Try the command again. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: rsi_enc_msg_err` | The XIPVER tool application has a problem. | Quit the XIPVER tool and start a new session. Try the command again. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: rsi_misc_send_fail_err` | The XIPVER tool application has a problem. | Quit the XIPVER tool and start a new session. Try the command again. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: BAD RSI MESSAGE` | The CM sent the XPM an IP-related message that the XPM does not recognize. | Contact Nortel Networks technical support. (See Note 1.) |

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| `<Command> request failed: INSUFFICIENT RESOURCES` | The TCP and/or UDP resources on the XPM are currently overburdened. | Lower the IP resource usage on the XPM. If this error persists, contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: BAD COMID` | The COMID is incorrect or the XPM is no longer using the COMID. | Enter the correct COMID or use the QUERYCOMID command to determine if the XPM is still using the COMID. (See Note 1.) |
| `<Command> request failed: BAD SOCKET` | The socket number is not correct or the XPM is no longer using the socket. | Enter the correct socket number or use the QUERYCOMID command to determine if the XPM is still using the socket. (See Note 1.) |
| `<Command> request failed: XPM DATA COMM NOT READY` | One or more of the following problems may apply:<br>1. The XPM is not yet in service.<br>2. Table XPMIPMAP and table XPMIPGWY (if used) may contain incorrect datafill. Also, if a DHCP server is used, its configuration may be incorrect.<br>3. Hardware connections to the LAN are not functioning. | 1. Wait for the XPM to come into service and try the command again. Also try to RTS the XPM again. (See Note 1.)<br>2. Check datafill in tables XPMIPMAP and XPMIPGWY (if used), and possibly the configuration of the DHCP server.<br>3. Check the hardware connections. |
| `<Command> request failed: ENDPOINT ADDRESS NOT AVAILABLE` | Depending on the operation requested, a CM or XPM software error occurred. | Contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: ADDRESS IN USE` | An attempt was made to re-use an IP port that was previously used. | Wait 5 to 10 minutes and try the command again. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| `<Command> request failed: INVALID PING RESPONSE` | The XPM received a response to a ping that it did not originate. | Contact Nortel Networks and/or the network administrator for support. (See Note 1.) |
| `<Command> request failed: ENDPOINT REFUSED CONNECTION` | A connect attempt was made to a node on the network but the node refused the connection. | Check the far-end node to verify that its hardware and software are functioning properly. (See Note 1.) |

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| <Command> request failed: DESTINATION ADDRESS ID REQUIRED | A message that requires a destination IP address was sent to the XPM without the IP address. | Contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: INVALID PARAMETER | An XPM software error occurred. | Contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: INTERFACE CLOSED | One or more of the XPM IP interfaces was closed. This should not occur. | Contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: INVALID FUNCTION CALL | An IP operation that is not supported by the XPM was invoked. A possible CM or XPM software error occurred. | Contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: SOCKET IS ALREADY CONNECTED | An attempt was made to perform a connect operation on a TCP socket after it was connected. | Quit the XIPVER tool and start a new session. Try the command again. (See Note 1.) |
| <Command> request failed: OUT OF PORTS | The TCP and/or UDP socket resource limit was reached on the XPM. | Lower the IP resource usage on the XPM. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: OUT OF PACKETS | There may be too much outgoing IP traffic on the XPM. | Try the command again. If the error persists, reduce the IP traffic on the XPM. If the error still persists, contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: SOCKET IS NOT CONNECTED | An operation that needs a connected socket was invoked before the socket was connected. | Verify that the command is being performed in the correct sequence. (See Note 1.) |
| <Command> request failed: INVALID SOCKET DESCRIPTOR | An XPM software error occurred. | Contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: SOCKET TYPE SPECIFIED IS NOT SUPPORTED | The XPM was requested to perform an action that was not TCP or UDP related. | Contact Nortel Networks technical support. (See Note 1.) |

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| <Command> request failed: ILLEGAL OPERATION DUE TO SOCKET SHUTDOWN TIMEOUT | Either the sending or the receiving of IP messages was shut down on the XPM for the socket, and an attempt to send or receive a message was performed. | Quit the XIPVER tool and start a new session. Try the command again. If the error persists, contact Nortel Networks technical support. (See Note 1.) |
| <Command> request failed: IP STACK NOT INITIALIZED | One or more of the following problems may apply:<br>1. The XPM is not yet in service.<br>2. Table XPMIPMAP and table XPMIPGWY (if used) may contain incorrect datafill. Also, if a DHCP server is used, its configuration may be incorrect.<br>3. Hardware connections to the LAN are not functioning. | 1. Wait for the XPM to come into service and try the command again. Also try to RTS the XPM again. (See Note 1.)<br>2. Check datafill in tables XPMIPMAP and XPMIPGWY (if used), and possibly the configuration of the DHCP server.<br>3. Check the hardware connections. |
| <Command> request failed: TIMEOUT | 1. If this error is a result of using the PING command, the ping request timed out. The network node being pinged may not be working.<br>2. If this error is not a result of using the PING command, a possible XPM software problem exists. | 1. Check the network configuration and also the node being pinged. (See Note 1.)<br>2. Contact Nortel Networks technical support. |
| <Command> request failed: PROTOCOL NOT SUPPORTED | The XPM was requested to perform an action that was not TCP or UDP related. | Contact Nortel Networks technical support (See Note 1.) |
| <Command> request failed: DNS SERVER RETURNED ERROR | The DNS server returned an error to the requested command. | Check the DNS server configuration (See Note 1.). |
| <Command> request failed: DNS NAME TOO LONG | The DNS server returned a DNS name that is too long. | Check the DNS server configuration. (See Note 1.) |
| <Command> request failed: DNS SERVER FAILED | The DNS server failed to process the request. | Check the DNS server configuration. (See Note 1.) |
| <Command> request failed: DNS ADDRESS RESOLUTION PROBLEM | The IP address or the DNS name is not in the DNS database. | Check the DNS database to make sure the IP address and/or DNS name is present. (See Note 1.) |

**Table 135 Error messages**

| Message | Explanation | User action |
|---|---|---|
| `<Command> request failed: DNS SOCKET CALL FAILED` | The DNS server did not respond to the request that was sent to it. | Check the DNS server to verify that it is functioning properly. Also check the network to verify that IP messages can reach the DNS server. (See Note 1.) |
| `<Command> request failed: DNS SERVER LIST NOT SET` | 1. If the CM configuration method is datafilled in table XPMIPMAP, then either the DNS datafill is incorrect or is not present in that table.<br>2. If the DHCP configuration method is datafilled in table XPMIPMAP, then the DNS information returned by the DHCP server is incorrect or is not present. | 1. Check DNS datafill in table XPMIPMAP. (See Note 1.)<br>2.Check DNS datafill at the DHCP server. |
| `<Command> request failed: UNKNOWN ERROR` | An unrecognizable error occurred. | Contact Nortel Networks technical support. (See Note 1.) |
| ***Note 1:*** This error message applies only to the following commands: CLOSE, FORCECLOSE, COMIDUNBIND, CONNECT, PING, QUERYCOMID, SEND, TCPSERVER, UDPSOCKET.<br>***Note 2:*** This error message applies only to the following commands: CONNECT, TCPSERVER, UDPSOCKET. | | |

## Unsolicited messages

Unsolicited messages may appear at the MAP during an XIPVER session. These messages report certain events at the switch as they occur. They are for information only; no user action is required. The following table lists the unsolicited message and an explanation.

**Table 136 Unsolicited messages**

| Message | Explanation |
|---|---|
| `15:11:03:280 Connection made with 47.142.226.116:14000 thru 494 socket` | The XPM accepted a connection for a TCP server. |
| `XPM: <PM name> <PM number> status changed to <INSERVICE/OUT OF SERVICE>` | The XPM came into service or went out of service. |

## CONVERTCSLINKS

The CONVERTCSLINKS tool automatically converts C-side links on the IP-XPM. Converting to C-side 14 extended messaging has the following requirements:

- The IP-XPM has been engineered with ENET, DS512 fiber links to the IP-XPM, and the NT6X40FC network interface card.
- The TEL00011 SOC option (CSide14-Extended Messaging) is in the ON state.

***Note:*** It is recommended that the conversion be performed during a period of low traffic.

### LTCINV datafill example (before conversion)

Figure 228 shows an example of datafill for DTC 4. Notice that the value in the EXTLINKS field is 0. During the conversion, the CONVERT command will automatically update this value to 6 to reflect 6 *pairs* of extended C-side links (see page 433).

**Figure 228 MAP display example for table LTCINV—before conversion**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
-------------------------------------------------------------------------
DTC 4   1001   LTE    0    51    0     C   0    6X02NA  QTP22xx (ABTRK DTCEX)$
   (0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5) (0 11 0 6)
(0 11 0 7) (0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11) (0 11 0 12) (0 11 0 13)
(0 11 0 14) (0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     0          SXFWAKxx     (CCS7) $
       6X40FC    N
```

### CONVERT command example

Users enter the tool by typing “CONVERTCSLINKS” at the CI level of the MAP. The CONVERT command has the following syntax:

```
CONVERT <XPM name> <XPM number> <from> <to>
```

So, for example, entering “CONVERT DTC 4 0 6” will convert the C-side links on DTC 4 from 0 pairs to 6 pairs.

To minimize call processing degradation, the system performs the conversion one plane at a time (plane 0 followed by plane 1). During the conversion, users are prompted two times for confirmation (YES, Y, NO, N): before converting plane 0 and before converting plane 1.

Conversion consists of the following broad steps performed for each plane:

1 The links are busied and offlined.

2 The capability of the links is changed.

3 The links are busied and returned to service.

***Note:*** After the conversion, users are automatically returned to the CI level of the MAP.

An example of the CONVERT command and system response is shown in Figure 229, Figure 229, Figure 229, Figure 229, and Figure 229.

**Figure 229 MAP display example for CONVERT command**

```
>convert dtc 4 0 6
The affected links are:
 shelf 0, slot 11, link 1, ds30 equiv 4
 shelf 0, slot 11, link 1, ds30 equiv 6
 shelf 0, slot 11, link 1, ds30 equiv 5
 shelf 0, slot 11, link 1, ds30 equiv 7
 shelf 0, slot 11, link 1, ds30 equiv 8
 shelf 0, slot 11, link 1, ds30 equiv 10
 shelf 0, slot 11, link 1, ds30 equiv 9
 shelf 0, slot 11, link 1, ds30 equiv 11
 shelf 0, slot 11, link 1, ds30 equiv 12
 shelf 0, slot 11, link 1, ds30 equiv 14
 shelf 0, slot 11, link 1, ds30 equiv 13
 shelf 0, slot 11, link 1, ds30 equiv 15
MAPCI:
MTC:
ENET:
SHELF:
CARD:
Warning: DO NOT break hx this process.
It is recommended that this activity be done
during a low traffic period.
This conversion is done on a plane basis
to minimize call processing degradation.
The DS30s will be bsyed and offled, their
capability changed and then the DS30s will
be bsyed and rtsed. You will then be prompted
to convert the other plane.
Confirm when ready to start.
```

**Figure 229 MAP display example for CONVERT command (continued)**

```
Please confirm ("YES", "Y", "NO", or "N"):
>y

Info: Affected links on plane 0 will be bsyed and offled.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 passed.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to OFFLINE ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 passed.

Info: Affected link capability on plane 0 will be changed.

Info: Affected links on plane 0 will be bsyed and rtsed.
```

**Figure 229 MAP display example for CONVERT command (continued)**

```
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to MAN BUSY ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 passed.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to RTS ENET Plane:0 Shelf:00 Slot:11 Link:01 DS30:15 passed.

Info: Links on plane 0 are now insv.
Please consider a delay before starting the other plane
to minimize integrity errors.
Confirm when ready to start.
Replying No will back out changes made thus far.
```

**Figure 229 MAP display example for CONVERT command (continued)**

```
Please confirm ("YES", "Y", "NO", or "N"):
>y

Info: Affected links on plane 1 will be bsyed and offled.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 passed.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to OFFLINE ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 passed.

Info: Affected link capability on plane 1 will be changed.

Info: Affected links on plane 1 will be bsyed and rtsed.
```

**Figure 229 MAP display example for CONVERT command (continued)**

```
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:04 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:06 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:05 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:07 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:08 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:10 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:09 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:11 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:12 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:14 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:13 passed.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to MAN BUSY ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 passed.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 submitted.
Request to RTS ENET Plane:1 Shelf:00 Slot:11 Link:01 DS30:15 passed.

Info: Links on plane 1 are now insv.

Info: Extlinks has been updated in table LTCINV.

Info: Process is now complete.
```

### LTCINV datafill example (after conversion)

Figure 230 shows an example of datafill for DTC 4 after the conversion.

**Figure 230 MAP display example for table LTCINV—after conversion**

```
LTCNAME  ADNUM FRTYPE FRNO SHPOS FLOOR ROW FRPOS EQPEC   LOAD    EXECTAB
   CSLNKTAB
       OPTCARD
   TONESET           PROCPEC             EXTLINKS    E2LOAD     OPTATTR
       PEC6X40   EXTINFO
-------------------------------------------------------------------------
DTC 4   1001   LTE    0    51    0     C   0    6X02NA  QPT18xx (ABTRK DTCEX)$
   (0 11 0 0) (0 11 0 1) (0 11 0 2) (0 11 0 3) (0 11 0 4) (0 11 0 5) (0 11 0 6)
(0 11 0 7) (0 11 0 8) (0 11 0 9) (0 11 0 10) (0 11 0 11) (0 11 0 12) (0 11 0 13)
(0 11 0 14) (0 11 0 15)$
       (MX76C14 HOST) $
   NORTHAA          SX05DA $ SX05DA $     6          SXFWAKxx    (CCS7) $
       6X40FC    N
```

***Note:*** The CONVERT command is also used to convert *back* to 0 pairs of C-side links. So, for example, “CONVERT DTC 4 6 0” would reverse the conversion process shown previously.

## IPGWSTAT

The IPGWSTAT tool is a DMS MAP command that displays information about TOPS-IP Gateways (IPGW) and their associated IP-XPMs, C-side links, and dynamic voice trunks.

***Note 1:*** IPGWSTAT is intended to be used primarily by Nortel Networks field support.

***Note 2:*** For details on maintenance of the Gateway card, refer to Chapter 10: “TOPS-IP maintenance activities.”

Refer to Figure 231 for a datafill example of table IPINV. In this example, DTC 10 and DTC 11 each support three Gateways. Two trunk groups for OC-IP, OCIPTOREMOTE and OCIPTOHOST, are distributed across DTC 10 and DTC 11. Each trunk group supports 144 members.

**Figure 231 MAP display example for table IPINV**

```
IPNO       PMTYPE  PMNO IPPEC  LOAD PORT  IPZONE              GWTYPE
-------------------------------------------------------------------------------
TGWY 10 3  DTC     10   7X07AA  $    6    47 174 68 7 0 0 0 0  TOPS OCIPTOREMOTE 0
TGWY 10 4  DTC     10   7X07AA  $    8    47 174 68 8 0 0 0 0  TOPS OCIPTOHOST 0
TGWY 10 5  DTC     10   7X07AA  $    10   47 174 68 9 0 0 0 0  TOPS OCIPTOREMOTE 48
TGWY 11 3  DTC     11   7X07AA  $    6    47 174 69 7 0 0 0 0  TOPS OCIPTOHOST 48
TGWY 11 4  DTC     11   7X07AA  $    8    47 174 69 8 0 0 0 0  TOPS OCIPTOREMOTE 96
TGWY 11 5  DTC     11   7X07AA  $    10   47 174 69 9 0 0 0 0  TOPS OCIPTOHOST 96
```

Figure 232 shows an example MAP display output from the IPGWSTAT command. Refer to the sections that follow the figure for a description of all the fields in the output.

**Figure 232 MAP display example for IPGWSTAT command**

```
>IPGWSTAT

     IPGW      |     XPM      |  C-side links   |        Lines or trunks
---------------+--------------+-----------------+------------------------------
TGWY 10 3 -OK- | DTC  10 -OK- |  6 -OK-  7 -OK- | ( a) hOC t48 IDL CPB
TGWY 10 4 -OK- | DTC  10 -OK- |  8 -OK-  9 -OK- | ( b) rOC t30 IDL CPB
TGWY 10 5 Offl | DTC  10 -OK- | 10 PBsy 11 PBsy | ( a) hOC INB
TGWY 11 3 Offl | DTC  11 -OK- |  6 PBsy  7 PBsy | ( b) rOC INB
TGWY 11 4 Offl | DTC  11 -OK- |  8 PBsy  9 PBsy | ( a) hoc INB
TGWY 11 5 -OK- | DTC  11 -OK- | 10 -OK- 11 -OK- | ( b) rOC t30 IDL
---------------+--------------+-----------------+------------------------------
( a) OCIPTOREMOTE    Avail: 47  Calls: 1  MAXCONNS: 60  HoldQ:  0
( b) OCIPTOHOST      Avail: 58  Calls: 2  MAXCONNS: 60  HoldQ: 36
```

***Note:*** The C-side links column shown in Figure 232 indicates the HDLC links between the IP-XPM (DTC) and the IPGW. These links are on the C-side from the perspective of the IPGW, but they are on the P-side from the perspective of the DTC.

### States displayed for IPGWs, IP-XPMs, C-side links

The IPGWSTAT output indicates one of the following states for IPGWs, IP-XPMs, and C-side links:

- -OK- is in service
- CBsy is C-side busy
- PBsy is P-side busy
- CBPB is both CBsy and PBsy (only possible for links)
- SysB is system busy
- ManB is manual busy
- Offl is offline
- Uneq is unequipped
- ???? is unknown (software error)

### States displayed for dynamic trunks

The IPGWSTAT output indicates on of the following states for dynamic trunks:

- UNEQ
- INB
- MB

- NWB
- PMB
- RMB
- SYSB
- CFL
- LO
- DELO
- INI
- CPB
- CPD
- RES
- IDL
- SZD
- ???

### Column 1: IPGW

Column 1 indicates the states for Gateways datafilled in table IPINV. (These are ordered according to an internal table, so the order will not necessarily be the same as shown in table IPINV.) Users can view and change the Gateway state at the MAP by posting the Gateway, for example:

```
MAPCI;MTC;PM;POST IPGW TGWY 10 3
```

### Column 2: XPM

Column 2 indicates the states for the associated IP-XPM (DTC) datafilled in table IPINV. Users can maintain the IP-XPM at the PM level at the MAP by posting the DTC, for example:

```
MAPCI;MTC;PM;POST DTC 10
```

### Column 3: C-side links

Column 3 indicates the state of the two C-side links (HDLC) between the IP-XPM and the Gateway card. There are two links per card. Users can view these links at the PM level after posting a DTC and issuing the TRNSL P command (since the HDLC links are on the P-side from the perspective of the DTC). The number associated with the link corresponds to the PORT field in table IPINV. The first link is port n and the second link is port n+1.

Users can update the link status by issuing the BSY LINK <link#> command, and following this with the RTS LINK <link#> command or RTS LINK <link#> FORCE (faster than normal RTS).

### Column 4: Trunks

The letter in parentheses indicates the corresponding trunk CLLI name in the CLLI list that follows the four-column table. After 26 CLLIs are output, two-letter designations are used.

The next field indicates the dynamic trunk application name in table TRKOPTS. The only valid value for TOPS-IP dynamic trunks is "OC." An "r" preceding OC indicates a Gateway card used on the remote side, and an "h" indicates a card used on the host side.

The next field indicates the dynamic trunk member *threshold* for the associated Gateway card (if it is in service). This output appears only when the MAXCONNS (maximum connections) function is in effect for the trunk group. With MAXCONNS in effect, the card is thresholded so that certain higher trunk members will not be used. The MAXCONNS value is datafilled in table TOPSTOPT (page 255).

Refer to the IPGWSTAT example shown again in Figure 233. In this example, each trunk group supports 144 members (table IPINV), and has a MAXCONNS value set to 60. Since only one Gateway card (TGWY 10 3) is in service for OCIPTOREMOTE, the trunk group can provide a maximum of 48 connections. So the threshold display for TGWY 10 3 shows "t48." For OCIPTOHOST, two Gateway cards (TGWY 10 4 and TGWY 11 5) are in service, so the trunk group can provide a maximum of 60 connections across the two in-service cards, 30 on each card. The threshold display shows "t30" for each card.

**Figure 233 MAP display example for IPGWSTAT command**

```
>IPGWSTAT

     IPGW      |     XPM      |  C-side links   |        Lines or trunks
---------------+--------------+-----------------+-------------------------------
TGWY 10 3 -OK- | DTC  10 -OK- |  6 -OK-  7 -OK- | ( a) hOC t48 IDL CPB
TGWY 10 4 -OK- | DTC  10 -OK- |  8 -OK-  9 -OK- | ( b) rOC t30 IDL CPB
TGWY 10 5 Offl | DTC  10 -OK- | 10 PBsy 11 PBsy | ( a) hOC INB
TGWY 11 3 Offl | DTC  11 -OK- |  6 PBsy  7 PBsy | ( b) rOC INB
TGWY 11 4 Offl | DTC  11 -OK- |  8 PBsy  9 PBsy | ( a) hoc INB
TGWY 11 5 -OK- | DTC  11 -OK- | 10 -OK- 11 -OK- | ( b) rOC t30 IDL
---------------+--------------+-----------------+-------------------------------
( a) OCIPTOREMOTE    Avail: 47  Calls: 1  MAXCONNS: 60  HoldQ:  0
( b) OCIPTOHOST      Avail: 58  Calls: 2  MAXCONNS: 60  HoldQ: 36
```

***Note:*** Refer to "TOPSTOPT" on page 67 for details on the MAXCONNS function.

The last field is a list of trunk states for trunks associated with the Gateway card. Up to four trunk states may be output if trunks supported by the Gateway are in different states. If five or more trunk states are detected, "+" indicates the additional states. The states output roughly correspond to the display at the MAPCI;MTC;TRKS;TTP level, but some letters might be different.

## CLLI list

Following the four-column table is the CLLI list. Each CLLI is indexed by the letter in column 4. The text output describes conditions applying to the entire trunk group. Except for the “MAXCONNS” value, these fields apply only to in-service trunk members.

Table 137 gives an explanation for the output.

**Table 137 Text displayed in the CLLI list**

| Display | Meaning |
|---|---|
| Avail: n | Number of trunks that are IDL or INI |
| Calls: n | Number of trunks that are CPB or CPD |
| IdleQ: n | Size of the trunk group’s idle queue, which may include trunks which are not IDL or INI. This field is only output if the size of the idle queue is not equal to the number of IDL or INI trunks for the group. |
| MAXCONNS: n | The MAXCONNS limit for the trunk group from table TOPSTOPT |
| HoldQ: n | The size of the holding queue, which should eventually be equal to (number of trunk group members) - (limit). |
| ResQ: n | Also the size of the holding queue, obtained in a second manner. This field is only output if the HoldQ size is not equal to the ResQ size. |
| ResIdle: n | The number of trunks in the RES state, which should eventually be equal to the size of the holding queue. This field is only output if the HoldQ size is not equal to the number of RES trunks. |
| Lockout: n | The number of trunk group members in the lockout condition (LO). These should be corrected by XPM action or by the 15-minute trunk audit. If they are not, the trunks are in permanent lockout and cannot be used again until maintenance is performed on the card. |
| Orphans: n | The number of members that are RES, IDL, or INI, but are not in the idle queue or the holding queue, and therefore are not accessible to call processing. The 15-minute trunk audit should correct these, and a log is generated when this happens. Orphans happen when call processing traps trying to dequeue a trunk from the idle queue. |

## TQMIST

The TQMIST tool allows users to capture QMS MIS event messages based on specified call trace selection criteria. The captured data is stored in a buffer and can be displayed at the MAP. For output on the status of the QMS MIS queues, users can issue the SHOW command.

***Note:*** This function of TQMIST is intended to be used primarily by Nortel Networks field support.

# Chapter 12: TOPS-IP logs

This chapter provides information on logs for TOPS-IP. For each log there is a brief description, example, action, and list of any associated OM registers. Table 138 lists each log and the page in this chapter where its description begins.

**Table 138 TOPS-IP logs**

| Log name | Page number |
|---|---|
| **XPM IP data communication (XIP) logs** | |
| XIP600 | 440 |
| XIP890 | 443 |
| XIP891 | 445 |
| XIP892 | 446 |
| XIP893 | 446 |
| **External alarm (EXT) logs** | |
| EXT106 | 447 |
| EXT107 | 447 |
| EXT108 | 448 |
| **QMS MIS (QMIS) logs** | |
| QMIS102 | 449 |
| QMIS103 | 449 |
| **TOPS logs** | |
| TOPS106 | 450 |
| TOPS112 | 450 |
| TOPS133<br>***Note:*** TOPS133 replaces TOPS105 on OC-IP calls. | 451 |
| TOPS134 | 460 |

**Table 138 TOPS-IP logs**

| Log name | Page number |
|---|---|
| TOPS135 | 464 |
| TOPS136 | 465 |
| TOPS137 | 466 |
| TOPS304 | 469 |
| TOPS305<br>***Note:*** The TOPS305 log is never generated. | 470 |
| TOPS502 | 471 |
| TOPS504 | 474 |
| TOPS505<br>***Note:*** The TOPS505 log is never generated. | 475 |
| TOPS614 | 475 |
| TOPS615 | 475 |

***Note:*** For information on IPGW (IP Gateway) log reports, refer to *Log Report Reference Manual*.

## XIP600

This log is generated when a communication problem occurs between the CM data communication application and the SX05DA. The log report displays reason text (values are listed in Table 63) and an optional field that contains message data in hexadecimal format. If the message data can be displayed, it is limited to 280 bytes. Any data greater than or equal to 280 bytes is truncated with the text: “Message truncated to 280 bytes.”

The following figure shows an example log report.

**Figure 234 Example log report for XIP600**

```
XIP600 AUG31 08:16:32 8658 INFO Miscellaneous Problem
         REASON: Invalid DNS Address
         MESSAGE:
         00 30 00 30 00 30 00 00 00 65 00 28 00 00 00 00 00 00 40 07
         00 00 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72
         73 74 75 76 77 78 79 7A
```

The XIP600 log report includes reason text, the values for which are listed in Table 139.

**Table 139 XIP600 reason text**

| Reason text | Meaning |
|---|---|
| Reassembly Failure | The CM data communication (CMDC) application is unable to re-assemble the message packets received from the XPM. |
| MTS_RC= <return code> <return code text> | The MTS_RC return code and return text are the reasons the message could not be sent. |
| Invalid BCS Number | The CMDC application received an invalid BCS number from the XPM. |
| ComID out of Range | The CMDC application received a ComID from the XPM or another application that was out of the allowable range. |
| Invalid Operation Code | The CMDC application received an invalid operation code from the XPM. |
| Invalid Operation Status | The CMDC application received an invalid operation status from the XPM. |
| Invalid Socket Identification Number | The CMDC application received invalid socket id number from the XPM. |
| Invalid IP Address | The CMDC application received an invalid IP address from the XPM. |
| Port Number out of Range | The CMDC application received a port number out of the allowable range from the XPM. |
| Invalid DNS Address Length | The CMDC application received a DNS Address with an invalid length from the XPM. |
| Invalid DNS Address | The CMDC application received an invalid DNS address from the XPM. |
| Invalid Read Status | The CMDC application received an invalid read status from the XPM. |
| Invalid Write Status | The CMDC application received an invalid write status from the XPM. |
| Invalid Ethernet Type | The CMDC application received an invalid ethernet type from the XPM. |
| Invalid Device Type | The CMDC application received an invalid Device Type from the XPM. |
| Number of Gateway Entries out of Range | The CMDC application received an invalid number of gateway entries from the XPM. |
| Number of ComIDs out of Range | The CMDC application received an invalid number of ComIDs from the XPM. |
| Invalid IP Mask | The CMDC application received an invalid IP mask from the XPM. |
| Number of IP Addresses out of Range | The CMDC application received an invalid number of IP addresses from the XPM. |
| Number of Sockets out of Range | The CMDC application received an invalid number of socket identifiers from the XPM. |

**Table 139 XIP600 reason text**

| Reason text | Meaning |
|---|---|
| Number of Bytes in Data out of Range | The CMDC application received an invalid number of bytes in the application data from the XPM. |
| Number of Bytes Queued for Sending out of Range | The CMDC application received an invalid number of bytes queue for sending from the XPM. |
| Invalid ComID Status | The CMDC application received an invalid ComID status from the XPM. |
| Invalid Socket Port Type | The CMDC application received an invalid socket port type from the XPM. |
| Invalid Socket State | The CMDC application received an invalid socket state from the XPM. |
| Invalid Message Length | The CMDC application received an invalid message length from the XPM. |
| Invalid Packet Length | The CMDC application received an invalid packet length from the XPM. |
| Invalid Packet Offset | The CMDC application received an invalid packet offset from the XPM. |
| Invalid ICMP Code | The CMDC application received an invalid ICMP code from the XPM. |
| Invalid ICMP Type | The CMDC application received an invalid ICMP type from the XPM. |
| BMS Buffers Extended | The CMDC application extended the number of BMS buffers (see Note 1). |
| BMS Buffer Extension Failure | The CMDC application failed to extend the number of BMS buffers (see Note 1). |
| RSI Reassembly Packet Collision | The CMDC application received a packet that has caused a reassembly collision (see Note 2). |
| Miscellaneous Decode Error | The CMDC application encountered a miscellaneous decode error. |
| Unknown Reason | The CMDC application received an unknown error from the XPM. |
| Invalid Socket Option Type | The CMDC application received an invalid socket option from the XPM. |
| ***Note 1:*** The CMDC application uses Buffer Management System (BMS) buffers to hold incoming messages from the XPM while the application decodes the message. These buffers are neither engineered nor visible by the user. During high traffic times, the CMDC application may need to increase the number of BMS buffers it uses.<br>***Note 2:*** When a reassembly packet collision occurs the packet may be discarded, which results in a reassembly failure. | |

## Action

If message corruption is suspected, investigate the data path from the CM to the IP-XPM. If message corruption is not suspected, get additional information from PM189 logs or SWERRs (software errors).

### Associated OM registers

This log is associated with the following registers in OM group XIPCOMID:

- UMSSNF
- UMSRCF
- TMSSNF
- TMSRCF

This log is associated with the following registers in OM group XIPDCOM:

- UMSGSNF
- UMSGRCF
- TMSGSNF
- TMSGRCF
- ICREQSF
- ICREPF

This log is associated with the following registers in OM group XIPSVCS:

- UMSGSNDF
- UMSGRCVF
- TMSGSNDF
- TMSGRCVF

This log is associated with the following registers in OM group XIPMISC:

- PKTSNER
- PKTRCER

***Note:*** For details on these OM registers, refer to Chapter 13: "TOPS-IP OMs."

## XIP890

This log is generated when the message tracing option is enabled in the XIPVER tool. The log report displays the following information on the *outgoing* message sent from the CM to the SX05DA:

- service name
- COMID
- XPM name and number
- message identifier
- destination IP address
- destination port

- operation code
- message data

***Note 1:*** If a message cannot be sent to the XPM for any reason, this log is not generated.

***Note 2:*** The message data field is limited to 280 bytes. Any data greater than (or equal to) 280 bytes is truncated with the text: “Message truncated to 280 bytes.”

***Note 3:*** For details on XIPVER commands, refer to Chapter 11: “TOPS-IP CI tools.”

The following figure shows an example log report.

**Figure 235 Example log report for XIP890**

```
XIP890 SEP08 14:59:57 1032 INFO Trace Outgoing Message
          SERVICE   : REMOTE1_IPSVC        COMID      :     4
          PERIPHERAL: DTC       10         MSGID      :     9
          SRC IP    :                      SRC PORT # :
          DST IP    :  47 156 160 179      DST PORT # :  8600
          OP CODE   : 00001101 00001010
          MESSAGE DATA:
          00 30 01 7C 01 18 00 00 00 09 00 28 00 00 01 02 03 04 80 15
          FF FF 2F 9C A0 B3 15 7C 01 5E 48 65 6C 6C 6F 20 57 6F 72 6C
          64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C
          6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64
          0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F
          20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D
          0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20
          57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A
          48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57
          6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48
          65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F
          72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65
          6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72
          6C 64 0D 0A 48 65 6C 6C 6F 20 57 6F 72 6C 64 0D 0A 48 65 6C
          Message truncated to 280 bytes.
```

***Note:*** The SRC (source) IP field and SRC PORT # field are not filled in for outgoing messages. Also, depending on whether data is sent over the IP network, the DST IP field and DST PORT # field may not be filled in.

## Action

None; this log is for information only.

## Associated OM registers

None.

## XIP891

This log is generated when the message tracing option is enabled in the XIPVER tool. The log report displays the following information on the *incoming* message sent from the SX05DA to the CM:

- service name
- COMID
- XPM name and number
- message identifier
- source IP address
- source port
- operation code
- message data

***Note 1:*** If the message received from the XPM cannot be decoded for any reason, this log is not generated.

***Note 2:*** The message data field is limited to 280 bytes. Any data greater than (or equal to) 280 bytes is truncated with the text: "Message truncated to 280 bytes."

***Note 3:*** For details on XIPVER commands, refer to Chapter 11: "TOPS-IP CI tools."

The following figure shows an example log report.

**Figure 236 Example log report for XIP891**

```
XIP891 SEP08 14:59:57 1032 INFO Trace Incoming Message
          SERVICE   : REMOTE1_IPSVC        COMID      :     4
          PERIPHERAL: DTC       10         MSGID      :    80
          SRC IP    : 47 156 160 179       SRC PORT # :  8600
          DST IP    :                      DST PORT # :
          OP CODE   : 00001101 00001010
          MESSAGE DATA:
          00 30 01 7C 01 18 00 00 00 09 00 28 00 00 01 02 03 04 80 15
          FF FF 2F 9C A0 B3 15 7C 01 5E 48 65 6C 6C 6F 20 57 6F 72 6C
          64 0D 0A 48 65 6C 6C 6F 20 57
```

***Note:*** The DST (destination) IP field and DST PORT # field are not filled in for incoming messages. Also, depending on whether data is received over the IP network, the SRC IP field and SRC PORT # field may not be filled in.

### Action

None; this log is for information only.

### Associated OM registers

None.

## XIP892

This log is generated when the packet tracing option is enabled in the XIPVER tool. The log report displays the message identifier and packet data for the *outgoing* packet sent from the CM to the SX05DA. When a message is segmented into multiple packets, this log is generated for each packet of the message.

***Note:*** If a packet cannot be sent to the XPM for any reason, this log is not generated.

The following figure shows an example log report.

**Figure 237 Example log report for XIP892**

```
XIP892 AUG31 08:16:32 8658 INFO Trace Outgoing Packet
         MSGID: 9
         PACKET DATA:
         00 30 00 30 00 30 00 00 00 65 00 28 00 00 00 00 00 00 40 07
         00 00 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72
         73 74 75 76 77 78 79 7A
```

### Action

None; this log is for information only.

### Associated OM registers

None.

## XIP893

This log is generated when the packet tracing option is enabled in the XIPVER tool. The log report displays the message identifier and packet data for the *incoming* packet sent from the SX05DA to the CM. When a message is segmented into multiple packets, this log is generated for each packet of the message.

***Note:*** This log is not generated under any of the following conditions:

- if the packet received from an XPM cannot obtain a buffer
- if the packet contains an invalid BCS number
- if the packet length does not equal the number of bytes in the packet

The following figure shows an example log report.

**Figure 238 Example log report for XIP893**

```
XIP893 AUG31 08:16:32 8658 INFO Trace Incoming Packet
         MSGID: 80
         PACKET DATA:
         00 30 00 30 00 30 00 00 00 65 00 28 00 00 00 00 00 00 40 07
         00 00 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72
         73 74 75 76 77 78 79 7A
```

### Action

None; this log is for information only.

### Associated OM registers

None.

## EXT106

This log is generated each time the TQMS_MIS_MINOR alarm goes on or off for the TOPS QMS MIS IP application. The log report displays the name of the alarm and its state (ON or OFF). The following figure shows an example log report.

**Figure 239 Example log report for EXT106**

```
EXT106 NOV10 20:15:39 2500 INFO TQMS_MIS_MINOR ON
         TQMS_MIS_IP_CONN
```

### Action

Check the value of the parameter QMS_MIS_MINOR_ALARM_THRESH datafilled in table TQMISOPT. Also, check the state of the TCP/IP connection.

### Associated OM registers

None.

## EXT107

This log is generated each time the TQMS_MIS_MAJOR alarm goes on or off for the TOPS QMS MIS IP application. The log report displays the name of the alarm and its state (ON or OFF). The following figure shows an example log report.

**Figure 240 Example log report for EXT107**

```
EXT107 NOV10 20:15:39 2500 INFO TQMS_MIS_MAJOR ON
         TQMS_MIS_IP_CONN
```

### Action

Check the value of the parameter QMS_MIS_MAJOR_ALARM_THRESH datafilled in table TQMISOPT. Also check the state of the TCP/IP connection.

### Associated OM registers

None.

## EXT108

This log is generated each time the TQMS_MIS_CRITICAL alarm goes on or off for the TOPS QMS MIS IP application. The log report displays the name of the alarm and its state (ON or OFF). The following figure shows an example log report.

**Figure 241 Example log report for EXT108**

```
EXT108 NOV10 20:15:39 2500 INFO TQMS_MIS_CRITICAL ON
         TQMS_MIS_IP_CONN
```

An EXT108 log is also generated when the TQMS_MIS_PROCESS alarm goes on or off. The log report displays the name of the alarm and its state (ON or OFF). The following figure shows an example log report.

**Figure 242 Example log report for EXT108**

```
EXT108 NOV10 20:15:39 2500 INFO TQMS_MIS_PROCESS ON
         TQMS_MIS_IP_CHILD_DEAD
```

### Action

- For a TQMS_MIS_CRITICAL alarm, check the value of the parameter QMS_MIS_CRITICAL_ALARM_THRESH datafilled in table TQMISOPT. Also check the state of the TCP/IP connection.
- For a TQMS_MIS_PROCESS alarm, use the MISCHILD command in the TQMIST tool to manually recreate the MIS child process.

### Associated OM registers

None.

## QMIS102

This log is generated the first time an IP connection is unable to transmit a TOPS QMS MIS buffer. If the IP connection fails to transmit consecutive buffers, the log is not generated again. The log report displays the date and time of the transmission failure, the application (TOPS), and the associated COMID. The following figure shows an example log report.

**Figure 243 Example log report for QMIS102**

```
QMIS102 AUG31 08:16:32 8658 INFO QMS_MIS_IP_SEND_FAIL
          APPLN = TOPS
          COMID = 20
```

### Action

Investigate data connectivity between the DMS switch and the external MIS reporting facility.

### Associated OM registers

None.

## QMIS103

This log is generated if a closesocket failure occurs when the TOPS QMS MIS IP application tries to close an established connection. The log report displays the date and time of the closesocket failure, the application (TOPS), and the associated COMID. The following figure shows an example log report.

**Figure 244 Example log report for QMIS103**

```
QMIS103 AUG31 08:16:32 8658 INFO QMS_MIS_CLOSESOCKET_FAIL
          APPLN = TOPS
          COMID = 18
```

### Action

Use the FORCECLOSE command in the XIPVER tool to close the open socket. To determine why the socket is failing, use the QUERYCOMID command in the XIPVER tool. Refer to Chapter 11: “TOPS-IP CI tools” for details on the commands.

### Associated OM registers

None.

## TOPS106

This log is generated for various problems with OC-IP and TDM OC data links. With OC-IP, it is generated only when no data links are available. The log report displays the virtual circuit number, OC office name, trouble code, and other fields that are not relevant when no data links are available. The following figure shows an example log report.

***Note:*** TDM OC links must be replaced by OC-IP links. Once upgraded to SN08 or higher, the function of this log will change.

**Figure 245 Example log report for TOPS106**

```
TOPS106 AUG31 08:16:32 8658 SYSB TOPS DATALINK TROUBLE
TOPSVCCT 0503CD
PROBLEMNO = 0
OCOFC = DAHOST  OCIPDLNUM = NA
TRBLCODE = NO_DATALINK_MEMBERS_AVAILABLE
```

### Action

Check the data links to the reported office at the OCDL level of the MAP. Refer to Chapter 10: “TOPS-IP maintenance activities” for details on MAP commands.

### Associated OM registers

TOPS106 is associated with the VCFL register in OM group TOPSVC.

## TOPS112

This log is generated when an audit process finds a virtual circuit that was marked busy but not linked to a call. The system idles the virtual circuit. No action is needed. The following figure shows an example log report.

**Figure 246 Example log report for TOPS112**

```
TOPS112 AUG31 08:16:32 8658 INFO BUSY TERMINAL CIRCUIT FOUND
   HOST OFFICE IS DAHOST
   VIRTUAL CIRCUIT NUMBER = 17
   THE VIRTUAL CIRCUIT HAS BEEN IDLED
```

### Action

None.

### Associated OM registers

None.

# TOPS133

This log is generated when trouble occurs during OC-IP call processing. It displays information on the IP voice and data connections used during an OC-IP call. The following figure shows an example log report.

***Note:*** TOPS133 replaces TOPS105 on OC-IP calls.

**Figure 247 Example log report for TOPS133**

```
TOPS133 AUG31 08:16:32 8658 SYSB TOPS OC-IP TROUBLE
Reported in:    Host          To office: REMOTECIP1
Problem number: 1320          Trouble: VOICE_LINK_CONN_FAIL
Remote callid:  Not avail     Host callid: 1967890
Voice info:     CKT REMOTEIPVL 271
   Remote IPGW: Not avail
   Host IPGW:   OCGW 14 5      95.92.9.109 Trunk TID: 103 61
Data info:      TOPSVCCT 1707B6  DLNUM: 0
Text1:          None
Text2:          None
```

## Field description

Because the TOPS133 log report provides many details used to diagnose and troubleshoot OC-IP problems, its fields and values are further explained in Table 140.

***Note:*** Since a single TOPS OC call actually consists of two calls, one in the OC remote and one in the OC host, this section uses the terms “remote call” and “host call.” In some situations, a single TOPS133 log contains information relevant to both the remote and host calls.

**Table 140 TOPS133 field descriptions**

| Field | Value | Description |
|---|---|---|
| Reported in | Remote or Host | Indicates the TOPS OC office type of the switch and call where the log was generated. This information is useful since the TOPS OC HRNQT feature allows a single TOPS OC office to be both a host and a remote. |
| To office | Symbolic text | The name of the distant OC office from table OCOFC. If the “Reported in” field indicates the log was generated in the host, then the “To office” field will contain the call’s remote switch. If the “Reported in” field indicates the log was generated in the remote, then the “To office” field will contain the call’s host switch. |
| Problem number | Numeric | This field contains an integer from 1 to 5 digits in length. The number is generated by TOPS OC-IP software and is intended to be used by Nortel Networks field support. More information about problem numbers begins on page 456. |

**Table 140 TOPS133 field descriptions**

| Field | Value | Description |
|---|---|---|
| Trouble | MESSAGING_PROBLEM,<br>OPR_ACK_WAIT_TIMEOUT,<br>TABLE_OCGRP_DATA,<br>VOICE_LINK_NOT_ AVAILABLE,<br>VOICE_LINK_CONN_FAIL,<br>VOICE_BYPASS_CONN_FAIL,<br>EXT_BLOCK_UNAVAILABLE,<br>PORTPERM_BLOCK_ UNAVAILABLE,<br>OC_MISCELLANEOUS | Indicates the reason the log was generated. See “Action” on page 454 for more explanation. |
| Remote callid | 0 to 4294967295, or “Not avail” | The call identifier of the call in the OC remote switch. This call identifier is passed to the host switch during OC-IP call setup, so TOPS133 logs generated in the host as well as the remote should contain the remote callid.<br>Since the TOPS133 log can also be generated by TOPS OC-IP maintenance code, this field may contain “Not avail,” which means the callid is not available. |
| Host callid | 0 to 4294967295, or “Not avail” | The call identifier of the call in the OC host switch. This call identifier is not passed to the remote switch. So when the TOPS133 is generated in the remote, the “Host callid” field will contain “Not avail,” which means the callid is not available.<br>“Not avail” can also appear if the TOPS133 log is generated by TOPS OC-IP maintenance code. |
| Voice info | Call processing identifier (CP_ID) | The OC-IP voice link in use by the call that generated the log. Since the TOPS133 log can be generated before a voice link is allocated, or by a maintenance process, it is possible for this field to be blank, which means no voice link is in use.<br>***Note:*** The voice link is a trunk member datafilled on the call’s NT7X07 Gateway card. |

**Table 140 TOPS133 field descriptions**

| Field | Value | Description |
|---|---|---|
| Remote IPGW | Contains three components:<br>1. The IP Gateway (NT7X07 card) in use by the remote call.<br>2. The IP address of that IPGW.<br>3. The terminal identifier (TID) of the specific voice link in use by the remote call.<br>Otherwise, if no IPGW card is in use by the call or maintenance process, the value is “None.” | Provides information about the OC-IP voice link, which is provided by the IP Gateway card as datafilled in table IPINV. Each IPGW card supports 48 TOPS OC-IP voice links. The IPGW card converts voice from the DMS switch to voice over IP (VoIP), and vice versa.<br>When this log is generated in the host, or by a maintenance process, the remote IPGW is not known, and the value is “None.” |
| Host IPGW | Same as Remote IPGW (previous).<br>When generated in remote, contains the host’s IPGW IP address and trunk TID. But the name of the IPGW card (as datafilled in the host’s table IPINV) is not sent to the remote. So the first component is set to “Not avail.” | Same as “Remote IPGW,” except that this field will be populated in the remote. During TOPS OC-IP call setup, the remote receives the IP address and trunk TID of the host’s voice link. This enables the remote to initiate a VoIP call to the host. Since the remote knows the IP address and trunk TID, these values are output in the log (if the call has progressed to the point where this information is received by the remote).<br>During an OC-IP host voice bypass call, there is no voice path in the host switch, so there is no host IPGW to display in this field. Instead, this field is populated with the IP address and floor plan number of the IP position. |
| Data info | Virtual circuit call processing identifier (CP_ID) | The virtual circuit identifier. An OC-IP call is not given its own data link. Instead, it is given a virtual data link on a physical link shared with many other OC-IP calls. This virtual circuit is identified by an office number (the most significant two digits) and a circuit number (the least significant 4 digits).<br>The office number corresponds to the tuple in table OCOFC.<br>For example, TOPSVCCT 160568 means office number 16 (hex) and circuit number 0568 (hex).<br>***Note:*** To determine the IP addresses and IP-XPMs involved, it is necessary to examine the DLNUM field. |

**Table 140 TOPS133 field descriptions**

| Field | Value | Description |
|---|---|---|
| DLNUM | 0 to 7 | Identifies the specific OC-IP data link number that encountered trouble. OC-IP data links are datafilled in table OCIPDL.<br><br>To determine the local IP-XPM and the local and distant IP addresses involved in the call, use the "To office" field combined with the "DLNUM" field to post the data link at the MAPCI->MTC->APPL->TOPSIP->OCDL level of the MAP, and then issue the QOCDL command both with and without the CNTRS parameter. |
| Text1 | Alphanumeric characters or "None" | Provides an additional character string that is useful in debugging OC-IP problems. The contents of the string are determined by the code for the particular call event. If no string is supplied by the code, "None" is output. |
| Text2 | Alphanumeric characters or "None" | Same as "Text1" |

## Action

Table 141 lists user actions for each trouble code.

**Table 141 TOPS133 trouble code text descriptions and actions**

| Trouble code text | Description | Action |
|---|---|---|
| MESSAGING_PROBLEM | The OC host and remote are not in sync in their messaging on a call. This can occasionally happen in race situations when the call has been taken down in the host or remote but not in both. If this problem happens often, there may be a network failure.<br><br>This trouble code can also appear when the IP-XPM cannot send an IP message due to insufficient resources. If this is the case, appropriate error test is output in the "Text1" field. | Using IP network management tools, investigate the network to ensure that it is operating properly.<br><br>Field support can use the other information in the log to further analyze the problem. |

**Table 141 TOPS133 trouble code text descriptions and actions**

| Trouble code text | Description | Action |
|---|---|---|
| OPR_ACK_WAIT_TIMEOUT | The host or remote timed out waiting for a call control message on the OC data link.<br>Occasional appearance of this log can indicate race conditions, which may be ignored. More frequent appearance suggests probable network problems, which should be corrected.<br>If a message was lost, this log always indicates that it was an OC data link message. | Using IP network management tools, investigate the network to ensure that it is operating properly.<br>Field support can use the other information in the log to further analyze the problem. |
| TABLE_OCGRP_DATA | A call is trying to initiate communication on a data link to an office that is not datafilled in table OCGRP. This could happen in an extremely rare race scenario if a tuple has just been removed from OCGRP, but more likely it indicates a software error. | Ignore this log if it is generated immediately after a change in table OCGRP. Otherwise, contact technical support. |
| VOICE_LINK_NOT_ AVAILABLE | Indicates a trunk selection failure in the host or remote. It can also indicate an insufficient number of voice links to a given OC office. | Ensure that the associated 7X07 Gateway card, trunk, and peripheral are in service. Also ensure that enough voice links are available to handle the anticipated volume of traffic. |
| VOICE_LINK_CONN_FAIL | Indicates a voice setup failure between OC host and remote switches.<br>Failure could be due to the loss of an OC data link message, loss of an ISUP/IGIP message, or a release message received on the voice link. | Field support can use information in TOPS133 to diagnose these failures. Also check for any associated IPGW log reports. |
| VOICE_BYPASS_CONN_ FAIL | Similar to VOICE_LINK_CONN_FAIL, except the voice setup failure was between an OC remote switch and an IP position.<br>Here the failure was either loss of a voice setup or answer message, or a release message received on the voice link. | Field support can use information in TOPS133 to diagnose these failures. Also check for any associated IPGW log reports. |

**Table 141 TOPS133 trouble code text descriptions and actions**

| Trouble code text | Description | Action |
|---|---|---|
| EXT_BLOCK_UNAVAILABLE | An OC EXT block could not be allocated in a host office. | Consider increasing the TOPS_NUM_OC parameter in table OFCENG. |
| PORTPERM_BLOCK_ UNAVAILABLE | A PORTPERM EXT block could not be allocated in a remote office. | The number of available PORTPERM blocks is controlled by the OFCAUT utility, which automatically allocates additional data store when needed. (Refer to the NUMPERMEXT tuple in table OFCAUT.) Consider increasing system memory. |
| OC_MISCELLANEOUS | Any trouble other than the ones listed above. The “Text1” and “Text2” fields provide more information about the trouble.<br>This value will appear when the TOPS133 log is generated due to an operator entering a trouble report. See “Other associations” on page 459 for more information. | The additional information can be used to diagnose the problem.<br>If an IP position number is present, field support can bring test calls to the position to verify VoIP speech quality. |

***Note:*** A TOPS102 log and/or a TRK123 log may be generated along with a TOPS133 log. Typically TOPS133 is seen in one switch, while TOPS102 or TRK123 is generated in the other switch. When this situation occurs, TOPS102 and TRK123 logs indicate that a problem was detected at the distant end and resources are being released at this end. Refer to *Log Report Reference Manual* for details on these log reports.

As previously noted, the problem number field of the TOPS133 log is intended for use by Nortel Networks field support. However, some operating companies may find an explanation of the problem numbers useful in troubleshooting, or at least in assessing the seriousness of a log. The following material about problem numbers is optional and requires a deeper understanding of internal DMS call processing than some operating companies may have.

TOPS133 problem numbers have different meanings for different trouble codes, and for some trouble codes they have no meaning. The problem numbers most likely to be useful in troubleshooting are the ones for trouble codes MESSAGING_PROBLEM, OPR_ACK_WAIT_TIMEOUT, VOICE_LINK_CONN_FAIL, and VOICE_BYPASS_CONN_FAIL.

Problem numbers for trouble code MESSAGING_PROBLEM are listed with explanations in Table 142. In this table, “initial” and “non-initial” messages refer to ones designated by the sender as the first, or not the first, message in a call. Table 142 applies only if the Text1 field does not provide further information.

**Table 142 TOPS133 problem numbers for trouble code MESSAGING_PROBLEM**

| Problem number | Explanation |
|---|---|
| 1 | An initial message was received on a virtual circuit that was not associated with any call on this switch, but was marked as being in-use. This may indicate a software bug. |
| 2 | A non-initial message was received on a virtual circuit that was associated with a call on this switch but was marked idle. This may indicate a software bug. |
| 3 | An initial message was received on a virtual circuit that was already associated with a call on this switch. This is most likely to happen in an OC host when the remote has terminated a call but the host doesn’t know that yet, and the remote selects the same virtual circuit for a new call. |
| 4 | A non-initial message was received on a virtual circuit that was not associated with any call on this switch. This is most likely to happen when either the host or the remote has terminated the call but the other switch doesn’t know that yet, and sends a message about the call. Usually this problem number for a MESSAGING_PROBLEM does not indicate an operation-affecting problem. |

The problem number for trouble codes VOICE_LINK_CONN_FAIL and VOICE_BYPASS_CONN_FAIL provides information about the point in the call where the problem was detected. These problem numbers have four digits, say "ABCD," which can be interpreted as follows:

**Table 143 TOPS133 problem numbers for trouble codes VOICE_LINK_CONN_FAIL and VOICE_BYPASS_CONN_FAIL**

| Digit position | Meaning of digit position | Value[a] | Explanation |
|---|---|---|---|
| A | Voice link type | 1 | OC-IP (with TDM position) |
| | | 2 | IP position |
| B | Environment of call for which log was generated | 1 | Standalone |
| | | 2 | OC Remote |
| | | 3 | OC Host |
| | | 4 | OSSAIN (may be standalone or OC remote) |
| C | Event | 1 | Time-out waiting for Got Operator message, after sending voice setup request (ISUP IAM) |
| | | 2 | Time-out waiting for OC-IP voice setup request (ISUP IAM) or voice answer message |
| | | 3 | Time-out waiting for IP position voice answer message |
| | | 4 | Clear Forward message (ISUP Release) received on IP voice link |
| D | Operator type | 1 | Main operator (the usual case) |
| | | 2 | Auxiliary operator (CSE for assistance) |
| **Examples** | | | |
| Problem number: 1320 | | OC-IP call timed out in OC host waiting for voice setup request (ISUP IAM) from remote. | |
| Problem number: 1242 | | OC-IP call in remote switch received unexpected Clear Forward or ISUP Release message on IP voice link of second operator on the call. | |

a. If the category for a digit position does not apply, or if the value is unknown, value 0 is used.

The problem number for trouble code OPR_ACK_WAIT_TIMEOUT also provides information about the point in the call where the problem was detected, but a different scheme is used here. Table 144 lists the most common problem numbers for OPR_ACK_WAIT_TIMEOUT, with explanations. (The problem numbers not listed are for more obscure scenarios that require a deeper knowledge of the DMS code and message flows.

**Table 144 Selected TOPS133 problem numbers for trouble code OPR_ACK_WAIT_TIMEOUT**

| Problem number | Explanation |
|---|---|
| 1 | OC remote requested an operator and timed out waiting for response from host. |
| 2 | OC remote sent message to host to cancel a request for an operator, and timed out waiting for acknowledgment from host. |
| 3 | OC remote sent message to host telling it to release an operator, and timed out waiting for response from host. |
| 9 | OC host timed out waiting for the remote to send the first screen update in a call. |

### Associated OM registers

TOPS133 is associated with the following registers in OM group TOPSVC:

- VCFL
- MSGLOST
- OPRLOST

### Other associations

The TOPS133 log is generated when an operator on an OC-IP call enters a trouble report. Operators should be instructed to enter a trouble report (using the Trouble function) when they experience poor speech quality. The TOPS133 provides information which might be useful when troubleshooting poor speech quality on a TOPS-IP call.

Entry of a trouble report by an operator usually results in the generation of a SNAC log or a TOPS104 (ACTS trouble) log. The TOPS133 will accompany these logs.

When the TOPS133 log is generated as a result of trouble report entry, the fields will be set as follows. Other fields will be set as described in “TOPS133 field descriptions” on page 451.

- Problem number: Contains trouble code number entered by operator
- Trouble: Set to “OC_MISCELLANEOUS”
- Text1: Set to “SNAC additional OC-IP information”
- Text2: Contains the operator and position numbers

# TOPS134

This log was added in TOPS17. It reports call processing problems with IP positions. It displays information about the voice connection and the position.

The TOPS134 log can be generated during standalone calls, or in the host when TDM OC and IP positions are in use. If a failure occurs during an OC-IP host voice bypass call, the TOPS133 log is generated because it contains OC information as well as IP position information. The TOPS133 log is described beginning on page 451.

The following figure shows an example TOPS134 log report.

**Figure 248 Example log report for TOPS134**

```
TOPS134 AUG31 08:16:32 8658 SYSB TOPS IPPOS TROUBLE
Problem number: 2131          Trouble: VOICE_LINK_CONN_FAIL
Callid:         131812
Voice info:     CKT POSIPVL1 45
   IPGW:        TGWY   2 5  95.64.10.113     Trunk TID: 68 78
Position info:  Pos: 613    IP Addr: 95.92.18.13
Text1:          None
Text2:          None
```

## Field description

Because the TOPS134 log report provides many details used to diagnose and troubleshoot IP position problems, its fields and values are further explained in Table 145.

**Table 145 TOPS134 field descriptions**

| Field | Value | Description |
|---|---|---|
| Problem number | Numeric | This field contains an integer from 1 to 5 digits in length. The number is generated by TOPS-IP position software and is intended to be used by Nortel Networks field support. More information about problem numbers is on page 463. |
| Trouble | VOICE_LINK_NOT_ AVAILABLE,<br>VOICE_LINK_CONN_FAIL,<br>EXT_BLOCK_UNAVAILABLE,<br>PORTPERM_BLOCK_ UNAVAILABLE,<br>OC_MISCELLANEOUS | Indicates the reason the log was generated. See “Action” on page 461 for more explanation. |
| Callid | 0 to 4294967295 | The call identifier of the call in the standalone or OC host switch. |

**Table 145 TOPS134 field descriptions**

| Field | Value | Description |
|---|---|---|
| Voice info | Call processing identifier (CP_ID) | The IP position voice link in use by the call that generated the log. Since the TOPS134 log is generated when voice link allocation fails, it is possible for this field to be blank, which means no voice link was associated with the call.<br>***Note:*** The voice link is a trunk member datafilled on the call's NT7X07 Gateway card. |
| IPGW | Contains three components:<br>1. The IP Gateway (NT7X07 card) in use by the call.<br>2. The IP address of that IPGW.<br>3. The terminal identifier (TID) of the specific voice link in use by the call.<br>Otherwise, if no IPGW card is in use by the call or maintenance process, the value is "None." | Provides information about the IP position voice link, which is provided by the IP Gateway card as datafilled in table IPINV. Each IPGW card supports 48 TOPS IP position voice links. The IPGW card converts voice from the DMS switch to voice over IP (VoIP), and vice versa.<br>When this log is generated due to voice link allocation failure, the IPGW is not known, and the value is "None." |
| Position info | Contains two components:<br>1. The position's floor plan number from Table TOPSPOS.<br>2. The position's IP address. | This field indicates the IP position whose voice connection failed. The IP address is included since this is not available through switch datafill. The IP address is provided by the position when it requests to be brought into service. |
| Text1 | Alphanumeric characters or "None" | Provides an additional character string that is useful in debugging IP position problems. The contents of the string are determined by the code for the particular call event. If no string is supplied by the code, "None" is output. |
| Text2 | Alphanumeric characters or "None" | Same as "Text1" |

## Action

Table 146 lists user actions for each trouble code. Note these trouble codes are a subset of the trouble codes applicable to OC-IP calls (see "Action" on page 454).

**Table 146 TOPS134 trouble code text descriptions and actions**

| Trouble code text | Description | Action |
|---|---|---|
| VOICE_LINK_NOT_ AVAILABLE | Indicates a trunk selection failure in the standalone or host. It can also indicate an insufficient number of voice links to connect all available IP positions. | Ensure that the associated 7X07 Gateway card, trunk, and peripheral are in service. Also ensure that enough voice links are available to handle the anticipated volume of traffic. |

**Table 146 TOPS134 trouble code text descriptions and actions**

| Trouble code text | Description | Action |
|---|---|---|
| VOICE_LINK_CONN_FAIL | Indicates a voice setup failure between the standalone or host switch and the IP position.<br>Failure could be due to the loss of an ISUP/VoIP call setup message, or a release message received on the voice link. | Field support can use information in TOPS134 to diagnose these failures. Also check for any associated IPGW and position log reports. |
| EXT_BLOCK_UNAVAILABLE | An OC EXT block could not be allocated in a host office. | Consider increasing the TOPS_NUM_OC parameter in table OFCENG. |
| PORTPERM_BLOCK_ UNAVAILABLE | A PORTPERM EXT block could not be allocated in a standalone or host office. | The number of available PORTPERM blocks is controlled by the OFCAUT utility, which automatically allocates additional data store when needed. (Refer to the NUMPERMEXT tuple in table OFCAUT.) Consider increasing system memory. |
| OC_MISCELLANEOUS | Any trouble other than the ones listed above. The “Text1” and “Text2” fields provide more information about the trouble.<br>This value will appear when the TOPS134 log is generated due to an operator entering a trouble report. See “Other associations” on page 463 for more information. | The additional information can be used to diagnose the problem.<br>If an IP position number is present, field support can bring test calls to the position to verify VoIP speech quality. |

As previously noted, the problem number field of the TOPS134 log is intended for use by Nortel Networks field support. However, some operating companies may find an explanation of the problem numbers useful in troubleshooting, or at least in assessing the seriousness of a log. The following material about problem numbers is optional and requires a deeper understanding of internal DMS call processing than some operating companies may have.

As with TOPS133 problem numbers, TOPS134 problem numbers have different meanings for different trouble codes, and for some trouble codes they have no meaning. The problem numbers most likely to be useful in troubleshooting IP positions are related to the VOICE_LINK_CONN_FAIL trouble code. These problem numbers have four digits, say "ABCD," which can be interpreted as follows:

**Table 147 TOPS134 problem numbers for trouble code VOICE_LINK_CONN_FAIL**

| Digit position | Meaning of digit position | Value[a] | Explanation |
|---|---|---|---|
| A | Voice link type | 2 | IP position |
| B | Environment of call for which log was generated | 1 | Standalone |
| | | 3 | OC Host |
| | | 4 | OSSAIN (may be standalone or OC host) |
| C | Event | 3 | Time-out waiting for IP position voice answer message |
| | | 4 | Clear Forward message (ISUP Release) received on IP voice link |
| D | Operator type | 1 | Main operator (the usual case) |
| | | 2 | Auxiliary operator (CSE for assistance) |
| **Examples** | | | |
| Problem number: 2141 | On a standalone call, the voice setup to an IP position failed because an unexpected ISUP Release was received. | | |
| Problem number: 2331 | The host call timed out waiting for the answer message from the IP position. | | |

a. If the category for a digit position does not apply, or if the value is unknown, value 0 is used.

## Associated OM registers

None.

## Other associations

The TOPS134 log is generated when an operator at a standalone IP position enters a trouble report. Operators should be instructed to enter a trouble report (using the Trouble function) when they experience poor speech quality. The TOPS134 provides information which might be useful when troubleshooting poor speech quality on a TOPS-IP call.

Entry of a trouble report by an operator usually results in the generation of a SNAC log or a TOPS104 (ACTS trouble) log. The TOPS134 will accompany these logs.

When the TOPS134 log is generated as a result of trouble report entry, the fields will be set as follows. Other fields will be set as described in "TOPS134 field descriptions" on page 460.

- Problem number: Contains trouble code number entered by operator
- Trouble: Set to "OC_MISCELLANEOUS"
- Text1: Set to "SNAC additional IPPOS information"
- Text2: Contains the operator and position numbers

## TOPS135

This log is generated whenever the system attempts to open a socket for IP position data connectivity. It reports on the success or failure of the attempt. Failure to open a socket causes positions datafilled against the corresponding COMID to be SYSB, and a major TPSysB (TOPS position system busy) alarm is raised.

In addition to the alarm indication, this log includes the COMID (from table IPCOMID), the XPM name, and the event. Possible events are "Failed to open socket" and "Socket opened." The following figure shows examples.

**Figure 249 Example log report for TOPS135**

```
** TOPS135 JUN23 18:12:05 5050 SYSB IP Position Socket Info
Comid: 302 (DTC 14)
Event: Failed to open socket

TOPS135 JUN23 18:12:05 5050 SYSB IP Position Socket Info
Comid: 302 (DTC 14)
Event: Socket opened
```

***Note:*** Even when a TOPS135 log indicates that a socket has been opened, as in the second example above, the TPSysB alarm may still be raised. This happens if there are SYSB positions that use other comids, or there may be positions that use this COMID but are SYSB for reasons other than socket trouble.

### Action

No action is necessary if the log indicates that a socket has been opened.

If the log reports failure to open a socket, first check the XPM at the PM level of the MAP. After any trouble with the XPM has been resolved, go to the MAPCI;MTC;APPL;TOPSIP;TOPSPOS MAP level and post the positions that use the COMID. Manually BSY/RTS one or more of the positions. If the problem continues after several manual attempts, collect logs and contact Nortel Networks technical support.

***Note:*** SX05DA socket states are preserved over XPM SWACTs. So if the system has failed to open a socket, simply SWACTing the XPM will not cause the system to try again to open the socket. RTSing a position that is datafilled to use the socket will cause the system to attempt to open the socket if it is not already open.

### Associated OM registers

None.

## TOPS136

This log reports information that IP positions may provide to the switch about their external database connectivity. It is associated with the TPExDB (TOPS position external database) alarm.

The log identifies the position that provided the information (position number from table TOPSPOS), tells whether the position reported that trouble exists or does not exist, and includes an alarm indication. The following figure shows an example.

**Figure 250 Example log reports for TOPS136**

```
** TOPS136 AUG31 08:16:32 8658 INFO IP Position External Database
Pos:   653
Event: Position reported trouble

TOPS136 AUG31 08:17:05 8658 INFO IP Position External Database
Pos:   653
Event: Position reported trouble is cleared
```

***Note:*** The number of asterisks displayed in the log indicates whether the position reported the trouble as minor (*), major (**), critical (***), or cleared (none). This does not necessarily correspond to the status of the TPExDB alarm. The log concerns only the position that reported the event, while the alarm takes into account all information received from all positions. For example, the alarm may still be raised when the log indicates that a position has reported that any trouble has been cleared, because another position may still be reporting trouble.

### Action

Use the LISTALMS command at the MAPCI;MTC;APPL;TOPSIP;TOPSPOS MAP level to determine which positions are reporting external database trouble. Refer to “TPExDB alarm” on page 366 for more information and actions.

### Associated OM registers

None.

## TOPS137

This log provides information that is useful in troubleshooting a variety of IP position maintenance problems. It includes the position number from table TOPSPOS, trouble and reason text, and additional information text. The following figure shows several examples.

**Figure 251 Example log reports for TOPS137**

```
TOPS137 AUG31 08:16:32 8658 INFO IP Position Maintenance Info
Pos:     431
Trouble: Position datafill error
Reason:  Position not datafilled in TOPSPOS as IP
Info:    InSv message received from 47.142.225.3:6522


TOPS137 AUG31 08:16:32 8658 INFO IP Position Maintenance Info
Pos:     431
Trouble: Position datafill error
Reason:  XPM socket mismatch between switch and position
Info:    TOPSPOS comid 17, position comid 4


TOPS137 AUG31 08:16:32 8658 INFO IP Position Maintenance Info
Pos:     431
Trouble: Unexpected message source
Reason:  Message received from 47.142.221.2:6000
Info:    Expected 47.142.225.61:6000


TOPS137 AUG31 08:16:32 8658 INFO IP Position Maintenance Info
Pos:     431
Trouble: Destination unreachable
Reason:  ICMP code 1
Info:    Address 47.142.225.9:6522


TOPS137 AUG31 08:16:32 8658 INFO IP Position Maintenance Info
Pos:     431
Trouble: Mtc protocol violation
Reason:  Invalid message received from position
Info:    01332A0000C5


TOPS137 AUG31 08:16:32 8658 INFO IP Position Maintenance Info
Pos:     431
Trouble: System dropped pos to CRes
Reason:  Call cleared ack not received
Info:    Address 47.142.225.9:6522
```

The following table details the possible values for the text fields and the recommended actions.

**Table 148 TOPS137 reason text descriptions and actions**

| Trouble text | Reason text | Info text | Explanation | Action |
|---|---|---|---|---|
| Position datafill error | Position not datafilled in TOPSPOS as IP | InSv message received from <ipaddr: port> | The switch received an IP in-service request message from the IP address and port shown in the log, but the position number in the log either is not datafilled in table TOPSPOS, or is datafilled as a TDM position. | Check table TOPSPOS against the position number datafill in the position. |
| Position datafill error | XPM socket mismatch between switch and position | TOPSPOS comid <n>, position comid <m><br>where <n> and <m> are numbers with up to 4 digits | The position is datafilled in table TOPSPOS to use comid <n>, but an in-service request from the position was received at the SX05DA socket associated with comid <m>. | Check datafill in the position for the DMS IP address and port. For the port, compare this with switch datafill in tables TOPSPOS, IPCOMID, and IPSVCS. For the IP address, compare against tables TOPSPOS, IPCOMID, and XPMIPMAP if the CM configuration method is used, or against the DHCP server if the network method is used. |
| Unexpected message source | Message received from <ipaddr1>: <port1> | Expected <ipaddr2>: <port2> | An InSv request message was received from the position, with source IP address and port <ipaddr1:port1>. When the message was received, the same position number was already InSv at the switch, using IP address and port <ipaddr2:port2>. | If the position's IP address or port has recently been changed, and if the position was not properly removed from service at the switch before the change was made, then the log is harmless and normal procedures may be used for bringing the position InSv.<br>Otherwise, investigate whether two different positions might be datafilled with the same position number.<br>If both of the above causes have been ruled out and the log continues to appear, then contact your IP network security personnel, because this log could possibly indicate rogue traffic on the IP network. |

**Table 148 TOPS137 reason text descriptions and actions**

| Trouble text | Reason text | Info text | Explanation | Action |
|---|---|---|---|---|
| Destination unreachable | ICMP code <n><br><br>where <n> is a number with up to 3 digits | Address <ipaddr: port> | The switch received an Internet Control Message Protocol (ICMP) message indicating that the address listed in the Info text could not be reached.<br>The ICMP codes, shown in the reason text, are documented in RFC 792 and may be useful to your network group. | This may be a transient problem. For example, it can occur if the position is rebooted without first removing it from service at the MAP.<br>If the problem does not correct itself within a few minutes and the position appears to be OK, contact your network group for assistance. |
| Mtc protocol violation | Invalid message received from position | <hex dump of message> | An invalid maintenance message has been received from the position.<br>Note: For real-time protection from babbling nodes, the switch does not generate this log if the message has a malformed header. | Contact Nortel Networks (or other position vendor) support, especially if the scenario is reproducible. |
| System dropped pos to CRes | Call cleared ack not received | Address <ipaddr: port> | After releasing a call from the position, the switch did not receive the expected message from the position indicating it was ready to receive the next call. The system has therefore dropped the position to the CRes state. | Normally when this happens, the position will display the assigned activities screen, the operator will key to accept calls, and no further action is necessary.<br>If data communication is really lost with the position, the system will eventually make the position SysB. |

## Action

Refer to Table 148, “TOPS137 reason text descriptions and actions,” on page 467.

## Associated OM registers

None.

## TOPS304

This log is generated when an OC-IP data link enters (or leaves) the system busy (SYSB) state. Since this condition may affect traffic, the OCSysB alarm is also generated. The log report displays the alarm severity, the data link number, and the reason text. The alarm severity is indicated as follows:

- Three asterisks (***) for a critical alarm (no OC-IP data links to a distant office are INSV and at least one data link is SYSB).
- Two asterisks (**) for a major alarm (at least one OC-IP data link to a distant office is SYSB).

The following figure shows an example log report for a major OCSysB alarm.

**Figure 252 Example log report for TOPS304**

```
** TOPS304 JUN23 18:12:05 5050 TBL TOPS IP DataLink Fault
Data Link:  OCIPDL DAHOST 1
Trouble:    Data Link is System Busy
Reason:     Network failure
Error Code: 3
```

The TOPS304 log is also generated when an OC-IP data link leaves the SYSB state (problem successfully resolved). In this case, the log report does not display the asterisks and the TROUBLE field text shows “Resolved.” However, the OCSysB alarm may still be raised due to other SYSB links.

The following figure shows an example log report for a resolved OCSysB alarm (applies only to the specified data link).

**Figure 253 Example log report for TOPS304**

```
TOPS304 JUN23 18:12:05 5050 TBL TOPS IP DataLink Fault
Data Link:  OCIPDL DAHOST 1
Trouble:    Resolved
Reason:     No failure
Error Code: 0
```

### Action

Table 149 lists user actions for each reason. The actions are listed in the order of recovery method, so if a given action succeeds in recovering the data link, no further action is necessary.

**Table 149 TOPS304 reason text descriptions and actions**

| Reason text | Description | Action |
|---|---|---|
| No failure | The data link is not in trouble. | No action is required. |

**Table 149 TOPS304 reason text descriptions and actions**

| Reason text | Description | Action |
|---|---|---|
| CM child dead | The maintenance child process for the data link is dead and not scheduled for recovery. | 1. Use the RECREATE command.<br>2. Delete and re-add datafill for the data link (table OCIPDL), and BSY and RTS it.<br>3. Perform a maintenance SWACT. |
| CM resource failure | The CM encountered problems with internal messaging or sending a message to the XPM. | 1. Check all logs.<br>2. Wait 30 seconds for automatic recovery.<br>3. BSY and RTS the data link. |
| Peripheral failure | 1.The XPM is out of service.<br>2. A socket/COMID error occurred in the XPM.<br>3. The XPM is not responding.<br>4. Other XPM failure | 1. Check the maintenance state of the XPM at the MAP, and recover the XPM if necessary.<br>2. Check all logs.<br>3. Wait 30 seconds for automatic recovery.<br>4. BSY and RTS the data link. |
| Network failure | ICMP destination unreachable errors have occurred on the data link. | 1. Check the maintenance state of the data link at the far-end office.<br>***Note:*** This reason is expected when attempting to bring into service a data link when the socket for the distant data link is not established.<br>2. Check the network.<br>3. Use the PING command in the XIPVER tool to determine if the far end is reachable.<br>***Note:*** Refer to Chapter 11: TOPS-IP CI tools for details on the XIPVER tool. |
| End to end connectivity failure | There is loss of connectivity with the far-end data link. | 1. Check the maintenance state of the data link at the far-end office.<br>2. Use the QOCDL CNTRS command at the MAP.<br>3. Check the network. |

### Associated OM registers

None.

## TOPS305

This log was introduced in TOPS15 to report various troubles related to IP positions. However, it has been obsoleted by several other logs that are described in this section.

## TOPS502

This log is generated when an IP position transitions to or from the SYSB state, unless the SYSB reason is peripheral failure. It is also generated whenever the SYSB reason for a position changes, unless the new reason is peripheral failure. The log is associated with the TPSysB (TOPS position system busy) alarm.

The TOPS502 log displays the position number from table TOPSPOS, the state transition, reason text, and a minor alarm indication (one asterisk) if the transition is to SYSB. The following figure shows several examples.

**Figure 254 Example log reports for TOPS502**

```
* TOPS502 JUN23 18:12:05 5050 INFO IP Position State Change
Pos: 613    Change: from URes to SysB
Reason: InSv request timeout

* TOPS502 JUN23 18:12:05 5050 INFO IP Position State Change
Pos:  613     Change: from CRes to SysB
Reason: MTXBASE_DIED

* TOPS502 JUN23 18:12:05 5050 INFO IP Position State Change
Pos:  613     Change: from CRes to SysB
Reason: Unsolicited OOS notify received (EC 158)

TOPS502 JUN23 18:12:05 5050 INFO IP Position State Change
Pos:  613   Change: from SysB to CRes
Reason: System corrected trouble
```

***Note:*** The presence or absence of asterisks in the TOPS502 log does not necessarily indicate the status of the TPSysB alarm. The log concerns only the position identified in the report, while the alarm takes into account the states of all positions in the office. Refer to “Related alarms” on page 366 for more information about the TPSysB alarm.

The following two tables list and describe the reason texts in the TOPS502 log, along with recommended actions for each. Table 150 includes the reason texts that may accompany a transition *to* SYSB.

**Table 150 TOPS502 reason text descriptions (transition to SYSB) and actions**

| Reason text | Description | Action |
|---|---|---|
| InSv request timeout | The position has been in the URES state for approximately 15 seconds or longer, and the DMS has not received the expected message from the position requesting to come into service.<br>***Note:*** IP positions datafilled in table TOPSPOS with field URESOK=N do not transition to SYSB on failure to send an InSv request message, so this SYSB reason applies only to positions datafilled with URESOK=N. | If the problem resulted from message loss during maintenance activity, it should correct itself automatically. Otherwise the first action is to manually BSY/RTS the position at the MAP. If that fails with the same reason, then check the position itself. If the position is OK, check data connectivity between the switch and position. |
| No response to audit | The position has been in the CRes state for several minutes, and has failed to respond to three consecutive audit requests during the last 15 seconds. | Check the position itself. If the position is OK, check data connectivity between the switch and position. |
| Unsupported BCS level | The difference between the switch and position software release levels exceeds the maximum supported difference. | Upgrade either the position software load or the switch software load. |
| <text from table MTCFAIL> | The position sent an unsolicited out-of-service notification message to the switch. This message included an error code which is datafilled in switch table MTCFAIL. The reason text is from table MTCFAIL. (The second example in Figure 254 illustrates this.) | Actions are specific to the error code sent by the position. Check the position itself, including any position logs. Refer to *TOPS IWS Base Platform User's Guide* for an explanation of the error codes the IWS can send with an out-of-service notification. |

**Table 150 TOPS502 reason text descriptions (transition to SYSB) and actions**

| Reason text | Description | Action |
|---|---|---|
| Unsolicited OOS notify received (EC <n>)<br><br>where <n> is a number with up to 3 digits | The position sent an unsolicited out-of-service notification to the switch, and the message did not include an error code that is datafilled in switch table MTCFAIL. (The third example in Figure 254 illustrates this.)<br><br>***Note1:*** Error code 0 is reserved and indicates that the position reported it was not troubled.<br><br>***Note2:*** When a positions sends an unsolicited out-of-service notification, it indicates whether it is troubled or not. If the position is datafilled in table TOPSPOS with field URESOK=Y, and the position indicates it is not troubled, then the position transitions to URES rather than SYSB, and no TOPS502 log is generated. | Same as above. |
| CM-position state mismatch | An in-service request message was received from a position that was already marked in-service at the switch. This typically results from message loss. The switch makes the position SYSB to straighten out the mismatch. Normally the position will be automatically returned to service again within less than a minute. | No action is required. |
| CM-position datafill mismatch | Position datafill does not agree with switch or DHCP server datafill on one or more of the following: position number, position data type in table TOPSPOS, SX05DA IP address, or SX05DA port.<br><br>This reason can also appear if two positions are datafilled to use the same position number. | If logs with this reason text are accompanied by TOPS137 logs with trouble text "Unexpected message source," it is likely that two positions are datafilled with the same position number. Find the positions and check the position number datafill in each.<br><br>Otherwise, check position datafill against switch tables TOPSPOS, IPCOMID, and IPSVCS, and against either table XPMIPMAP (if CM method is used to assign SX05 IP addresses) or DHCP server (if DHCP method is used). |
| Misc failure, check swers | An unexpected condition has occurred. | Collect swers and any other logs, and contact Nortel Networks support. |

Table 151 describes the reason texts for transitions *from* SYSB.

**Table 151 TOPS502 reason text descriptions (transition from SYSB) and actions**

| Reason text | Description | Action |
|---|---|---|
| System corrected trouble | System action removed the position from the SYSB state. | No action is required. |
| Manual action | The position was manually busied at the MAP. | No specific action is required. |

### Action

Refer to Table 150, "TOPS502 reason text descriptions (transition to SYSB) and actions," on page 472.

### Associated OM registers

None.

## TOPS504

This log is generated when an OC-IP data link transitions to another state. The log report displays the following information:

- data link
- reason text (manual command, system detected trouble, system corrected trouble, datafill change)
- from state and to state

The following figure shows an example log report.

**Figure 255 Example log report for TOPS504**

```
TOPS504 JUN23 18:12:05 5050 INFO TOPS IP DataLink Fault
Data Link: OCIPDL DAHOST 1
Reason:    Manual Command
From:      MANB
To:        INSV
```

### Action

None; this log is for information only.

### Associated OM registers

None.

## TOPS505

The TOPS505 log was introduced in TOPS15 to report IP position state changes. However, it has been obsoleted by several other logs that are documented in this section, and it is never generated.

## TOPS614

This log is generated when the switch receives an OC-IP data link message from an address that does not match the far-end address datafilled against the link. The mismatch may be in the IP address, the port, or both.

For real-time protection from babbling nodes, the generation of this log is throttled. For each data link that has received a message from a faulty IP address or port, this log is generated approximately once every 30 seconds. The following figure shows an example log report.

**Figure 256 Example log report for TOPS614**

```
TOPS614 JUN23 18:12:05 5050 INFO TOPS Msg IP Addr Mismatch
Source ID =     DAHOST 1
Expected Addr =  47.192.  5.216
Msg Addr =       47.103. 23. 95
```

### Action

If the IP address in the Msg Addr field does not match the IP address in the Expected Addr field, determine whether the correct datafill for the data link is present in the switch. See “Parallel datafill for OC-IP data links” on page 91 for details. If the datafill is correct, investigate the source of the faulty IP address. If the IP addresses are the same, then the port numbers do not match. This is likely due to inconsistent datafill

### Associated OM registers

None.

## TOPS615

This information log is generated to indicate the operator team number and number of positions in each team with auto-compression turned on. The IP position sends an auto-compression message to TOPS to indicate the position has voice auto-compression turned on. When the position exits the auto-compression mode, a message is sent indicating that auto-compression is off.

The log is generated if an auto-compression message has arrived during an approximate 5 minute audit period. It is also generated if an IP position with auto-compression turned on goes through a service affecting state change (i.e. bsy). Once auto-compression has been turned off for all positions, the log indicates no operator teams or positions have auto-compression on.

**Figure 257 Example log report for TOPS615 with auto-compression off**

```
TOPS615 mmmdd hh:mm:ss ssdd INFO IP Position Auto Compression
Operator teams reporting auto-compression in use:
               Team Number        Number of Positions
               -----------        -------------------
                   N/A                    0
```

**Figure 258 Example log report for TOPS615 with auto-compression on**

```
TOPS615 mmmdd hh:mm:ss ssdd INFO IP Position Auto Compression
Operator teams reporting auto-compression in use:
               Team Number        Number of Positions
               -----------        -------------------
                   1                      5
                   6                    975
                  30                      1
```

## Action

No user action is required.

## Associated OM registers

None.

# Chapter 13: TOPS-IP OMs

This chapter provides information on operational measurements (OM) for TOPS-IP. For each OM group there is a brief description, a list of registers, an OMSHOW example, and a list of any associated OM groups and logs. Table 152 lists each OM group associated with TOPS-IP and the page in this chapter where its description begins.

**Table 152 TOPS-IP OMs**

| OM group | Page number |
|---|---|
| QMSMIS | 478 |
| TOPSOC | 480 |
| TOPSVC | 481 |
| XIPCOMID | 482 |
| XIPDCOM | 484 |
| XIPMISC | 486 |
| XIPSVCS | 488 |
| XPMMSGOC | 490 |

***Note:*** For complete information on all OMs for the DMS switch, refer to *Operational Measurements Reference Manual*.

## QMSMIS

OM group QMSMIS (Queue Management System Management Information System) provides peg counts on events and call queue messages generated by the QMS MIS application (TOPS and OSSAIN). Sixteen registers apply to sending buffers across the four IP connections to the external reporting facility (MIS server).

***Note:*** The other nine registers apply to messages for positions, OSSAIN session pools, queues, and MPC buffers. OSSAIN does not use the 16 TOPS-IP registers.

The following table describes these registers.

**Table 153 OM group QMSMIS**

| Register | Description |
|---|---|
| BUFIP1SX | Buffer IP 1 success. This register is pegged each time a buffer is successfully sent across the first IP connection. |
| BUFIP1S2 | Buffer IP 1 success extension register |
| BUFIP2SX | Buffer IP 2 success. This register is pegged each time a buffer is successfully sent across the second IP connection. |
| BUFIP2S2 | Buffer IP 2 success extension register |
| BUFIP3SX | Buffer IP 3 success. This register is pegged each time a buffer is successfully sent across the third IP connection. |
| BUFIP3S2 | Buffer IP 3 success extension register |
| BUFIP4SX | Buffer IP 4 success. This register is pegged each time a buffer is successfully sent across the fourth IP connection. |
| BUFIP4S2 | Buffer IP 4 success extension register |
| BUFIP1TL | Buffer IP 1 total. This register is pegged each time a buffer is attempted to be sent across the first IP connection. |
| BUFIP1T2 | Buffer IP 1 total extension register |
| BUFIP2TL | Buffer IP 2 total. This register is pegged each time a buffer is attempted to be sent across the second IP connection. |
| BUFIP2T2 | Buffer IP 2 total extension register |
| BUFIP3TL | Buffer IP 3 total. This register is pegged each time a buffer is attempted to be sent across the third IP connection. |
| BUFIP3T2 | Buffer IP 3 total extension register |
| BUFIP4TL | Buffer IP 4 total. This register is pegged each time a buffer is attempted to be sent across the fourth IP connection. |
| BUFIP4T2 | Buffer IP 4 total extension register |

The following figure shows an example for OM group QMSMIS.

**Figure 259 MAP display example for OM group QMSMIS**

```
CLASS:   ACTIVE
START:2000/11/02 09:30:00 TUE; STOP: 2000/11/02 09:37:02 TUE;
SLOWSAMPLES:         5 ; FASTSAMPLES:         42 ;

       INFO (QMS_MIS_APPLN_INDEX_REGISTERINFO)
           POSMSG    POSMSG2    SESNMSG   SESNMSG2
           QUEMSG    QUEMSG2     BUFFSX    BUFFSX2
          BUFFAIL   BUFIP1SX   BUFIP1S2   BUFIP2SX
        BUFIP2S2   BUFIP3SX   BUFIP3S2   BUFIP4SX
        BUFIP4S2   BUFIP1TL   BUFIP1T2   BUFIP2TL
        BUFIP2T2   BUFIP3TL   BUFIP3T2   BUFIP4TL
        BUFIP4T2

    1 TOPS
               15          0          0          0
                0          0          0          0
                0          5          0          3
                0          0          0          0
                0          5          0          5
                0          0          0          0
                0
```

## Associated OM groups

None.

## Associated logs

None.

# TOPSOC

OM group TOPSOC (TOPS Operator Centralization) provides peg counts on OC call originations and abandons. This group is pegged in the host against the remote. The TOPSOC OM group provides a tuple for every remote switch datafilled in table OCGRP.

The following table describes each register.

**Table 154 OM group TOPSOC**

| Register | Description |
|---|---|
| OCINI | OC initiation. This register is pegged each time a call that requires a TOPS operator is routed to an OC host switch from an OC remote switch. |
| OCQABN | OC queue abandons. This register is pegged each time a call that originates at an OC remote switch and queues at an OC host switch is abandoned before being served by a TOPS operator. |

The following figure shows an example for OM group TOPSOC.

**Figure 260 MAP display example for OM group TOPSOC**

```
CLASS:   ACTIVE
START:2000/11/02 09:30:00 TUE; STOP: 2000/11/02 09:37:02 TUE;
SLOWSAMPLES:         5 ; FASTSAMPLES:         42 ;

       INFO (TOPS_OCINDEX_REGISTERINFO)
            OCINI         OCQABN

    3     REMOTE1
                0            0
    4     REMOTE2
                0            0
```

## Associated OM groups

TOPSOC is associated with the TOPQOCPS OM group.

## Associated logs

None.

## TOPSVC

OM group TOPSVC (TOPS Virtual Circuit) provides peg counts on events related to OC virtual circuits, which are used for OC data link messaging. This group is pegged in the host and in the remote against the far-end switch. The TOPSVC OM group provides a tuple for every switch datafilled in table OCOFC.

***Note:*** Events related to OC voice links are not tracked by this OM group.

The following table describes each register.

**Table 155 OM group TOPSVC**

| Register | Description |
|---|---|
| VCATT | Virtual circuit attempts. This register is pegged each time the switch attempts to obtain a virtual circuit. |
| VCFL | Virtual circuit failure. This register is pegged each time a virtual circuit fails to send a message. |
| VCNMSG | Virtual circuit number message. This register is pegged each time a virtual circuit sends a message. |
| VCNMSG2 | Virtual circuit message extension register |
| VCDEF | Virtual circuit deflection. This register is pegged each time an attempt to obtain a virtual circuit is deflected due to none available. |
| MSGLOST | Message lost. This register is pegged each time an expected OC message is not received by the remote or host during an OC call. |
| OPRLOST | Operator lost. This register is pegged each time a call is terminated in the remote or the host as a result of an expected OC data link message not being received. |

The following figure shows an example for OM group TOPSVC.

**Figure 261 MAP display example for OM group TOPSVC**

```
CLASS:   ACTIVE
START:2000/11/02 09:30:00 TUE; STOP: 2000/11/02 09:37:02 TUE;
SLOWSAMPLES:         5 ; FASTSAMPLES:         42 ;

       INFO (TOPS_OCINDEX_REGISTERINFO)
            VCATT       VCFL     VCNMSG    VCNMSG2
            VCDEF    MSGLOST    OPRLOST

    1        HOME
                0          0          0          0
                0          0          0
    2       REMOTE1
                0          0          0          0
                0          0          0
    3      REMOTE2
                0          0          0          0
                0          0          0
    4       DAHOST
                0          0          0          0
                0          0          0
```

### Associated OM groups

None.

### Associated logs

TOPSVC is associated with the following logs:

- TOPS102
- TOPS105
- TOPS106
- TOPS107

## XIPCOMID

OM group XIPCOMID (XPM IP Communication Identifier) provides peg counts for exchanges of UDP and TCP messages based on a particular COMID. The COMID associates a switch IP service name with an XPM used for data communication. The XIPCOMID OM group provides a tuple for each COMID datafilled in table IPCOMID.

The following table describes each register.

**Table 156 OM group XIPCOMID**

| Register | Description |
|---|---|
| UMSSN | UDP message send. This register is pegged when the CM sends a UDP message for a particular COMID to the XPM for transmission to the IP network. |
| UMSSN2 | UDP message send extension register |
| UMSSNF | UDP message send failure. This register is pegged when a failure occurs during the sending of a UDP message for a particular COMID from the CM to the XPM for transmission to the IP network. |
| UMSRC | UDP message receive. This register is pegged when the CM receives a UDP message that originated from the IP network for a particular COMID from the XPM. |
| UMSRC2 | UDP message receive extension register |
| UMSRCF | UDP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular COMID from the XPM to the CM.<br>***Note:*** If the message is severely corrupted, this register may not be pegged. |
| TMSSND | TCP message send. This register is pegged when the CM sends a TCP message for a particular COMID to the XPM for transmission to the IP network. |
| TMSSND2 | TCP message send extension register |
| TMSSNF | TCP message send failure. This register is pegged when a failure occurs during the sending of a TCP message for a particular COMID from the CM to the XPM for transmission to the IP network. |
| TMSRC | TCP message receive. This register is pegged when the CM receives a TCP message that originated from the IP network for a particular COMID from the XPM. |
| TMSRC2 | TCP message receive extension register |
| TMSRCF | TCP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular COMID from the XPM to the CM.<br>***Note:*** If the message is severely corrupted, this register may not be pegged. |

The following figure shows an example for OM group XIPCOMID.

**Figure 262 MAP display example for OM group XIPCOMID**

```
CLASS:   ACTIVE
START:2000/11/02 09:00:00 TUE; STOP: 2000/11/02 09:28:01 TUE;
SLOWSAMPLES:        17 ; FASTSAMPLES:        168 ;

       KEY (IP_COMID_RANGE)
            UMSSN     UMSSN2     UMSSNF      UMSRC
           UMSRC2     UMSRCF     TMSSND    TMSSND2
           TMSSNF      TMSRC     TMSRC2     TMSRCF

   30
                0          0          0          0
                0          0          0          0
                0          0          0          0

   40
                0          0          0          0
                0          0          0          0
                0          0          0          0
```

### Associated OM groups

XIPCOMID is associated with the following OM groups:

- XIPDCOM
- XIPMISC
- XIPSVCS

### Associated logs

XIPCOMID is associated with the XIP600 log.

## XIPDCOM

OM group XIPDCOM (XPM IP Data Communications) provides peg counts for exchanges of UDP, TCP, and ICMP messages. The XIPDCOM OM group provides a single tuple for all peg counts.

The following table describes each register.

**Table 157 OM group XIPDCOM**

| Register | Description |
|---|---|
| UMSGSN | UDP message send. This register is pegged when the CM sends a UDP message to the XPM for transmission to the IP network. |
| UMSGSN2 | UDP message send extension register |

**Table 157 OM group XIPDCOM**

| Register | Description |
|---|---|
| UMSGSNF | UDP message send failure. This register is pegged when a failure occurs during the sending of a UDP message from the CM to the XPM for transmission to the IP network. |
| UMSGRC | UDP message receive. This register is pegged when the CM receives a UDP message that originated from the IP network from the XPM. |
| UMSGRC2 | UDP message receive extension register |
| UMSGRCF | UDP message receive failure. This register is pegged when a failure occurs during the receiving of a UDP message from the XPM to the CM.<br>***Note:*** If the message is severely corrupted, this register may not be pegged. |
| TMSGSN | TCP message send. This register is pegged when the CM sends a TCP message to the XPM for transmission to the IP network. |
| TMSGSN2 | TCP message send extension register |
| TMSGSNF | TCP message send failure. This register is pegged when a failure occurs during the sending of a TCP message from the CM to the XPM for transmission to the IP network. |
| TMSGRC | TCP message receive. This register is pegged when the CM receives a TCP message that originated from the IP network from the XPM. |
| TMSGRC2 | TCP message receive extension register |
| TMSGRCF | TCP message receive failure.This register is pegged when a failure occurs during the receiving of a TCP message from the XPM to the CM.<br>***Note:*** If the message is severely corrupted, this register may not be pegged. |
| ICREQS | ICMP request send. This register is pegged when the CM sends an ICMP request to the XPM. |
| ICREQSF | ICMP request send failure. This register is pegged when a failure occurs during the sending of an ICMP request from the CM to the XPM. |
| ICREPRC | ICMP reply receive. This register is pegged when the CM receives an ICMP reply from the XPM. |
| ICREPF | ICMP reply failure. This register is pegged when a failure occurs during the receiving of an ICMP reply from the XPM to the CM. |

The following figure shows an example for OM group XIPDCOM.

**Figure 263 MAP display example for OM group XIPDCOM**

```
CLASS:   ACTIVE
START:2000/11/02 11:30:00 TUE; STOP: 2000/11/02 11:36:05 TUE;
SLOWSAMPLES:         4 ; FASTSAMPLES:         37 ;

           UMSGSN    UMSGSN2    UMSGSNF     UMSGRC
          UMSGRC2    UMSGRCF     TMSGSN    TMSGSN2
          TMSGSNF     TMSGRC    TMSGRC2    TMSGRCF
           ICREQS    ICREQSF    ICREPRC     ICREPF

    0           0          0          0          0
                0          0          0          0
                0          0          0          0
                0          0          0          0
```

### Associated OM groups

XIPDCOM is associated with the following OM groups:

- XIPCOMID
- XIPMISC
- XIPSVCS

### Associated logs

XIPDCOM is associated with the XIP600 log.

## XIPMISC

OM group XIPMISC (XPM IP Miscellaneous) provides peg counts for miscellaneous CM IP data communication functions, including sending and receiving packets. The XIPMISC OM group provides a single tuple for all peg counts.

***Note:*** A UDP, TCP, or ICMP message consists of one or more packets.

The following table describes each register.

**Table 158 OM group XIPMISC**

| Register | Description |
|---|---|
| PKTSN | Packet send. This register is pegged when the CM sends a packet to the XPM. |
| PKTSN2 | Packet send extension register |
| PKTSNER | Packet send error. This register is pegged when an error occurs during the sending of a packet from the CM to the XPM. |
| PKTRC | Packet receive. This register is pegged when the CM receives a packet from the XPM. |

**Table 158 OM group XIPMISC**

| Register | Description |
|---|---|
| PKTRC2 | Packet receive extension register |
| PKTRCER | Packet receive error. This register is pegged when an error occurs during the receiving of a packet from the XPM to the CM. |
| BUFERR | Buffer error. This register is pegged when the CM cannot obtain a buffer to store messages received from the XPM. |

The following figure shows an example for OM group XIPMISC.

**Figure 264 MAP display example for OM group XIPMISC**

```
CLASS:   ACTIVE
START:2000/11/02 14:00:00 TUE; STOP: 2000/11/01 14:28:25 MON;
SLOWSAMPLES:        18 ; FASTSAMPLES:        171 ;

            PKTSN     PKTSN2    PKTSNER      PKTRC
           PKTRC2    PKTRCER     BUFERR

    0           2          0          0          2
                0          0          0
```

## Associated OM groups

XIPMISC is associated with the following OM groups:

- XIPCOMID
- XIPDCOM
- XIPSVCS

## Associated logs

XIPMISC is associated with the XIP600 log.

## XIPSVCS

OM group XIPSVCS (XPM IP Services) provides peg counts for exchanges of UDP and TCP messages based on a particular IP service name. The service associates a particular COMID with a port number and transport protocol. The XIPSVCS OM group provides a tuple for each service datafilled in table IPSVCS.

The following table describes each register.

**Table 159 OM group XIPSVCS**

| Register | Description |
|---|---|
| UMSGSND | UDP message send. This register is pegged when the CM sends a UDP message for a particular service to the XPM for transmission to the IP network. |
| UMSGSND2 | UDP message send extension register |
| UMSGSNDF | UDP message send failure. This register is pegged when a failure occurs during the sending of a UDP message for a particular service from the CM to the XPM for transmission to the IP network. |
| UMSGRCV | UDP message receive. This register is pegged when the CM receives a UDP message that originated from the IP network for a particular service from the XPM. |
| UMSGRCV2 | UDP message receive extension register |
| UMSGRCVF | UDP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular service from the XPM to the CM.<br>***Note:*** If the message is severely corrupted, this register may not be pegged. |
| TMSGSND | TCP message send. This register is pegged when the CM sends a TCP message for a particular service to the XPM for transmission to the IP network. |
| TMSGSND2 | TCP message send extension register |
| TMSGSNDF | TCP message send failure. This register is pegged when a failure occurs during the sending of a TCP message for a particular service from the CM to the XPM for transmission to the IP network. |
| TMSGRCV | TCP message receive. This register is pegged when the CM receives a TCP message that originated from the IP network for a particular service from the XPM. |
| TMSGRCV2 | TCP message receive extension register |

**Table 159 OM group XIPSVCS**

| Register | Description |
|---|---|
| TMSGRCVF | TCP message receive failure. This register is pegged when a failure occurs during the receiving of a TCP message for a particular service from the XPM to the CM.<br><br>***Note:*** If the message is severely corrupted, this register may not be pegged. |

The following figure shows an example for OM group XIPSVCS.

**Figure 265 MAP display example for OM group XIPSVCS**

```
CLASS:   ACTIVE
START:2000/11/02 15:00:00 TUE; STOP: 2000/11/02 15:16:36 TUE;
SLOWSAMPLES:        10 ; FASTSAMPLES:        100 ;

       KEY (IP_SERVICES_RANGE)
          UMSGSND   UMSGSND2   UMSGSNDF    UMSGRCV
         UMSGRCV2   UMSGRCVF    TMSGSND   TMSGSND2
         TMSGSNDF    TMSGRCV   TMSGRCV2   TMSGRCVF

    REMOTE1_IPSVC
                0          0          0          0
                0          0          1          0
                0          0          0          0

    DAHOST_IPSVC
                0          0          0          0
                0          0          0          0
                0          0          0          0

    XIPVER
                0          0          0          0
                0          0          0          0
                0          0          0          0
```

## Associated OM groups

XIPSVCS is associated with the following OM groups:

- XIPCOMID
- XIPDCOM
- XIPMISC

## Associated logs

XIPSVCS is associated with the XIP600 log.

## XPMMSGOC

OM group XPMMSGOC (XPM Messaging Occupancy) provides peg counts that can be helpful in monitoring the messaging load on XPMs. When messaging overload occurs, performance is degraded, messages can be lost, and problems can occur during SWACTs.

The XPMMSGOC OM group provides five tuples for each supported XPM. Each tuple corresponds to a different messaging interface. Each messaging interface has a holding queue in which outgoing messages (from the XPM) are held for later delivery if the interface is busy when the XPM first attempts to send the message. Some use of the holding queues is expected on most of the interfaces. However, a high percentage of messages being placed in any holding queue is a warning sign of messaging overload.

The holding queue registers of OM group XPMMSGOC use the concept of "message load factor." For an XPM interface, the message load factor is the percentage of all the messages sent on the interface that had to be placed in the holding queue. The XPM computes the message load factor for each interface every 10 seconds. The actual holding queue registers count the number of 10-second intervals, during the reporting period, in which the message load factor was in various ranges.

***Note:*** Table OFCVAR parameter XPMMSGOC_OM_CONTROL must be set to Y (Yes) for pegging of OM group XPMMSGOC to occur.

The following table describes each register.

**Table 160 OM group XPMMSGOC**

| Register | Description |
|---|---|
| HQ00 | Holding queue 0%. This register is pegged when the message load factor computed is 0%. |
| HQ05 | Holding queue 5%. This register is pegged when the message load factor computed is greater than 0% and less than or equal to 5%. |
| HQ10 | Holding queue 10%. This register is pegged when the message load factor computed is greater than 5% and less than or equal to 10%. |
| HQ20 | Holding queue 20%. This register is pegged when the message load factor computed is greater than 10% and less than or equal to 20%. |
| HQ30 | Holding queue 30%. This register is pegged when the message load factor computed is greater than 20% and less than or equal to 30%. |
| HQ40 | Holding queue above 40%. This register is pegged when the message load factor computed is greater than 30% and less than or equal to 40%. |

**Table 160 OM group XPMMSGOC**

| Register | Description |
|---|---|
| HQABV40 | Holding queue above 40%. This register is pegged when the message load factor computed is greater than 40%. |
| AVGRATE | Average rate. This register records the average message rate in messages per second. |
| MAXRATE | Maximum rate. This register records the maximum transfer rate in messages per second. |
| NUMREPTS | Number of reports. This count is generally 1. |

The following figure shows an example for OM group XPMMSGOC.

**Figure 266 MAP display example for OM group XPMMSGOC**

```
CLASS:   ACTIVE
START:2000/11/02 15:00:00 TUE; STOP: 2000/11/02 15:16:36 TUE;
SLOWSAMPLES:        10 ; FASTSAMPLES:        100 ;

       INFO (XPMMSGOC_OM_KEY)
            HQ00       HQ05       HQ10       HQ20
            HQ30       HQ40    HQABV40    AVGRATE
         MAXRATE   NUMREPTS

   30        DTC      5 NET
               0          0          0          0
               0          0          0          0
               0          1

   31        DTC      5 NETY
               0          0          0          0
               0          0          0          0
               0          1

   32        DTC      5 IMC
               0          0          0          0
               0          0          0          0
               0          1

   33        DTC      5 SPCHBUS
               0          0          0          0
               0          0          0          0
               0          1

   34        DTC      5 HDLC
               0          0          0          0
               0          0          0          0
               0          1
```

### Monitoring the IP-XPM

The interfaces that are most useful to monitor are SPCHBUS and, especially on a BRISC switch, NET. The SPCHBUS interface is used for inter-mate communication, and if it is overloaded, there may be problems with XPM SWACTs. The NET interface refers to the two C-side DMSIO links. On a BRISC switch these links are often the first bottleneck in a heavily-loaded IP-XPM. (On XA-Core, Destination Protection algorithms in the core smooth out the rate at which messages are sent to XPMs, but BRISC switches do not have this functionality. On XA-Core the SPCHBUS interface is often the first bottleneck.)

No hard rules are available for interpreting the data provided by this OM group, but changes in its characteristic patterns are of interest, and the following rules of thumb may be useful:

- Any number of pegs in the HQABV40 register indicates a messaging capacity problem.
- Pegs in the HQ40 register are of concern, and pegs in HQ30 suggest that the XPM is approaching the capacity limit of the interface.
- In general, the more pegs there are in the lowest HQ registers, the more extra capacity the XPM has for the interface.

### Associated OM groups

None.

### Associated logs

None.

# Appendixes

The following appendixes are included in *TOPS-IP User's Guide*:

# Appendix A: DHCP server guidelines

The Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses to devices on a network. DHCP is based on the Bootstrap Protocol (BOOTP). (For details on DHCP refer to RFC2131.)

Nortel Networks NetID (NetID) software provides the DHCP server function in the TOPS-IP network. The DHCP server is used to configure the 7X07AA Gateway cards and (optionally) the SX05DA processor cards in the IP-XPM. DHCP provides the following configuration information:

- IP addresses of the Gateway cards (voice)
- IP addresses of the SX05 processor (data)
- IP addresses of the default routers

***Note:*** The FTP function provides the Gateway card with its software load from the DHCP server.

This appendix describes how to install and configure the DHCP servers (primary and backup), focusing on the following areas:

- preparation
- installation
- configuration

***Note:*** The procedures in this appendix provide general guidelines for setting up and using NetID software. Data values shown in the sample configuration reflect *examples only.* Your TOPS-IP network configuration is unique and requires site-specific data values. Before performing any procedures, contact your network engineering group for information on the configuration and IP addressing scheme used for your network, and for details on how these procedures need to be adapted at your site.

This appendix also provides procedures for managing logs on the NetID server, procedures for stopping and restarting NetID services, and notes about remedies for certain Microsoft Windows anomalies that may be encountered during installation and configuration.

Finally, this appendix provides information on upgrading the Gateway load (page 527) and changing the configuration of the Gateway (page 530).

## DHCP server requirements

Two DHCP servers must be provisioned in the TOPS-IP network. The first server is the primary one; the second is for backup.

### DHCP server hardware

The following hardware is required:

#### Minimum System Requirements with NetID 4.3.2 and NetID 4.3.3:

- Intel Pentium-family processor running 600 Mhz or faster
- 256 MB RAM
- Minimum 6 GB Hard Drive space available for OS, NetID, Oracle and 7X07 load(s)
- CD-ROM drive
- 10/100 Ethernet NIC with RJ45 connector
- Monitor with VGA or higher resolution
- Keyboard and mouse

***Note:*** This configuration assumes that the NetID Network Server is dedicated for use with TOPS-IP IP-XPMs.

#### Recommended System Requirements with NetID 4.3.2:

- Intel Pentium-family processor running at 733 MHz or faster
- 512 MB RAM
- Minimum 6 GB hard disk space available for OS, NetID, Oracle, and 7X07 load(s)
- CD-ROM Drive
- 10/100 Ethernet NIC with RJ45 connector
- Monitor with SVGA or higher resolution
- Keyboard and mouse

#### Recommended System Requirements with NetID 4.3.3 and 4.5:

- Intel Pentium-family processor running at 1.0 GHz or faster
- 512 MB RAM
- 20 GB hard disk space available for OS, NetID, Oracle, and 7X07 load(s)
- CD-ROM Drive
- 10/100 Ethernet NIC with RJ45 connector
- Monitor with SVGA or higher resolution
- Keyboard and mouse

## DHCP server software

The following software is required:

- One of the following operating systems:
  - — Microsoft Windows 2000 Server, Latest Service Pack
  - — Microsoft Windows 2000 Professional, Latest Service Pack
  - — NetID 4.3.3 and 4.5 is also supported on Windows 2003 Server.
- Oracle 9.2 Runtime Database for Windows is required for NetID 4.3.3

  ***Note:*** Oracle 8i (8.1.7) and Oracle 9i are supported clients for NetID 4.3.2. Oracle can be bundled with the NetID product. See "NetID ordering" below.
- Oracle 10.1.0.2 Runtime Database for Windows is required for NetID 4.5
- Nortel Networks NetID product (version 4.3.2 or version 4.3.3 or version 4.5)

  ***Note:*** The NetID CD-ROM contains the NetID product suite, the NetID user documents, and the Adobe Acrobat Reader software used to read the documents.
- Java 1.4.2 -compliant Web browser

  ***Note:*** As of the latest Windows 2000 Service Pack, Microsoft no longer distributes or supports the Microsoft Virtual Machine (VM) as part of the Microsoft Internet Explorer package. NetID 4.3.3 requires the SUN Java Runtime Environment (JRE). If you are running the NetID management console through Microsoft Internet Explorer, you must ensure that the SUN JRE (version 1.4.2 or later) is installed and enabled on the same system and that Microsoft Virtual Machine (VM) is disabled. JRE is available for free download at http://java.com. For enabling instructions, please refer to Step 5 on page 513. The JRE is also included on the NetID installation CD.

### NetID ordering

The versions of NetID and their features include:

- **DH0008039: NetID 1500**
  - — Supports IP addressing for up to 1500 IP nodes in the network. This is not expandable.
  - — Includes an Oracle Runtime database licensed for 5 concurrent database users. This is not expandable.
- **DH0008037: NetID (unlimited)**
  - — Supports IP addressing for up to 2,500 IP nodes in the network. This is expandable in units of 2,500, 5,000, and 25,000.

— Includes an Oracle Runtime database licensed for 5 concurrent database users. Additional concurrent database licenses can be purchased.

### Gateway software

The 7X07AA Gateway cards require the TGWY0004 NCL software load. The Gateway CD-ROM contains the executable loadfile and the Gateway-related Management Information Base (MIB) files used by the network administrator. For details on these MIBs, refer to Appendix B: "TOPS-IP support for SNMP."

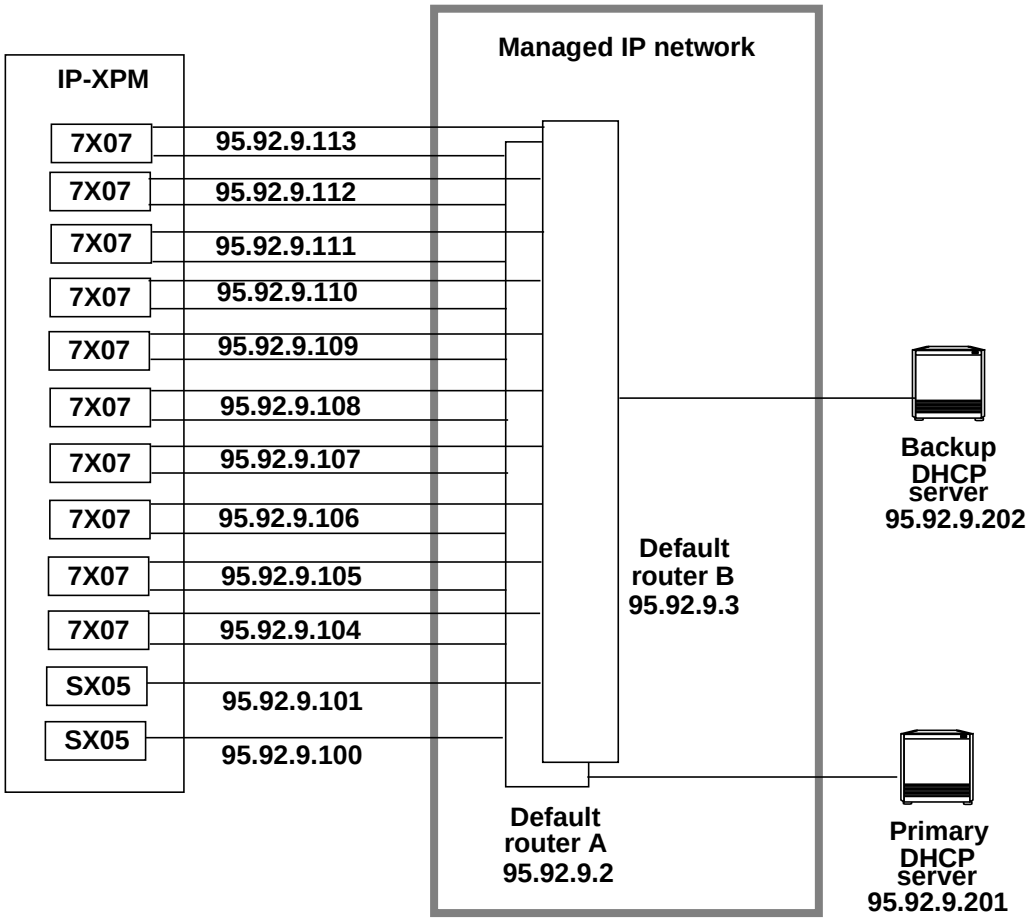
## Preparation

Before installing the DHCP servers for TOPS-IP, it is recommended that you collect and diagram your site-specific IP addressing information. Figure 267 shows an *example* configuration that illustrates IP addresses for ten 7X07 Gateway cards (see Note 2), two SX05 cards, two default routers, and the primary and backup DHCP servers. In this example subnetwork, all components are in the same subnet: 95.92.9.0.

***Note 1:*** The site-specific diagram of your TOPS-IP network will consist of several subnetworks.

***Note 2:*** Chapter 7: "TOPS-IP engineering guidelines" contains important information on how many 7X07 Gateway cards to provision in an IP-XPM.

**Figure 267 Example IP addresses for one subnet**




***Note:*** In this example, IP addresses 95.92.9.102 and 95.92.9.103 are reserved for unit 0 and unit 1 of the SX05 to complete the block of four IP addresses. Not shown in the figure is the virtual router IP address 95.92.9.1.

## Provisioning information worksheets

Users can capture provisioning data on the worksheets that follow. These values will be used in the installation and configuration procedures discussed later in the chapter. All worksheets require *site-specific* values for each subnetwork in your TOPS-IP network.

### Network provisioning worksheet

Use the following worksheet to record network provisioning information. Example values are shown in column 2. (Make copies of the worksheet for each subnetwork.)

**Table 161 Network provisioning information worksheet**

| System variable | Example value | Your value |
|---|---|---|
| Windows 2000 user ID | Administrator | |
| Windows 2000 password | topsip1 | |
| Windows 2000 domain | topsip | |
| Company domain name | nortelnetworks.com | |
| TOPS-IP subnetwork IP address (see Note 1) | 95.92.9.0 | |
| Subnet mask | 255.255.255.0 | |
| Default domain | topsip | |
| Primary DHCP server IP address | 95.92.9.201 | |
| Primary DHCP server name | topsipserver1 | |
| Backup DHCP server IP address | 95.92.9.202 | |
| Backup DHCP server name | topsipserver2 | |
| NetID user ID | admin | |
| NetID password | NETID | |
| NetID Application Server port number | 8080 | |
| NetID Server Manager IP address | 95.92.9.201 | |
| NetID Server Manager port number | <use default value> | |
| NetID Alternate Server Manager IP address | <use default value> | |
| NetID Alternate Server Manager port number | <use default value> | |
| SNMP trap destination IP address | 95.92.9.203 | |
| SNMP trap community | public | public |
| Physical router 1 IP address (see Note 2) | 95.92.9.2 | |
| Physical router 2 IP address (see Note 2) | 95.92.9.3 | |
| Virtual router 1 IP address (see Note 2) | 95.92.9.1 | |
| Virtual router 2 IP address (see Note 2) | 95.92.9.1 | |
| Gateway loadfile directory | C:\Gateway | |
| Gateway loadfile (boot file) name | topsipgw40ae | |
| Gateway load user access password | tazmanian | tazmanian (see Note 3) |
| ***Note 1:*** This IP address will be unique for each subnetwork.<br>***Note 2:*** This exact password is required by the TOPS-IP 7X07 Gateway card. | | |

## IP-XPM provisioning worksheet

Use the following worksheet to record IP-XPM (DTC) provisioning information. (Make copies of the worksheet for additional IP-XPMs.)

Examples of IP addresses for the SX05s, the Gateways, and the default routers are shown in Figure 267 on page 499. The following list provides guidelines on the other values to record:

- An example of a NetID host name for an SX05 card is “dtc10sx0.” Likewise, an example host name for a Gateway card is “dtc10gw4.” These values are examples only.
- IP addressing of the two SX05 cards requires a *block of four* consecutive IP addresses. The last octet of the active address must be divisible by four, for example, 95.92.9.100. The inactive address is assigned N+1, and unit 0 and unit 1 are reserved to complete the block.
- An example of a MAC address is “00:3d:44:01:2a:40.” Each 7X07 Gateway card has two MAC addresses printed on it. The numerically lower of the two is used by the DHCP server.

**Table 162 IP-XPM provisioning information worksheet**

| Component | NetID host name | IP address | MAC address | Primary default router IP address | Secondary default router IP address |
|---|---|---|---|---|---|
| SX05 active | | | Reserved | | |
| SX05 inactive | | | Reserved | | |
| SX05 unit 0 | | | | | |
| SX05 unit 1 | | | | | |
| Gateway 0 | | | | | |
| Gateway 1 | | | | | |
| Gateway 2 | | | | | |
| Gateway 3 | | | | | |
| Gateway 4 | | | | | |
| Gateway 5 | | | | | |
| Gateway 6 | | | | | |
| Gateway 7 | | | | | |
| Gateway 8 | | | | | |
| Gateway 9 | | | | | |

## DHCP options worksheets

NetID software needs DHCP options to configure the 7X07 Gateway cards and the SX05 cards. With NetID, each card is configured as a “host” with specific DHCP parameter values.

Use the following worksheets to record site-specific DHCP options. The parameter names appear under various sub-trees of the “Standard” tree. Sub-tree names (for example, “Application and Service Parameters”) are indicated in italics. Example values are shown in column 2.

***Note:*** Details on how to locate the parameters in NetID are in the section “Configuration” on page 515.

**Table 163 DHCP options for Gateway cards**

| Parameter | Example value | Your value |
|---|---|---|
| *Application and Service Parameters:* | | |
| Boot File | topsipgw40ae | |
| MobileIP Home Agents (see Note 1) | 95.92.9.203 | |
| *NetID Managed:* | | |
| DNS Domain | nortelnetworks.com | |
| HostIP Address (BootP only) | 95.92.9.104 | |
| Host Name | dtc10gw4 | |
| Lease Time | 67108864 | |
| *RFC2132:* | | |
| Routers (see Note 2) | 95.92.9.1 | |
| ***Note 1:*** The MobileIP Home Agents parameter stores the IP address of the default SNMP management node.<br>***Note 2:*** The Gateway cards must use the virtual router IP address (or addresses). | | |

**Table 164 DHCP options for SX05 cards**

| Parameter | Example value | Your value |
|---|---|---|
| *Application and Service Parameters:* | | |
| Mobile IP Home Agents | 95.92.9.203 | |
| *NetID Managed:* | | |
| DNS Domain | nortelnetworks.com | |
| Host IP Address (BootP only) | 95.92.9.100 | |
| Host Name | dtc10sx1 | |
| Lease Time | 67108864 | |
| *RFC2132:* | | |
| Routers (see Note) | 95.92.9.2, 95.92.9.3 | |
| ***Note:*** The SX05 cards must use the physical router IP addresses. | | |

## Procedures in this appendix

Table 165 lists the procedures needed to install and configure NetID as a DHCP server for TOPS-IP. It also includes procedures for managing NetID logs, stopping and restarting NetID services, and upgrading the Gateway load.

**Table 165 DHCP server procedures**

| Procedure | Name | Page |
|---|---|---|
| 1 | Install Windows 2000 Professional | 504 |
| 2 | Install Oracle database | 506 |
| 3 | Install Adobe Acrobat Reader | 508 |
| 5 | Create an Oracle table space and user ID | 509 |
| 6 | Install the NetID product | 510 |
| 7 | Set a permanent NetID administrator | 512 |
| 8 | Set up Gateway load user access | 513 |
| 9 | Configure NetID | 516 |
| 10 | Prevent Windows 2000 “Log table full” warnings | 522 |
| 11 | Trim NetID logs | 523 |
| 12 | Truncate NetID logs | 524 |
| 13 | Stop NetID services | 525 |
| 14 | Restart NetID services | 526 |
| 15 | Upgrade the Gateway load | 528 |

***Note:*** Users of these procedures must have a basic knowledge of PCs and the Microsoft Windows operating system. Before beginning these procedures, follow the standard instructions to set up the PC hardware, and ensure that the PC is connected to the Ethernet LAN. Also before performing any steps, *read each procedure at least once* to prepare and to obtain the required information.

## Installation

This section provides procedures to install NetID as a DHCP server for TOPS-IP.

***Note:*** Follow all the installation procedures to set up the primary DHCP server first, then follow them again to set up the backup DHCP server. Any variations in setting up the backup server are noted where applicable.

### Procedure 1 Install Windows 2000 Professional

Installation media and methods used when installing Microsoft products vary from release to release. These steps reflect one way to install Windows 2000 Professional. Your steps may vary depending upon your software release.

Installing Windows 2000 Professional consists of the following broad steps:

- Delete the existing partitions on the hard disk, and create a new partition on which to install Windows 2000 Professional.
- Install the Windows 2000 Professional software.
- Enable File Transfer Protocol (FTP) Service

***At the PC***

**1** Boot the PC from the Compact Disk and enter Product Key (if required) as instructed.

**2** Delete the existing partition (or partitions) on the PC and install a fresh copy of Windows using the following steps:

**a** Read the instructions on the text screens and press Enter to continue through all the screens.

**b** Use the page down key to scroll through the Windows licensing agreement and press F8 to continue.

*The system displays a list of all hard disks and partitions.*

**c** If no previous version of Windows exists on the PC, press Enter and continue to step h.

**d** If a previous version does exist, select D to delete the existing partition.

**e** Use the arrow keys to select the partition to delete.

**f** Press D to delete the selected partition.

**g** Press Enter and L to continue with the deletion.

**h** Press Enter to install Windows on the selected new (unformatted) partition.

**i** Select the NTFS file system type and press Enter.

**j** The system formats the new partition. This may take a few minutes.

**k** The PC restarts and starts the Windows Setup Wizard

**l** The Setup Wizard installs the detected devices. This may take a few minutes.

**3** Setup Windows 2000 Professional using the following steps:

**a** Enter Regional Settings (language and keyboard type).

**b** Click next.

**c** Enter the name and organization.

**d** Click next.

**e** Enter the unique computer name.

**f** Enter the administrator password.

**g** Click next.

**h** If needed enter the correct Date, Time and Time Zone.

*The Server setup continues and installs the network components.*

**i** Click next.

**j** When prompted for Network Settings, select Custom.

**k** Click next.

**l** Select Internet Protocol (TCP/IP).

**m** Click Properties.

**n** Select *Use the following IP address* and enter the IP address, network mask and default gateway supplied by your network administrator.

***Note:*** **The IP address is used in procedure 4 step 6, procedure 6 step 4 o and procedure 9 step 6 c.**

**o** Click OK, then next.

**p** At the Workgroup or Computer Domain Window:

If you are configuring for a Workgroup, select NO and enter the Workgroup name. If you are configuring for a Domain, enter the Domain name, user id and password supplied by your network administrator.

*Installing network components will take several minutes.*

**q** Remove the CD and click finish to restart.

*The Network Identification Wizard appears.*

**r** Click next

**s** Select “Users must enter a username and Password”.

**t** Click next, then finish.

**u** Log on by pressing Ctrl+Alt+Delete and entering the administrator password.

**v** Uncheck the box *Show this screen at startup.*

**w** Exit the *Network Identification Wizard*.

**4** Enable File Transfer Protocol (FTP) Service

**a** At the Windows Task bar: Click Start -> Settings->Control Panel ->Add/ Remove Programs

**b** Select Add/Remove Windows Components

**c** Deselect all components.

**d** Click Internet Information Services

**e** Click details

**f** Deselect all subcomponents.

**g** Check File Transfer Protocol (FTP) Service

**h** Click OK, then next

*The Windows Components Wizard may request that you insert the Windows 2000 CD*

**i** When the process completes, click finish

**j** Close the Add/Remove Programs window and remove the Windows 2000 CD.

5 Install the latest Microsoft Windows 2000 Professional Service Pack.

6 You have completed this procedure. Windows 2000 Professional is now installed.

**Procedure 2 Install Oracle database**

***From the Windows 2000 desktop, perform the following instructions for installing Oracle 9.2.0 database. If installing Oracle 10.1.0.2, start on the next page.***

1 Insert the Oracle 9.2.0 CD #1 into the CD-ROM drive.

2 Click the Install/Deinstall Products button.

*The Welcome Screen appears.*

3 Click next.

4 Accept the default source in the File Locations field.

5 In the Destination field, accept the suggested folder, or type a new name and path.

6 Click next.

7 At the Available Products screen Select Oracle 9i Database 9.2.0.1.0.

8 Click next.

*The Installation Types screen appears.*

9 Click the Enterprise edition button.

10 Click next.

*The Database Configuration screen appears.*

11 Select General Purpose

12 Click next

*Oracle Services for Microsoft Transaction Server Screen appears*

13 Accept port number 2030 and click next

14 Type a global database name in the Global Database Name field I (i.e NETID).

***Note: Make note of the Global Database Name. It is recommended to use this exact name in procedure 5, step 5 (Net Service Name) and procedure 6 step 4 i (Net Service Name).***

15 Click next to accept the default Database File Location.

16 Click next to accept the default Database Character Set.

*The Summary screen appears.*

17 Click Install.

18 When prompted, replace CDs and Click OK as instructed.

*Installation will take several minutes (perhaps 10 to 15 minutes per CD).*

*When the Install has completed, the Configuration Tools page appears.*

19 Permit the listed configuration tools to be automatically created.

20 When the database is successfully created, the Oracle Database Configuration Assistant screen appears.

**21** Enter and confirm passwords for the accounts SYS and SYSTEM.

***Note: Make note of these passwords. The name "system" is entered into the User ID field and the SYSTEM password is entered into the Password field in procedure 5, step 5 to create an Oracle table space and user ID.***

**22** At the End of Installation screen click exit.

**23** Confirm that you want to exit and reboot the PC.

**24** You have completed this procedure. The Oracle 9.2.0 database is installed.

***From the Windows 2000 desktop, perform the following instructions for installing Oracle 10.1.0.2 database.***

**1** Insert the Oracle 10.1.0.2 CD into the CD-ROM drive.

**2** Click the Install/Deinstall Products button.

*The Welcome Screen appears.*

**3** Accept the default path in the Oracle Home Location field and accept Enterprise Edition in the Installation Type field.

**4** The Create Starter Database field should already be selected. If not, click the selection box.

**5** Type a database name in the Global Database Name field. (i.e. NETID).

***Note: Make note of the Global Database Name. It is recommended to use this exact name in procedure 4, step 6 (Oracle Net Service / Oracle Service Name), procedure 5, step 5 (Net Service Name) and procedure 6 step 4 i (Net Service Name).***

**6** Enter and confirm the Database Password for the SYS, SYSTEM, SYSMAN and DBSNMP accounts.

***Note: Make note of the Database Password. The name "system" is entered into the User ID field and the password is entered into the Password field in procedure 5, step 5 to create an Oracle table space and user ID.***

**7** Do not select Advanced Installation. Click next.

*The Summary screen appears.*

**8** Click install.

*The Install screen appears.*

*The Configuration Assistants screen appears.*

***Note:*** *Move this window from the center of the terminal to allow in progress screens to be viewed. Installation will take approximately 1 hour 10 minutes depending upon machine speed.*

**9** Permit the listed configuration tools to be automatically created.

*The Password Management screen appears after the database is successfully created.*

**10** Click ok.

*The End of Installation screen appears.*

**11** Click exit.

**12** Confirm that you want to exit and reboot the PC.

**13** You have completed this procedure. The Oracle 10.1.0.2 database is installed.

### Procedure 3 Install Adobe Acrobat Reader

***From the Windows 2000 desktop***

**1** Insert the CD with NetID 1500 software in the CD drive.

*The NetID 1500 Setup window opens.*

**2** Click next.

*The Welcome to NetID Setup window opens.*

**3** Read the instructions on the window. When you finish, click next.

*The Setup Type window opens.*

**4** Click the Setup Adobe Acrobat Reader button.

*When the installation is complete, click OK to return to the Setup Type dialog box.*

**5** Choose to exit Setup. You can view the documentation for NetID after you have installed the NetID documentation.

**6** You have completed this procedure. Adobe Acrobat Reader is installed.

### Procedure 4 Setup an Oracle 9i Client Kit

***NOTE: From the Windows 2000 desktop, perform the following instructions for installing NETID 4.5.***

**1** Insert the NetID CD into the CD-ROM drive. The installation procedure should begin automatically, and the NetID Setup screen should appear. You can also install the NetID application from the Control Panel by selecting Add/Remove Programs.

*The NetID Setup Version screen appears.*

**2** Click next.

*The Welcome To NetID Setup screen appears, with some information about the product.*

**3** Read the Welcome To NetID Setup screen, and click next.

*The Setup Type screen appears.*

**4** Click Setup Oracle 9i Client Kit.

**5** Accept the Oracle license agreement, click yes.

*The Oracle Client Kit Setup screen appears.*

**6** In the appropriate fields type in the Global Database Name from the Oracle 10.1.0.2 installation in procedure 2, step 5 for the Oracle Net Service and Oracle Service Name. The IP address should be the address entered in procedure 1 step 3 n. Accept the default port number.

Oracle Net Service (i.e. NETID)

Oracle Service Name (i.e. NETID)

IP address

Port (1521)

**7** Click next.

*The Oracle 9i Client Kit Product Directory screen appears.*

**8** Accept the default path. Click next.

*The System Restart screen appears.*

**9** Click yes, then finish.

**10** Ensure the system restart occurs automatically or manually.

**11** You have completed this procedure. The Oracle 9i Client Kit has been setup.

### Procedure 5 Create an Oracle table space and user ID

***Note:*** If using Oracle 9.2.0, stop the Oracle HTTP server before you begin the installation of Net ID. Select Start->Settings->Control Panel-> Administrative Tools->Services. Scroll down and double click on OracleOraHome92HTTPSERVER process. In the resulting window click Stop Service, then OK.

***From the Windows 2000 desktop***

**1** Insert the NetID CD into the CD-ROM drive. The installation procedure should begin automatically, and the NetID Setup screen should appear. You can also install the NetID application from the Control Panel by selecting Add/Remove Programs.

*The NetID Setup Version screen appears.*

**2** Click next.

*The Welcome To NetID Setup screen appears, with some information about the product.*

**3** Read the Welcome To NetID Setup screen, and click next.

*The Setup Type screen appears.*

**4** Click Create NetID Table space and User.

*The Oracle Server Connection Parameters screen appears.*

**5** In the appropriate fields type in the exact Global Database Name and Database Password from the Oracle installation in procedure 2. For Oracle 9.2.0 use steps 14 and 21. For Oracle 10.1.0.2 use steps 5 and 6.

Net Service Name (i.e. NETID)

User ID (i.e. system)

Password. (i.e. <the password you chose for SYSTEM>)

**6** Click next.

*The Database UserID & Password screen appears.*

**7** Type a user ID and password in the appropriate fields. (example: NETID, NETID).

*The Oracle Table space Parameters screen appears.*

**8** Type a name for the table space and the amount of disk space allocated for that table space in the appropriate fields (example: NETID, 100Mb), and click next.

*The SQL Utility dialog appears.*

**9** Make note of any error messages that appear, then click OK.

*When the installation is complete, the setup program returns to the Setup Type dialog box.*

**10** You have completed this step. The Oracle table space is created.

### Procedure 6 Install the NetID product

***Note:*** If using Oracle 9.2.0, stop the Oracle HTTP server before you begin the installation of Net ID. Select Start->Settings->Control Panel-> Administrative Tools->Services. Scroll down and double click on OracleOraHome92HTTPSERVER process. In the resulting window click Stop Service, then OK.

***From the Windows 2000 desktop***

**1** Reinsert the CD with NetID software in the CD drive.

*The NetID Setup window opens.*

**2** Click next.

*The Welcome to NetID Setup window opens.*

**3** Click next.

*The Setup Type window opens.*

**4** Install the NetID product using the following steps:

**a** Click Setup NetID Products.

*The NetID License Agreement window opens.*

**b** Read the license agreement. When you finish, click yes.

*The Organization Name window opens.*

**c** The organization name defaults to the company name entered in the Windows 2000 installation. Click next.

*The NetID Product Setup Type window opens.*

**d** Select Typical to use the default NetID configuration parameters and click next.

*The NetID Product Directory window opens.*

**e** Follow the instructions on the window if you want to change the destination directory. When the destination directory is correct, click next.

*The NetID Component & Subcomponent Selection window opens.*

**f** Ensure that all desired NetID components are checked and click next. Unselect DNS Server if you are not using this NetID server for DNS.

**g** Click next.

**h** If installing NETID 4.5:

*The Existing Database Client Kit Type window opens.*

Click Oracle Server 9i / Net 9 Client.

Click next.

*The Oracle Connection Parameters window opens.*

**i** Type in the exact Global Database Name from the Oracle installation in procedure 2 in the Net Service Name field. For Oracle 9.2.0 use step 14. For Oracle 10.1.0.2 use step 5.

Net Service Name (i.e. NETID)

**j** Click next.

*The Database UserID and password window opens.*

**k** Use the defaults for User ID and Password. Click next.

*The NetID Application Server Setup window opens.*

**l** For the application server, enter port number 8181.

***Caution**: Although the Application Server uses port 80 as its default, you must set the port number if you have another server running on that standard server port. For example, Internet Information Services (IIS), by default, also uses port 80. In addition, by default, the Oracle HTTP server uses port 8080 and, by default, automatically starts at startup. If you want to use port 80 or 8080 for your Application Server, it is recommended that you uninstall or stop any other servers on that system that will use that port.*

**m** Click next.

*The NetID Server Manager Setup window opens.*

**n** For the server manager, use the defaults for Port Number and Max Connections. Click next.

***Note:*** If installing NETID 4.5, there is not a Max Connections field.

*The NetID Server Manager Connection Setup window opens.*

**o** For the server manager, ensure that the IP Address is for the primary DHCP server. Use the default for Port Number. Click next.

***Note:*** Even when installing the backup DHCP server, use the IP address for the primary DHCP server, because the primary DHCP server provides the server manager function.The IP address should be the address entered in procedure 1 step 3 n (primary DHCP server installation).

*If you installed DNS services The NetID DNS Server Setup window opens.*

**p** The Fully Qualified Domain Name (FQDN) of the DNS server defaults to the name entered in the Windows 2000 installation. Click next.

*The NetID SNMP Trap Destination window opens.*

**q** Enter the IP address of the SNMP network management node in the Trap Destination IP field. For the Trap Community, enter the SNMP community name as datafilled in parameter IPGW_SNMP_COMMUNITY_NAME in Table OFCENG.

***Note:*** This only affects the 7X07AA cards defined in Table IPINV as TOPS IPGWs (GW_TYPE=TOPS).

**r** Click next.

*The NetID Services Startup Selection window opens.*

**s** Leave all the selections checked. Click next.

***Note:*** If DNS is not used, uncheck NetID DNS Server.

*The NetID Product Setup Summary window opens.*

**t** Follow the instructions on the window to change the information if needed. When the information is correct, click next.

*NetID begins the installation process. Note any errors during the installation.*

*The NetID Database Client Kit Configuration Verification window opens.*

***Note**: The appearance of IP address 127.0.0.1 as the server address indicates the primary server may be unable to connect to the server manager. The appearance of 127.0.0.1 may be a result of the server not being connected to the LAN network.*

*The Verification Complete information should state "No critical errors were detected." and the database connection should indicate connected.*

**u** Click OK.

*The SQL Utility window opens.*

**v** When the installation process finishes, click OK.

*"Installing/Updating NETID 1500 IP License" and "Checking Database integrity" messages appear.*

**w** Click the Finish button to complete the NetID setup.

*The Windows 2000 desktop opens.*

**5** Load the Sun JRE from the NetID 4.3.3 or 4.5 CD using the following steps:

**a** From the Windows task bar Click Start-> Run

**b** Type *explorer* and click OK

**c** Select My Computer-> CD Drive->Auxiliary->common->JRE1.4.2->nt

**d** execute j2re-1_4_2-windows-i586.exe by double clicking it.

**e** Accept the licensing agreement. Click next.

**f** Set installation type to typical. Click next.

**g** When the InstallShield Wizard completes, Click finish.

**6** Close the Explorer window and remove the NetID CD.

**7** Restart your system for the application to run properly.

**8** You have completed this procedure. The NetID product is installed.

### Procedure 7 Set a permanent NetID administrator

***Note:*** If you are the system administrator who is initially setting up NetID, use the default user ID (admin) and password (ADMIN) the first time you log in to NetID. However, for security reasons, you should immediately change the default system administrator account to restrict the general availability of administrator access privileges in NetID.

***From the Windows 2000 desktop***

**1** Select Start->Programs->NetID->NetID Management Console.

*If this is the first use of the Internet Explorer, the Internet Connection Wizard will open.*

**2** Initialize Internet Explorer as follows:

**a** Select "I want to set up my Internet connection manually or I want to connect through the Local Area Network (LAN)."

**b** Click next.

**c** Select "I connect through a Local Area Network (LAN)".

**d** Click next.

**e** Select Automatic detection of proxy server.

**f** Click next.

**g** Select No to setting up an email account.

**h** Click finish.

**3** Internet Explorer Enhanced Security Configuration Warning will appear. Click Add this as a trusted site.

**4** Another Security warning will ask if you want to trust the signed applet from Nortel Networks. Click Always.

***Note**:Refer to the "Introduction to the Management Console" chapter in Managing IP Addressing in NetID for more information.*

**5** Verify that SUN Java Runtime Environment (JRE) version 1.4.2 or later is installed and enabled. Please refer to "DHCP server software" on page 497 for additional information. Enable JRE as follows:

**a** In Internet Explorer, click Tools->Internet Options.

**b** In the Internet Options dialog box, click on the Advanced tab.

**c** In the Settings list, scroll down to the Java (SUN) entry and enable the Use Java <version_number> for Applets check box.

**d** Uncheck the entry for Microsoft VM if present.

**e** Shut down and then restart Internet Explorer.

**6** Select Start->Programs->NetID->NetID Management Console.

*The NetID Login dialog box appears.*

**7** In the User ID field, type your user ID. The user ID cannot exceed eight characters.

**8** In the Password field, type the password assigned to you by the NetID system administrator (passwords are case sensitive). (initial logon: admin, ADMIN)

**9** Click OK.

*The NetID Management Console interface appears.*

**10** Under the Setup root object, expand the Users and Groups object, then expand the Users object.

**11** Highlight the administrator user object, and choose Properties from the Options pull-down menu.

**12** In the User Properties dialog box, enter your name and contact information in the appropriate fields, and click OK.

**13** From the File menu, choose Change Password.

*The Change Password dialog box appears.*

**14** In the Old Password field, type your old password.

**15** In the New Password field, type a new password.

**16** In the Confirm Password field, type the new password again.

**17** Click OK. If you type the incorrect password in the Old Password field, an error message appears. You cannot change your password unless you enter the correct old password. Click OK, and go back to step 13 of this procedure.

**18** You have completed this procedure. Users can no longer log in as the admin user using the default password.

### Procedure 8 Set up Gateway load user access

Setting up Gateway load user access consists of the following broad steps:

- Install the loadfile in the `C:\Gateway` directory.
- Add Gateway user access.
- Configure the FTP (file transfer protocol) service used to load the Gateway.

***From the Windows 2000 desktop***

**1** Install the Gateway loadfile using the following steps:

**a** Insert the CD with the Gateway loadfile.

*After a few seconds, the system displays a series of dialog boxes.*

**b** Click next to install the loadfile.

**c** Click next to accept the default destination location.

**d** Click next to accept the default program folder.

**e** Confirm the settings and click next.

*The system installs the Gateway load subdirectories and files in the C:\Gateway directory.*

**f** Click the Finish button.

**g** Read and close the Release Notes.

**h** Remove the CD from the drive.

**i** In the My Computer window, double-click the `C:\Gateway` folder.

**j** Open the program folder.

*The Gateway load subdirectories (folders) are listed. The loadfile is contained in the Ppc subdirectory.*

**k** Open the `Ppc` folder.

**l** Select the loadfile (for example, `topsipgw40ae`) and copy the file (Edit->Copy).

**m** Paste the file (Edit->Paste) in the `C:\Gateway` folder.

*The loadfile is listed.*

*You may also choose to rename this file to a generic name like 7x07load so that you can use a generic name in your DHCP options template.*

**n** Close all open windows on the desktop.

**2** Add user access for the `C:\Gateway` directory using the following steps:

**a** Select Start->Settings->Control Panel->Administrative Tools->Computer Management.

*The Computer Management window opens.*

**b** Expand Local Users and Groups, select Users.

**c** Click Action in the menu bar and select New user.

*The New User window opens.*

**d** Enter data in the new user window as follows:

- Enter `Gateway` as the username.
- Enter a full name (for example, `Gateway user`).
- Enter a description.
- Enter `tazmanian` as the password and confirm
- Uncheck User Must Change Password at Next Logon.
- Check User Cannot Change Password.

  ***Note:*** This default password *must not* be changed.
- Check Password Never Expires.
- Uncheck Account Disabled.
- Click Create then Close.

*The new Gateway user access is listed in the User Manager window.*

**e** Close the User Manager window.

**3** Configure the FTP service using the following steps:

**a** Select Start->Settings->Control Panel->Administrative Tools->Internet Services Manager

**b** Highlight the computer name in the left pane.

**c** Select Default FTP Site in the right pane.

**d** Click Action in the menu bar and select Properties.

**e** Click FTP Site tab.

**f** Ensure Enable Logging is checked.

**g** Click the properties button.

**h** Select Daily for the New Log Time period.

**i** Choose to file logs to the directory `C:\Gateway`.

**j** Click Apply, then click OK.

**k** Click the Security Accounts tab.

**l** Click Browse

**m** Select/highlight the user *gateway*.

**n** Click OK.

**o** Ensure that Allow anonymous connections is *not* checked. (Click the Yes button if you receive an authentication message.)

**p** Click the Messages tab and leave all fields blank.

**q** Click the Home Directory tab. Add the new directory as the Home (default) directory using the following steps:

**i** Select “a directory located on this computer”.

**ii** Click the Browse button and select `C:\Gateway.`

**iii** Ensure that Read and Write and Log Visits are all checked.

**iv** Click Apply, then click OK.

**r** You have completed this procedure.

## Configuration

This section provides a procedure to configure NetID as a DHCP server for TOPS-IP. This procedure uses values from the example configuration (page 499) and from the various provisioning worksheets beginning on page 499. These values are examples only.

***Note 1:*** For complete information on using NetID, refer to the NetID documentation suite.

***Note 2:*** If system performance becomes sluggish during the configuration, you may be able to improve the performance by truncating the NetID logs. See Procedure 12 on page 524.

### DHCP options guidelines

When setting up DHCP options for the cards in the IP-XPM (which NetID views as “hosts”), keep in mind the following guidelines:

- Datafill the IP address for every subnetwork in your TOPS-IP network before proceeding to datafill the host IP addresses associated with the subnetwork. Refer to Step 4.
- Ensure that the MAC Type field for each host is set to “Ethernet.”
- Since several DHCP parameter values are common across hosts, one or more DHCP options templates can be set up to avoid entering identical values repeatedly. Refer to Step 7 (Gateways) and Step 9 (SX05s) for details.
- The BOOTP function for the Gateway cards should be set to boot from either the primary or backup server (All DHCP/BootP Servers). See step 8 for details.

  ***Note:*** The BOOTP function does not apply to SX05 cards.
- The SX05 cards should be balanced across the default routers. For example, half the cards should use the first router as the default and half should use the second router as the default. Refer to Step 9 for details.

**Procedure 9 Configure NetID**

Configuring NetID consists of the following broad steps:

- Datafilling the domain name of the network.
- Datafilling the IP address of each subnetwork.
- Datafilling the IP addresses of the DHCP servers (primary and backup).
- Datafilling the DHCP server communication.
- Datafilling the DHCP options template for the Gateway cards.
- Datafilling each Gateway card (up to 10 per IP-XPM) as a host and apply the Gateway template to it.
- Datafilling the DHCP options template for the SX05DA cards.
- Datafilling each SX05 card (2 per IP-XPM) as a host and apply the SX05 template to it.

***From the Windows 2000 desktop***

**1** Open the NetID program in the browser window.

*The NetID Login window opens.*

**2** Enter the user ID and password. The default user ID is admin and the password is ADMIN. (Your office can change the user ID and password or create new user IDs and passwords.)

*The NetID Management Console window opens.*

**3** Datafill the network domain name using the following steps:

**a** Select the root object `Domain Names.`

**b** From the pull-down menu, select **Options->New Domain.**

*The New Domain window opens at the Label tab.*

**c** Enter the parent domain (for example, “com”) in the Label field.

**d** Click the OK button.

*The domain name appears in the right pane of the console window.*

**e** Expand the `Domain Names` tree in the left pane and select the parent domain.

**f** From the pull-down menu, select **Options->New Domain.**

**g** Enter the next portion of the company domain name (for example, “nortelnetworks”).

**h** Click the OK button.

*The domain name appears in the right pane of the console window.*

**4** Datafill the IP address of each subnetwork using the following steps:

**a** Select the root object `IP Addresses.`

**b** From the pull-down menu, select **Options->New Network.**

*The New Network window opens at the Network tab.*

**c** Enter the following information:

- Network Number (for example, 95.92.9.0)
- Network Name

**d** Check the Fixed box for Subnet Type and enter the Mask Length.

**e** Check the Classless Network box and enter the same Mask Length.

**f** Click the OK button.

*The network IP address and name appear in the right pane.*

**g** Repeat substeps a through f for *each subnetwork* supported by this DHCP server.

**5** Datafill the IP address of the DHCP servers using the following steps:

**a** Expand the `IP Addresses` tree, expand the network and select the network IP address.

**b** From the pull-down menu, select **Options->New Host.**

*The New Host window opens at the Host tab.*

**c** Enter the IP address of the primary DHCP server in the Host field.

**d** For the Domain Name, click the icon to the right of the field to open a window with the newly created domain name in it. Traverse the tree until the full domain name is displayed.

**e** Select the full domain name and click the OK button.

**f** Place the cursor in the Domain Name field in front of the domain name. Enter the name of the primary DHCP server, followed by a dot. (For example, “topsipserver1.” Then the Domain Name field would contain “topsipserver1.nortelnetworks.com.”)

**g** Click the OK button.

**h** Click the Yes button to save the new host.

*The IP address and name of the primary DHCP server appear in the right pane.*

**i** Repeat these substeps for the backup DHCP server, except use the unique IP address and domain name for the backup server.

*The IP addresses and names of both DHCP servers appear in the right pane.*

**6** Datafill the DHCP server communication using the following steps:

**a** Select the root object `DHCP Servers`.

**b** From the pull-down menu, select **Options->New DHCP server**.

*The New DHCP Server window opens at the DHCP Server tab.*

**c** Enter the IP address of the primary DHCP server in the Host IP Address field. The IP address should be the address entered in procedure 1 step 3 n.

**d** Click the OK button.

*The IP address of the primary DHCP server appears in the right pane of the console window. The Status field displays "Down."*

**e** Repeat these substeps for the backup DHCP server, except use the unique IP address for the backup server.

*The IP addresses of both DHCP servers appear in the right pane of the console window.*

**f** Double-click the IP address of the backup DHCP server in the right pane.

*The Update DHCP Server window opens at the DHCP Server tab.*

**g** Click the Backups tab. The primary DHCP server IP address and name should appear in the "All Available DHCP Servers" window. Select the primary server and click the left arrow to move it under "This DHCP Server Backs Up these DHCP Servers" window.

**h** Click the OK button.

*The IP addresses of both DHCP servers appear in the right pane of the console window. The Status displays for both servers may show "Disconnected." This is an anomaly if using the 4.3 release of NetID and does not indicate a problem. The backup DHCP server will ping the primary DHCP server every 60 seconds. When the backup server does not get a reply for 180 seconds, it takes over as the primary DHCP server.*

**7** Datafill the DHCP options template for the Gateway cards using the following steps:

***NOTE: This step should only be performed for the primary DHCP server.***

**a** Expand the root object `Setup`.

**b** Expand the object `Templates.`

**c** Select `DHCP Option Templates`.

**d** From the pull-down menu, select **Options->New DHCP Option Template**.

*The New DHCP Template window opens at the Name tab.*

**e** Enter a name for the Gateways template.

**f** Click the DHCP Options tab.

**g** Click Add.

**h** Expand the `Standard` tree.

**i** Expand `Application and Service Parameters.`

**j** Add the following DHCP options to the Gateway template by selecting and double-clicking the option name:

***Note***: Click Add after adding each option

- From the `Application and Service Parameters` tree:
  - `Boot File`
  - `MobileIP Home Agents`
- From the `System Managed` tree:
  - `DNS Domain Name`
  - `HostIP Address (BOOTP only)`
  - `Host name`
  - `Lease Time`
- From the `RFC2132 Options` tree:
  - `Routers`

**k** Highlight each option in the window, and enter your site-specific values next to each option. These are the values that are identical across all Gateway cards. The values will be applied to each Gateway in Step 8. Refer to Figure 163 on page 502 for examples of valid values used in the sample configuration.

**l** Click the OK button.

*The new template name appears in the right pane.*

**8** Datafill each Gateway card as a host and apply the Gateway template to each using the following steps:

***Note: This step should only be performed for the primary DHCP server.***

**a** Expand the `IP Addresses` tree and select the IP address of the subnet. Expand the subnet address tree.

**b** From the pull-down menu, select **Options->New Host.**

*The New Host window opens at the Host tab.*

**c** Enter the unique IP address of the Gateway card in the Host field.

***NOTE:*** *The IP address is datafilled in table IPINV in the TOPS switch.*

**d** Click the icon to the right of the domain name field to browse the domain levels. Select the correct domain name for the Gateway and click OK. Enter the unique name of the Gateway card at the front of the domain name in the field (for example, dtc10gw1.nortelnetworks.com).

**e** Enter the Time to Live (lease time, for example, 67108864) in the TTL field.

**f** Set MAC Type to Ethernet.

**g** Enter the MAC address of the Gateway card. (This is the numerically lower of the two MAC addresses printed on the card. i.e. 00:60:38:79:01:02)

**h** Click the DHCP Options tab.

**i** Click the Apply Template button.

**j** Select the Gateway template name defined in the previous step and click the OK button.

**k** Review the values imported by the template and adjust any parameter values as needed. Ensure that the host name and host IP address are correct for the individual Gateway being defined

**l** Click the Protocol tab.

**m** Click the DHCP Client box.

**n** Click the All DHCP/BootP Servers box.

***NOTE: Selecting the All DHCP/BootP Servers box and leaving the BootP Server (SI ADDR) field blank allows the gateway to load from either the primary or backup server.***

**o** Click the BootP Client Box

**p** Leave the BootP Server (SI ADDR) field blank.

**q** Enter the Gateway loadfile name in the BootP File field (for example topsipgw40ae or the generic name if you had renamed the current load)

**r** Enter the Time to Live (lease time, for example, 67108864) in the lease field.

**s** Click the OK button.

*The IP address and name of the Gateway host appear in the right pane, along with the status and MAC address.*

**t** Double-click the Gateway host in the right pane. Click the DHCP Options tab to review the options and adjust any parameter values as needed. Ensure that the host name and host IP address are correct for the individual Gateway being defined.

**u** Repeat these substeps for each Gateway.

**9** Datafill the DHCP options template for the SX05 cards using the following steps:

***NOTE: This step should only be performed for the primary DHCP server.***

***Do not perform step 9 if table XPMIPMAP in the TOPS switch has field IPCONFIG datafilled as "CM". This indicates the SX05 is loaded from the switch, not the DHCP server.***

**a** Expand the `Setup` tree.

**b** Expand the object `Templates.`

**c** Select DHCP Option Templates.

**d** From the pull-down menu, select **Options->New DHCP Options Template**.

**e** Enter a name for the SX05 template.

**f** Click the DHCP Options tab.

**g** Click Add.

**h** Expand the `Standard` tree.

**i** Expand `Application and Service Parameters.`

**j** Add the following DHCP options to the SX05 template by selecting and double-clicking the option name:

- From the `Application and Service Parameters` tree:
  - `MobileIP Home Agents`
- From the `NetID Managed` tree:
  - `DNS Domain Name`
  - `HostIP Address (BOOTP only)`
  - `Host name`
  - `Lease Time`
- From the `RFC2132 Options` tree:
  - `Routers`

**k** Highlight each option in the window, and enter your site-specific values next to each option. These same values will be applied to each SX05 in Step . Refer to Figure 164 on page 502 for examples of valid values used in the sample configuration.

**l** Click the OK button.

*The new template name appears in the right pane.*

**10** Datafill each SX05 card as a host and apply the SX05 template to each using the following steps:

***NOTE: This step should only be performed for the primary DHCP server.***

***Do not perform step 10 if table XPMIPMAP in the TOPS switch has field IPCONFIG datafilled as "CM". This indicates the SX05 is loaded from the switch, not the DHCP server.***

**a** Expand the `IP Addresses` tree and select the IP address of the subnet. Expand the subnet address tree.

**b** From the pull-down menu, select **Options->New Host.**

*The New Host window opens at the Host tab.*

**c** In the Host field, enter the *active* IP address when datafilling against the MAC address of unit 0. Enter the *inactive* IP address when datafilling against the MAC address of unit 1. (The MAC address is entered in substep f.)

***Note:*** During the IP bootstrapping process, the IP-XPM will automatically adjust to use its 4 IP addresses correctly.

**d** Enter the Time to Live (lease time, for example, 67108864).

**e** Click the icon to the right of the domain name field to browse the domain levels. Select the correct domain name and click OK. Enter the unique name of the SX05 card at the front of the domain name in the field (for example, dtc10sx1.nortelnetworks.com).

**f** Enter the MAC address of the SX05 card.

**g** Set MAC Type to Ethernet.

**h** Click the DHCP Options tab.

**i** Click the Apply Template button.

**j** Select the SX05 template name defined in the previous step and click the OK button.

**k** Click the Protocol tab.

**l** Select the primary DHCP server from the pull-down list.

**m** Click the DHCP Client box.

**n** Click the BootP Client box and enter the IP address of the DHCP server that will boot the SX05. (Do not enter a boot file name.)

**o** Click the OK button.

*The IP address and name of the SX05 host appear in the right pane, along with the status and MAC address.*

**p** Double-click the SX05 host in the right pane. Click the DHCP Options tab to review the options in the left pane and adjust any parameter values as needed. Ensure that the host name and host IP address are correct for the individual SX05 being defined.

**q** Repeat these substeps for the other SX05 card.

**11** You have completed this procedure.

***Note:*** You can verify the existence of the database transfer from the Primary DHCP Server to the Backup DHCP Server by examining the file **`C:\Program Files\Optivity\NetID\etc\dhcpcfg`** (NETID 4.3) or **C: \Program Files\Nortel Networks\NetID\etc\dhcpcfg** (NETID 4.5) on the Backup DHCP Server.

## Maintenance

This section provides procedures for managing logs generated by Windows 2000 and NetID, and for stopping and restarting NetID services. It also includes notes about eliminating two errors that may be seen in the Event Viewer during or following installation.

To maintain optimum performance of the NetID server, you should *trim* the NetID logs on a periodic basis. The procedure for *truncating* the NetID logs is not part of routine maintenance, but it may be useful during or following the initial configuration if system performance becomes sluggish.

The Windows 2000 logs and the NetID logs are related, but they are not the same thing. The NetID logs are used to populate the Windows 2000 logs. Clearing one set of logs does not clear the other.

The installation procedures configure the NetID services to start automatically at system startup, so it is not normally necessary to start the services manually. However, the services need to be manually stopped before truncating logs or collecting traces, and afterward you must either manually restart the services or reboot the PC.

Following the procedures for managing logs and for stopping and starting services, this section includes notes about how to remedy two errors that may occur during Windows and Oracle installation. These notes reference Microsoft Knowledge Base articles for more information.

### Procedure 10 Prevent Windows 2000 “Log table full” warnings

This procedure may be performed in conjunction with the initial NetID installation, or it may be performed at any time if Windows 2000 “Log table full” warnings appear. It prevents the warnings from appearing or reappearing.

Preventing “Log table full” warnings consists of the following broad steps:

- Open the Windows 2000 Event Viewer.
- Configure 2000 to overwrite system logs.
- Configure 2000 to overwrite application logs.

***From the Windows 2000 desktop***

**1** Select Start->Programs->Administrative Tools (Common)-> Event Viewer.

*The Event Viewer window opens.*

**2** Configure Windows 2000 to overwrite system logs using the following steps:

**a** Highlight System Logs, right-click and select Properties.

**b** Click the button to the left of “Overwrite Events as Needed.”

**c** Click OK.

*The system returns you to the Event Viewer window.*

**3** Configure Windows 2000 to overwrite application logs using the following steps:

**a** Highlight Application Logs, right-click and select Properties.

**b** Click the button to the left of “Overwrite Events as Needed.”

**c** Click OK.

*The system returns you to the Event Viewer window.*

**4** Exit the Event Viewer.

**5** You have completed this procedure.

### Procedure 11 Trim NetID logs

Perform this procedure periodically to maintain optimal performance of the NetID server. The NetID server generates logs that can grow large enough to cause sluggish performance if this is not done.

This procedure can be used to delete log entries that were generated earlier than the current date. (Note: To delete all logs, including those generated on the current date, see Procedure 12 on page 524.)

After logging into the NetID Management Console (**Start->Programs->NetID-> NetID**; enter your site’s NetID userid and password), Trimming NetID logs consists of the following broad steps:

- Trim history logs.
- Trim server alarms.

***From the NetID Management Console window***

**1** Trim the history logs using the following steps:

**a** Click on File, then select Trim Logs... from the pull-down menu.

*The Trim Logs window opens.*

**b** In the Log File box, select History.

**c** Click the Calculate button next to the Number of Existing Entry field.

*The number of history logs is displayed in the Number of Existing Entry field. This may take a few seconds depending on the size of the log file.*

**d** Click the calendar icon next to the Delete Entries Before field.

*The Date Properties box appears.*

**e** Select a date.

Selecting today's date will maximize the number of logs trimmed, but will still preserve all logs that were generated on today's date.

**f** Click OK.

*The system returns you to the Trim Logs window, and the selected date appears in the Delete Entries Before field.*

**g** Click OK.

*The system briefly displays some messages about the trim logs process.*

**h** Check the Scheduled Trim Events tab and configure automatic log trimming as desired.

**2** Trim the server alarm logs using steps a through h above, except in step b, select Server Alarms (rather than History) in the Log File box.

**3** You have completed this procedure.

### Procedure 12 Truncate NetID logs

This procedure can be used to delete all history and server alarm log entries, including those that were generated on the current date. This procedure may be performed, instead of Procedure 11 (Trim NetID logs), if system performance becomes sluggish because a large number of logs have been generated on today's date. For example, you may want to perform this procedure during or immediately following the initial installation and configuration of the NetID database.

This procedure accesses the same logs as Procedure 11, but it accesses them directly through the Oracle SQL Worksheet application rather than indirectly through the NetID Management Console. The SQL entity `nid4_delta_log` corresponds to the NetID history log. The SQL entity `nid4_server_alarms` corresponds to the NetID server alarms log.

Truncating NetID logs consists of the following broad steps:

- Stop all NetID services.
- Log into the SQL Worksheet application.
- Check the number of records in the nid4_delta_log and the nid4_server_alarms.
- Truncate both logs.
- Verify that there are no records for either log.
- Exit the SQL Tablet.
- Restart appropriate NetID services.

***From the Windows 2000 desktop***

**1** Stop all NetID services using Procedure 13 on page 525.

**2** Enter the SQL Worksheet application using the following steps:

**a** Select Start->Programs->Oracle->OraHome92->Application Development->SQLPlus Worksheet.

*The Oracle Login window opens.*

**b** Enter your site's userid and password.

*The SQL Tablet window opens. The SQL tablet has two frames. All entries are typed in the upper frame. Results are displayed in the lower frame.*

**3** Check the number of records in the nid4_delta_log and nid4_server_alarms using the following steps:

**a** In the upper frame, type:
```
select count (*) from nid4_delta_log;
```

**b** Click the Execute button (lightening bolt).

*In the lower frame, the system displays the number of records in the nid4_delta_log.*

**c** In the upper frame, type:
```
select count (*) from nid4_server_alarms;
```

**d** Click the Execute button (lightening bolt).

*In the lower frame, the system displays the number of records in the nid4_server_alarms log.*

**4** Truncate both logs using the following steps:

**a** In the upper frame, type:
```
truncate table nid4_delta_log;
```

**b** Click the Execute button (lightening bolt).

*In the lower frame, the system displays the command with a Statements processed result. This may take some time.*

**c** In the upper frame, type:
```
truncate table nid4_server_alarms;
```

**d** Click the Execute button (lightening bolt).

*In the lower frame, the system displays the command with a Statements processed result. This may take some time.*

**5** Verify that no records remain in either log you just truncated, by repeating Step 3 of this procedure.

*This time the number of records that the system displays should be 0 for both logs.*

**6** Exit SQL Tablet.

**7** Restart appropriate NetID services using Procedure 14 on page 526.

**8** You have completed this procedure.

### Procedure 13 Stop NetID services

This procedure is the first step of Procedure 12, which is described on page 524. This procedure should also be performed before collecting traces. (Traces are not collected as part of routine maintenance but may sometimes be helpful in debugging if problems arise. The method for collecting traces is described in the NetID documentation.)

Since your network has a primary and a backup DHCP server, it is safe to temporarily stop services on one DHCP server at a time. It is not safe for services to be stopped on both servers at the same time. Also, it is important that you remember to restart the services after you have stopped them.

The four NetID services are:

NetID Application Manager,
NetID DHCP Server,
NetID DNS Server, and
NetID Server Manager.

***Note:*** NetID services can be started and stopped from either the NetID Services window or the Services dialog box. The same method should be used to start and to stop services. The procedures in this section use the NetID Services window. The

Services dialog box may be used instead, as long as it is used both for starting and for stopping services.

***From the Windows 2000 desktop***

1. Select Start->Settings->Control Panel.

   *The Control Panel window opens.*

2. Double-click the Optivity Services icon.

   *The Optivity Services window opens.*

3. Choose the appropriate service from the Selected NetID Services drop-down list.

4. Click Stop Selected Service

   *A message appears in the message field indicating that the service has stopped.*

5. Repeat steps 1 through 4 of this procedure until all four of the NetID services have been stopped.

6. You have completed this procedure.

***Note:*** Stopping the NetID Application Manager will disable the NetID Management Console. It will be necessary to restart the NetID Management Console.

**Procedure 14 Restart NetID services**

Normally NetID is configured so that the services are started automatically at system startup. However, after manually stopping the services, you must restart them. You can do this either by rebooting the PC or by following this procedure.

The four NetID services are:
NetID Application Manager,
NetID DHCP Server,
NetID DNS Server, and
NetID Server Manager.

***From the Windows 2000 desktop***

1. Select Start->Settings->Control Panel.

   *The Control Panel window opens.*

2. Double-click the Optivity Services icon.

   *The Optivity Services window opens.*

3. Choose the appropriate service from the Selected NetID Services drop-down list.

4. Click Start Selected Service

   *A message appears in the message field indicating that the service has stopped.*

5. Repeat steps 1 through 4 of this procedure until all four of the NetID services have been stopped.

## Remedies for errors seen in Event Viewer during installation

The following errors may appear in the Microsoft Windows 2000 Event Viewer (Start->Programs->Administrative Tools->Event Viewer; select System Logs).

**NetBT Event 4311 Initialization failed because the driver device could not be found.**

Depending upon the installation method and Service Pack level of Microsoft Windows 2000 Server, there may be corruption of NetBIOS TCP/IP protocol. While this will not prevent the server from operating, removing this error will speed boot time. There are two alternative suggested remedies:

— Remove TCP/IP networking, reboot, and reinstall TCP/IP networking.

— Edit the Windows Registry key for the NetBT adapter and delete all the Ndiswan keys.

Refer to Microsoft Knowledge Base Articles 181548 and 123981 for more details.

**W3SVC Event 115 Service could not bind to instance "X".**

This message indicates that the default HTTP server has failed to start. By default, the Default HTTP Server attempts to start using port 80. The Oracle HTTP server also uses port 80. The Default HTTP Server fails to start because the Oracle HTTP Server is already using port 80 and generates this message. There are two alternative suggested remedies:

— Remove the Default HTTP Server.

Start->Programs->Administrative Tools->Internet Services Manager

Highlight the server name, highlight Default HTTP Server, right click and select Delete.

— Change the Default HTTP Server port number to an available port number.

Start->Programs->Administrative Tools->Internet Services Manager

Highlight the server name, highlight Default HTTP Server, right click and select Properties. Assign an unused port number.

Refer to Microsoft Knowledge Base Article 284984 and 186810 for details.

## Upgrading the Gateway load

This section provides a procedure to upgrade the Gateway load. Upgrading involves installing the new load and testing it on one or more Gateways before upgrading all the Gateways that reside at the DMS TOPS switch.

***Note:*** This procedure requires users to have handy the IP address and IPNO value (table IPINV) for each Gateway.

### Procedure 15 Upgrade the Gateway load

Installing an upgrade of the Gateway load consists of the following broad steps:

- Install the new loadfile in the `C:\Gateway` directory.
- Change to the new loadfile name in NetID for a test Gateway.
- Take down, reload, and bring the test Gateway into service at the DMS MAP.
- Test the new load.
- Change to the new loadfile name in NetID for all the Gateways.
- Change to the new loadfile name in the Gateways DHCP Options template (used to configure any new Gateways with the new load).
- Take down, reload, and bring each Gateway into service at the DMS MAP.

***From the Windows 2000 desktop***

**1** Install the new loadfile using the following steps:

**a** Insert the CD with the Gateway loadfile.

*After a few seconds, the system displays a series of dialog boxes.*

**b** Click next to begin the install process.

**c** Click next to accept the default destination location.

**d** Click next to accept the default program folder.

**e** Confirm the settings and click next.

*The system installs the new Gateway load subdirectories and files in the C:\Gateway directory.*

**f** Click the Finish button.

**g** Read the Release Notes and make note of the new loadfile name, for example, `topsipgw40ae`.

**h** Close the Release Notes.

**i** Remove the CD from the drive.

**j** In the My Computer window, double-click the `C:\Gateway` folder.

*The new Gateway load folder is listed, along with the old load folder.*

**k** Open the program folder of the *new* Gateway load.

*The load subdirectories (folders) are listed. The loadfile is contained in the Ppc subdirectory.*

**l** Open the `Ppc` folder.

**m** Select the loadfile (for example, `topsipgw40ae`) and copy the file (**Edit->Copy**).

**n** Paste the file (**Edit->Paste**) in the `C:\Gateway` folder.

*The new loadfile is listed, along with the old loadfile.*

**o** Close all open windows on the desktop.

**2** Change to the new loadfile name for a test Gateway in NetID using the following steps:

**a** Open the NetID program in the browser window.

*The NetID Login window opens.*

**b** Enter the user ID and password.

*The NetID Management Console window opens.*

**c** Expand the `IP Addresses` tree. In the left pane, expand the subnet address tree on which the test Gateway resides. Expand the next-level subdirectory.

*The IP addresses of all the hosts in the subnet appear in the right pane.*

**d** In the right pane, double-click the IP address of the test Gateway.

*The Update Host window for that Gateway opens.*

**e** Click the DHCP Options tab.

**f** In the left pane, adjust the column width of the Value field to display the entire loadfile name next to the Boot File field (or use the horizontal scroll bar).

**g** Enter the new loadfile name in the Value field.

**h** Click the OK button.

*NetID updates the loadfile name and closes the Update Host window.*

**i** Verify the change by double-clicking the IP address of the test Gateway again to open the Update Host window. Click the DHCP Options tab to check for the new loadfile name in the Boot File field. Click the Cancel button.

**3** Close all windows and exit the NetID program.

***From the DMS MAP***

**4** Take down, reload, and bring the test Gateway into service using the following steps:

**a** Post the test Gateway (IPGW) at the PM level of the MAP, for example, `POST IPGW TGWY 10 3`.

**b** Issue the BSY DRAIN command. Draining allows calls in progress on a Gateway to remain up until completion, while preventing future call originations.

*After draining is complete, the Gateway transitions to a MANB state.*

**c** Issue the PMRESET command to load the test Gateway with the new load. Ensure that the MTCE flag reappears at the MAP with the Who Am I status (MTCE:WAI/STATUS) before proceeding to the next step.

**d** Issue the LOADPMQ command to verify that the load the Gateway is running is the desired one. The response to this command includes the software release that the Gateway is actually running.

**e** Issue the RTS command. If RTS is not successful, refer to “Troubleshooting the Gateway” on page 308.

*Observe any PM or IPGW logs that accompany the RTS. After coming into service, the new Gateway load is available for use.*

**5** Follow your standard procedures for testing the new Gateway load. If the load is acceptable, continue with the next step. If the load is not acceptable, contact Nortel Networks technical support.

***From the Windows 2000 desktop***

**6** Change to the new loadfile name for each remaining Gateway in NetID by repeating Step 2 of this procedure.

**7** Change to the new loadfile name in the DHCP Options template using the following steps:

**a** Expand the root object `Setup`.

**b** Expand object `Templates`

**c** Select `DHCP Option Templates`.

*The currently defined DHCP option templates are shown in the right pane.*

**d** Double-click the name of the template used for Gateways.

*The Update DHCP Template window opens at the Name tab.*

**e** Click the DHCP Options tab.

**f** In the left pane in the Boot File field, enter the new loadfile name.

**g** Click the OK button.

*NetID updates the loadfile name and closes the Update DHCP Template window.*

**8** Close all windows and exit the NetID program.

***From the DMS MAP***

**9** Repeat Step 4 of this procedure for each remaining Gateway.

**10** You have completed this procedure.

## Changing the Gateway configuration

After installing the 7X07 Gateway cards, users may need or want to make certain configuration changes to their default settings. These changes include:

- changing the default Gateway Telnet password (see Note)
- configuring the Gateway to recognize additional SNMP network managers
- disabling SNMP set operations

These changes can be made *only through* the Gateway's PMDEBUG interface. Since using PMDEBUG can be dangerous while the Gateway is processing calls, it is recommended that any configuration changes be made soon after installation, before DMS translations allows the Gateway cards to process calls. Alternatively, the changes can be made at a later time, but the Gateway must first be drained of calls. For details on how to make these Gateway configuration changes, refer to "SNMP security for the Gateway" on page 560 in Appendix B: "TOPS-IP support for SNMP."

***Note 1:*** By default, the Gateway Telnet password is the same as the Gateway user access password set in Procedure 8 on page 513. However, the Gateway stores and handles them as two separate passwords. The Gateway user password *must not* be changed in Windows 2000. And since it is unsafe to Telnet to a Gateway that is processing calls, users may want to change the Gateway Telnet password from its default after installation. This change does not affect the Gateway user access password.

***Note 2:*** As of SN09, Telnet may be enabled or disabled using parameter IPGW_TELNET_ENABLED in Table OFCENG. The parameter defaults to N meaning Telnet is disabled. The setting does not take effect until the data is downloaded to the 7X07AA. The craftsperson must perform a PMRESET on each 7X07AA to download the Telnet setting.

# Appendix B: TOPS-IP support for SNMP

This appendix is intended for administrators of the TOPS-IP managed IP network. Administrators monitor network performance and activities in order to detect and prevent bottlenecks, improve performance, and predict capacity requirements.

The Simple Network Management Protocol (SNMP) is widely used for IP network monitoring. SNMP consists of a set of network management standards, including a protocol, a database structure specification, and a set of data objects.

This appendix focuses on the following areas:

- General SNMP functionality
- TOPS-IP Gateway Management Information Bases (MIBs)
- SNMP security for the Gateway
- Summary of persistence of user-configured Gateway data

## SNMP functionality

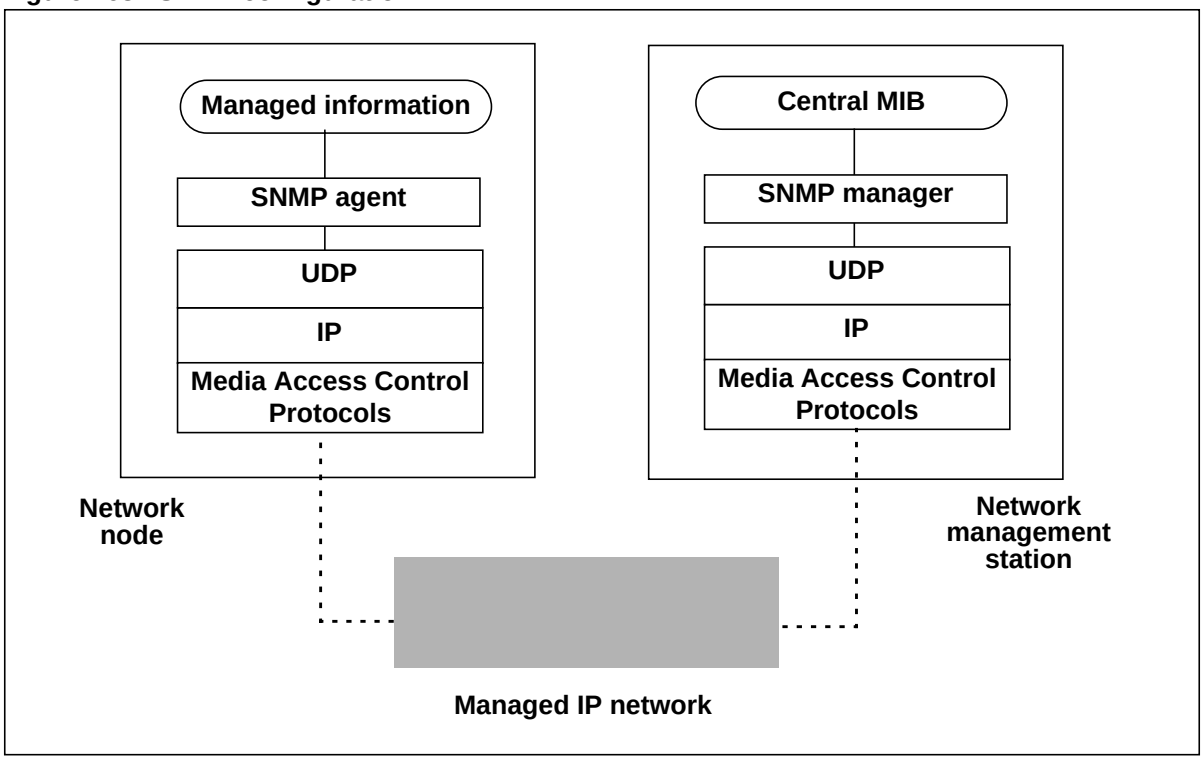
Using SNMP, a network administrator can do the following tasks from a centralized management station on the network:

- gather statistics such as CPU usage, throughput, and response time from individual network nodes
- gather node-specific data such as IP address, hardware interface information, system location, and default router information
- be made aware of network troubles from individual nodes, routers, and other devices
- control and configure a network node

A *network manager application* is used on the network management station, while an *agent application* is used on a network node that needs to be managed. Figure 268 shows an example of an SNMP configuration with the following key components:

- the managed IP network
- the network node to be managed (for example, a 7X07 Gateway)
- the network management station (for example, a PC or UNIX workstation running HP OpenView, or similar network management software)

**Figure 268 SNMP configuration**



## SNMP managed objects

Resources on a particular node are managed by representing them as objects. The collection of objects is commonly referred to as a MIB. All managed objects in SNMP are arranged in a tree structure. *Leaf objects* are the actual managed objects. Each leaf object represents some resource, activity, or other information to be managed. The tree defines the grouping of objects into logically related sets.

Each object in a MIB is identified by a unique Object Identification number (OID), for example, 1.3.6.1.2.1.1.3. This example OID refers to the system up time. The object identifier can also be interpreted in human-readable terms as "ISO.Org.DOD.Internet.Management.MIB.System.sysUPTime."

Basic messages to and from an SNMP manager consist of the following:

- GetRequest—This message retrieves the value of an object located at the agent. For example, the CPU occupancy of the node or the node's IP routing table.
- GetNextRequest—A variation of GetRequest, this message requests the object instance that is next in lexicographical order.
- SetRequest—This message is used by the manager to set information in the agent. For example, the jitter buffer minimum and maximum.
- Trap—This message is used by the agent to notify the manager of significant events. For example, when a node comes into service.

## TOPS-IP Gateway MIBs

This section introduces the TOPS-IP supported MIBs and provides details on each leaf object. Table 166 lists the TOPS-IP Gateway private MIBs provided in the TGWY0003 release.

**Table 166 TOPS-IP Gateway private MIBs**

| Name | OID | Description | Page |
|---|---|---|---|
| NT7X07AAHW.MIB | 1.3.6.1.4.1.562.28.0.2.0.2.1 | Provides 7X07 hardware details such as the card name, firmware version, memory information, and processor state. | 538 |
| AUDIOCODE.MIB | 1.3.6.1.4.1.562.28.0.2.1.5 | Provides digital signaling processor (DSP) information such as voice gain and jitter buffer settings. | 541 |
| TOPSIPGW.MIB | 1.3.6.1.4.1.562.28.0.2.4 | Provides messaging statistics for the ISUP, IGIP, H.225, and H.245 protocols. This MIB also defines items that aid in problem reporting and troubleshooting. | 544 |
| TOPSQOS.MIB | 1.3.6.1.4.1.562.28.0.2.4.4.4 | Provides voice over IP quality of service (QoS) information for the Gateway such as average network latency, high average network latency, average jitter, high average jitter, and packet loss. | 557 |
| ***Note:*** All OIDs in these private MIBs have the following prefix: 1.3.6.1.4.1.562 (ISO.Org.DOD.Internet.Private.Enterprises.Nortel) | | | |

### RFC standard MIBs

In addition to the preceding private MIBs, the following RFC (Request for Comments) standard MIBs are useful in SNMP management of the IP network:

- RFC1213.MIB (MIB-II)
- RFC1643.MIB (Ethernet-like interface types)

***Note 1:*** The TOPS-IP Gateway CD-ROM contains all six MIB files, private and standard. Network administrators should make sure to add these MIBs to their SNMP management node database.

***Note 2:*** This user guide does not detail the RFC MIBs; for more information on them, please refer to the specific RFC documents referenced in “About this document” on page 15.

### SX05DA limited SNMP capabilities

The SX05DA supports limited SNMP capabilities as defined in RFC1213 (MIB-II). The SX05DA also supports the User Security (USEC) basic group and USEC statistics from RFC1910.

No private MIBs are used for the SX05DA.

The SNMP settings apply to the SX05DA as follows:

- **SNMP community name:** The datafilled community name is validated for incoming read and write requests. The name is not sent in trap messages because the SX05DA does not send traps.
- **SNMP enable/disable:** By setting this parameter to N, the SX05DA will ignore all incoming SNMP requests. This parameter does not affect traps since the SX05DA does not send traps.

The SNMP community name and the SNMP enable/disable parameter are fields in Table XPMIPMAP, which is used to configure the SX05DA cards on the IP-XPMs. Each tuple represents one IP-XPM.

The SNMP settings are datafilled in the Succession core, but the new settings do not take effect until the data is downloaded to the IP-XPM. The craftsperson must perform a SWACT or Bsy/RTS on each unit to download the SNMP settings.

Because SNMP is present on deployed IP-XPMs, when upgrading from an older TOPS Succession core load, these fields are restored to the default after a dump and restore. The SNMP community name restores as “public,” which is also the name in use on previously deployed IP-XPMs. SNMP enable/disable restores to Y (SNMP enabled).

## NT7X07AAHW.MIB

Table 167 lists the OIDs in the NT7X07AAHW.MIB. This MIB provides the Gateway card name, firmware version, memory information, and processor state.

**Table 167 NT7X07AAHW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.0.2.1 nortelGWHardwareMIB** | Node | None | None | Hardware description of elements in the Nortel NT7X07AA circuit pack Hardware MIB |
| .28.0.2.0.2.1.1.1 norGwHwGenCardId | Leaf | Read | Display String | A textual string containing the name of the card |
| .28.0.2.0.2.1.1.2 norGwHwGenSerialNum | Leaf | Read | Display String | A textual string containing the serial number of the circuit pack |
| .28.0.2.0.2.1.1.3 norGwHwGenFPGARev | Leaf | Read | Display String | A textual string containing the revision release (major and minor) of the FPGA on the circuit pack (major and minor) |
| .28.0.2.0.2.1.1.4 norGwHwGenFWimage0 | Leaf | Read | Display String | A textual string containing the version (major and minor) of firmware image 0 |
| .28.0.2.0.2.1.1.5 norGwHwGenFWimage1 | Leaf | Read | Display String | A textual string containing the version (major and minor) of firmware image 1 |
| .28.0.2.0.2.1.1.6 norGwHwGenActFWImage | Leaf | Read | Integer | Indicates which firmware image the system is set to boot from:<br>0–firmware image 0<br>1–firmware image 1 |
| .28.0.2.0.2.1.1.7 norGwHwGenSWimage | Leaf | Read | Display String | A textual string containing the version or name of the software image name |
| **.28.0.2.0.2.1.2 norGwHwProcessors** | Node | None | None | |
| .28.0.2.0.2.1.2.1 norGwHwProcNumber | Leaf | Read | Integer 32 | The number of processors (regardless of their current state) present on this system |
| **.28.0.2.0.2.1.2.2 norGwHwProcTable** | Node | None | None | A list of processor entries. The number of entries is given by the value of procNumber. |
| **.28.0.2.0.2.1.2.2.1 norGwHwProcEntry** | Node | None | None | An entry containing management information applicable to a particular interface |
| .28.0.2.0.2.1.2.2.1.1 norGwHwProcIndex | Leaf | Read | Integer 32 | A unique index value, greater than zero, for each processor in this table |
| .28.0.2.0.2.1.2.2.1.2 norGwHwProcDescr | Leaf | Read | Display String | A textual string containing information about the Processor. This string should include the name of the manufacturer, the product name and the version of the Processor hardware/software. |
| .28.0.2.0.2.1.2.2.1.3 norGwHwProcType | Leaf | Read | Integer | The type of Processor |
| .28.0.2.0.2.1.2.2.1.4 norGwHwProcVendor | Leaf | Read | Display String | A textual string containing the Vendor name of processor |

**Table 167 NT7X07AAHW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.0.2.1.2.2.1.5 norGwHwProcID | Leaf | Read | Display String | A textual string containing Processor ID |
| .28.0.2.0.2.1.2.2.1.6 norGwHwProcRev | Leaf | Read | Integer | Processor revision |
| .28.0.2.0.2.1.2.2.1.7 norGwHwProcLoad | Leaf | Read | Integer | CPU load percentage (0-100%) |
| .28.0.2.0.2.1.2.2.1.8 norGwHwProcState | Leaf | Read | Integer | Processor State |
| .28.0.2.0.2.1.2.2.1.9 norGwHwProcFWImage | Leaf | Read | Display String | Processor Kernel Image name or Image version |
| .28.0.2.0.2.1.2.2.1.10 norGwHwProcSWImage | Leaf | Read | Display String | Processor Program Image Name or Version |
| **.28.0.2.0.2.1.3 norGwHwInterfaces** | Node | None | None | |
| .28.0.2.0.2.1.3.1 norGwHwIfNumber | Leaf | Read | Integer 32 | The number of interface devices (regardless of their current state) present on this system |
| **.28.0.2.0.2.1.3.2 norGwHwIfTable** (Note 1) | Node | None | None | A list of interface Devices entries. The number of entries is given by the value of ifDevNumber. |
| **.28.0.2.0.2.1.3.2.1 norGwHwIfEntry** | Node | None | None | An entry containing management information applicable to a particular interface |
| .28.0.2.0.2.1.3.2.1.1 norGwHwIfIndex | Leaf | Read | Integer 32 | A unique index value, greater than zero, for each interface in this table |
| .28.0.2.0.2.1.3.2.1.2 norGwHwIfDescr | Leaf | Read | Display String | A textual string containing information about the interface device. This string should include the name of the manufacturer, the product name and the version of the Interface hardware/ software. |
| .28.0.2.0.2.1.3.2.1.3 norGwHwIfType | Leaf | Read | Integer | The type of interface Device on the Gateway |
| .28.0.2.0.2.1.3.2.1.4 norGwHwIfVendor | Leaf | Read | Display String | A textual string containing the Vendor name of interface Device |
| .28.0.2.0.2.1.3.2.1.5 norGwHwIfID | Leaf | Read | Display String | A textual string containing Interface Device ID |
| .28.0.2.0.2.1.3.2.1.6 norGwHwIfRevision | Leaf | Read | Integer | Interface Device revision number |
| .28.0.2.0.2.1.3.2.1.7 norGwHwIfState | Leaf | Read | Integer | Interface Device State:<br>1–Interface Device is in reset<br>2–Interface Device is UP and active<br>3–Interface Device is UP and in backup mode for active device<br>4–Interface Device is DOWN<br>5–Interface Device is under Test |

**Table 167 NT7X07AAHW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.0.2.1.3.2.1.8 norGwHwIfEEprom | Leaf | Read | Integer | EEPROM status of the Interface device:<br>1–EEPROM content is valid<br>2–EEPROM content is invalid<br>3–EEPROM is not needed |
| **.28.0.2.0.2.1.4 norGwHwMemory** (Note 2) | Node | None | None | This group provides memory usage information in the VxWorks target |
| .28.0.2.0.2.1.4.1 numBytesFree | Leaf | Read | Unsigned 32 | The number of bytes that are free in system memory |
| .28.0.2.0.2.1.4.2 numBlocksFree | Leaf | Read | Unsigned 32 | The number of blocks that are free in system memory |
| .28.0.2.0.2.1.4.3 avgBlockSizeFree | Leaf | Read | Unsigned 32 | The average block size that is free in system memory |
| .28.0.2.0.2.1.4.4 maxBlockSizeFree | Leaf | Read | Unsigned 32 | The largest block size that is free in system memory |
| .28.0.2.0.2.1.4.5 numBytesAlloc | Leaf | Read | Unsigned 32 | The number of bytes of system memory that are currently allocated by tasks and system services |
| .28.0.2.0.2.1.4.6 numBlocksAlloc | Leaf | Read | Unsigned 32 | The number of system memory blocks that are currently allocated in the system |
| .28.0.2.0.2.1.4.7 avgBlockSizeAlloc | Leaf | Read | Unsigned 32 | The average memory block size allocated in the system |
| ***Note 1:*** The norGwHwIfTable displays the state of the Ethernet interfaces and shows which interface is active. This table also displays information on the 7X07's DS1 and ATM interfaces that are unused and held in a reset condition.<br>***Note 2:*** The norHwGwMemory group displays useful information on 7X07 memory usage and allocation. | | | | |

## AUDIOCODE.MIB

Table 168 lists the OIDs in the AUDIOCODE.MIB. This MIB provides some user configuration of the Gateway's DSP voice packetizer operation. The most useful control is provided for the jitter buffer and vocoder gain settings. Some of the items managed by this MIB are overridden by Gateway call processing as noted in Table 168.

**Table 168 AUDIOCODE.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.1.5 gwIPCxVocoderMIB** | Node | None | None | |
| **.28.0.2.1.5.1 gwIPCxVocoderGeneral** | Node | None | None | This group provides DSP control setting & visibility |
| .28.0.2.1.5.1.1 gwIPCxVCvoiceVolume | Leaf | Read Write | Integer | Voice volume 0 to 63, 32=0dB. The default setting is 32. Sets the voice decoder's output gain. |
| .28.0.2.1.5.1.2 gwIPCxVCinputGain | Leaf | Read Write | Integer | Input Gain 0 to 63, 32=0dB. The default setting is 32. Sets the voice encoder's input gain. |
| .28.0.2.1.5.1.3 gwIPCxVCdefaultCoder | Leaf | Read Write | Integer | Default Vocoder Type, 32 settings:<br>G711Alaw_64 = 0<br>G711Mulaw_64 = 1<br>G729 = 17<br>Invalid #s: 19, 20, 21, 23, 24<br><br>***Note:*** This parameter is not used by the Gateway. The vocoder (codec) used for voice processing is determined by CM datafill. |
| .28.0.2.1.5.1.4 gwIPCxVCframesPerPacket | Leaf | Read Write | Integer | Number of frames per packet. The default setting is 2.<br><br>***Note:*** This parameter is not used by the Gateway. The number of speech frames per packet is fixed at 2. |
| .28.0.2.1.5.1.5 gwIPCxVCechoCancelEnabled | Leaf | Read Write | Integer | Echo Cancellation–enabled by default:<br>0–Disabled<br>1–Enabled |
| .28.0.2.1.5.1.6 gwIPCxVChighPassFilter | Leaf | Read Write | Integer | High Pass Filter–enabled by default:<br>0–Disabled<br>1–Enabled |
| .28.0.2.1.5.1.7 gwIPCxVCpostFilter | Leaf | Read Write | Integer | Post Filter–enabled by default:<br>0–Disabled<br>1–Enabled |
| .28.0.2.1.5.1.8 gwIPCxVCsilenceCompression | Leaf | Read Write | Integer | Silence Compression–enabled by default:<br>0–Disabled<br>1–Enabled<br><br>***Note:*** This parameter is not used by the Gateway. It is overridden by CM datafill. |

**Table 168 AUDIOCODE.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.1.5.2 gwIPCxVocoderJitter** | Node | None | None | |
| .28.0.2.1.5.2.1 gwIPCxVCdJBufMinDelay | Leaf | Read Write | Integer | Jitter Buffer Min Delay (ms). Range is 0 to 150 ms. The default setting is 20. |
| .28.0.2.1.5.2.2 gwIPCxVCdJBufMaxDelay | Leaf | Read Write | Integer | Jitter Buffer Max Delay (ms). Range is 0 to 150 ms. The default setting is 100. |
| .28.0.2.1.5.2.3 gwIPCxVCdJBufOptFactor | Leaf | Read Write | Integer | Dynamic Jitter Buffer Frame/Error/Delay Optimization Factor. Range is 0 to 12. The default setting is 7. |
| **.28.0.2.1.5.3 gwIPCxVocoderDtmf** | Node | None | None | |
| .28.0.2.1.5.3.1 gwIPCxVCdTMFTransportType | Leaf | Read | Integer | DTMF Transport type–TransparentDTMF by default:<br>0–MuteDTMF<br>1–RelayDTMF<br>2–TransparentDTMF<br><br>***Note:*** This parameter is not used by TOPS-IP Gateway applications. |
| .28.0.2.1.5.3.2 gwIPCxVCdTMFVolume | Leaf | Read Write | Integer | DTMF Volume. Range is 0 to 31, 31 = 0dBm. The default setting is 24.<br><br>***Note:*** This parameter is not used by TOPS-IP Gateway applications. |
| **.28.0.2.1.5.4 gwIPCxVocoderAdmin** | Node | None | None | |
| .28.0.2.1.5.4.1 gwIPCxVCloadOnReboot | Leaf | Read Write | Integer | Which vocoder values to load on reboot. The default setting is 0.<br>0–default<br>1–custom |
| .28.0.2.1.5.4.2 gwIPCxVClastCustomSave | Leaf | Read | Display String | Date and time of last time custom Vocoder values were saved |
| .28.0.2.1.5.4.3 gwIPCxVCsaveCustomValues | Leaf | Read Write | Integer | Save Custom values so that they will persist across reboots and software upgrades. This variable triggers an action, has no default and will always read 0.<br>0–noAction<br>1–save |
| .28.0.2.1.5.4.4 gwIPCxVCresetToDefault | Leaf | Read Write | Integer | Reset vocoder values to default settings. This variable triggers an action, has no default and will always read 0.<br>0–noAction<br>1–save |

### Additional information on AUDIOCODE.MIB

Please note the following information:

- Adjustments to the performance of the Gateway's jitter buffer are possible by changing the values of gwIPCxVCdJBufMinDelay, gwIPCxVCdJBufMaxDelay, and gwIPCxVCdJBufOptFactor. The jitter buffer's minimum delay defaults to 20 ms, the maximum delay defaults to 100 ms, and the optimization factor defaults to 7.

  The minimum jitter buffer delay, gwIPCxVCdJBufMinDelay, determines the minimum speech path delay induced by the jitter buffer. Setting this bound too low in order to minimize delay can result in degraded speech quality due to increased speech packet loss.

  The maximum jitter buffer delay, gwIPCxVCdJBufMaxDelay, determines the maximum amount of network jitter that can occur without speech packet loss. When network jitter exceeds this bound, packet loss occurs and speech quality degrades. Note that setting this bound too high in a high jitter network can result in excessive speech path delays.

  The jitter buffer optimization factor, gwIPCxVCdJBufOptFactor, controls how the dynamic jitter buffer algorithm trades off added delay and packet loss. A low value for optimization factor (range is 0 to 12) results in minimum delay through the jitter buffer, but at increased risk of packet loss. A high value for optimization factor results in minimum packet loss, but higher speech path delay is induced by the jitter buffer.

- Changes to the writable variables in the AUDIOCODE.MIB result in temporary settings that will be lost over any type of Gateway reboot. Set gwIPCxVClastCustomSave to a value of "save" to cause their settings to persist across a Gateway reboot. Once this has been done, these settings will survive a Gateway reboot, PMRESET, or even a software upgrade. However, they are reset to default values if the 7X07 pack is reseated. The default values can be restored without a reboot by setting the gwIPCxVCresetToDefault variable to a value of "save."

## TOPSIPGW.MIB

Table 169 lists the OIDs in the TOPSIPGW.MIB. This MIB provides TOPS-specific information on ISUP, IGIP, H.225, and H.245 call signaling, as well as more general Gateway information. This MIB also provides the following:

- Gateway loadname, maintenance state, and current time
- DHCP and boothost information
- SNMP access for the Gateway log and exception (trap) tables
- Gateway task and resource pool information in table form
- Trap notifications of Gateway logs, exceptions, and in-service/busy maintenance state transitions

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.4 gwTOPS** | Node | None | None | |
| **.28.0.2.4.1 gwTOPSMIB** | Node | None | None | |
| **.28.0.2.4.2 nnTgwCallpAgents** | Node | None | None | This node is parent to the MIB's call agent groups |
| **.28.0.2.4.2.1 nnTgwCallAgentISUP** | Node | None | None | This node is parent to the ISUP messaging stats group |
| **.28.0.2.4.2.1.1 nnTgwISUPMsgStats** | Node | None | None | The ISUP messaging stats group |
| .28.0.2.4.2.1.1.1 nnTgwISUPMsgInIAM | Leaf | Read | Counter | The number of incoming ISUP IAM messages |
| .28.0.2.4.2.1.1.2 nnTgwISUPMsgInACM | Leaf | Read | Counter | The number of incoming ISUP ACM messages |
| .28.0.2.4.2.1.1.3 nnTgwISUPMsgInANM | Leaf | Read | Counter | The number of incoming ISUP ANM messages |
| .28.0.2.4.2.1.1.4 nnTgwISUPMsgInREL | Leaf | Read | Counter | The number of incoming ISUP REL messages |
| .28.0.2.4.2.1.1.5 nnTgwISUPMsgInRLC | Leaf | Read | Counter | The number of incoming ISUP RLC messages |
| .28.0.2.4.2.1.1.6 nnTgwISUPMsgInRSC | Leaf | Read | Counter | The number of incoming ISUP RSC messages |
| .28.0.2.4.2.1.1.7 nnTgwISUPMsgInUnknown | Leaf | Read | Counter | The number of incoming ISUP messages of unknown type |
| .28.0.2.4.2.1.1.8 nnTgwISUPMsgOutIAM | Leaf | Read | Counter | The number of outgoing ISUP IAM messages |
| .28.0.2.4.2.1.1.9 nnTgwISUPMsgOutACM | Leaf | Read | Counter | The number of outgoing ISUP ACM messages |
| .28.0.2.4.2.1.1.10 nnTgwISUPMsgOutANM | Leaf | Read | Counter | The number of outgoing ISUP ANM messages |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.2.1.1.11 nnTgwISUPMsgOutREL | Leaf | Read | Counter | The number of outgoing ISUP REL messages |
| .28.0.2.4.2.1.1.12 nnTgwISUPMsgOutRLC | Leaf | Read | Counter | The number of outgoing ISUP RLC messages |
| .28.0.2.4.2.1.1.13 nnTgwISUPMsgOutRSC | Leaf | Read | Counter | The number of outgoing ISUP RSC messages |
| .28.0.2.4.2.1.1.14 nnTgwISUPMsgOutUnknown | Leaf | Read | Counter | The number of outgoing ISUP messages of unknown type |
| **.28.0.2.4.2.2 nnTgwCallAgentIGIP** | Node | None | None | This node is parent to the IGIP messaging stats group |
| **.28.0.2.4.2.2.1 nnTgwIGIPMsgStats** | Node | None | None | The IGIP messaging stats group |
| .28.0.2.4.2.2.1.1 nnTgwIGIPMsgInSetup | Leaf | Read | Counter | The number of incoming IGIP Setup messages |
| .28.0.2.4.2.2.1.2 nnTgwIGIPMsgInAlerting | Leaf | Read | Counter | The number of incoming IGIP Alerting messages |
| .28.0.2.4.2.2.1.3 nnTgwIGIPMsgInConnect | Leaf | Read | Counter | The number of incoming IGIP Connect messages |
| .28.0.2.4.2.2.1.4 nnTgwIGIPMsgInRelComp | Leaf | Read | Counter | The number of incoming IGIP Release Complete messages |
| .28.0.2.4.2.2.1.5 nnTgwIGIPMsgInUnknown | Leaf | Read | Counter | The number of incoming IGIP messages of unknown type |
| .28.0.2.4.2.2.1.6 nnTgwIGIPMsgOutSetup | Leaf | Read | Counter | The number of outgoing IGIP Setup messages |
| .28.0.2.4.2.2.1.7 nnTgwIGIPMsgOutAlerting | Leaf | Read | Counter | The number of outgoing IGIP Alerting messages |
| .28.0.2.4.2.2.1.8 nnTgwIGIPMsgOutConnect | Leaf | Read | Counter | The number of outgoing IGIP Connect messages |
| .28.0.2.4.2.2.1.9 nnTgwIGIPMsgOutRelComp | Leaf | Read | Counter | The number of outgoing IGIP Release Complete messages |
| .28.0.2.4.2.2.1.10 nnTgwIGIPMsgOutUnknown | Leaf | Read | Counter | The number of outgoing IGIP messages of unknown type. |
| **.28.0.2.4.2.2.2 nnTgwIGIPSockStats** | Node | None | None | The IGIP socket stats group |
| .28.0.2.4.2.2.2.1 nnTgwIGIPSockConnectAtt | Leaf | Read | Counter | The number of IGIP connect attempts |
| .28.0.2.4.2.2.2.2 nnTgwIGIPSockConnectSucc | Leaf | Read | Counter | The number of successful IGIP connects |
| .28.0.2.4.2.2.2.3 nnTgwIGIPSockConnectFail | Leaf | Read | Counter | The number of failed IGIP connects |
| **.28.0.2.4.2.3 nnTgwCallAgentH323** | Node | None | None | This node is parent to the H.323 messaging stats groups |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.4.2.3.1 nnTgwH225MsgStats** | Node | None | None | The H.225 messaging stats group |
| .28.0.2.4.2.3.1.1 nnTgwH225MsgInAlerting | Leaf | Read | Counter | The number of incoming H.225 Alerting messages |
| .28.0.2.4.2.3.1.2 nnTgwH225MsgInProceeding | Leaf | Read | Counter | The number of incoming H.225 Call Proceeding messages |
| .28.0.2.4.2.3.1.3 nnTgwH225MsgInConnect | Leaf | Read | Counter | The number of incoming H.225 Connect messages |
| .28.0.2.4.2.3.1.4 nnTgwH225MsgInFacility | Leaf | Read | Counter | The number of incoming H.225 Facility messages |
| .28.0.2.4.2.3.1.5 nnTgwH225MsgInUserInfo | Leaf | Read | Counter | The number of incoming H.225 User Information messages |
| .28.0.2.4.2.3.1.6 nnTgwH225MsgInRLC | Leaf | Read | Counter | The number of incoming H.225 Release Complete messages |
| .28.0.2.4.2.3.1.7 nnTgwH225MsgInSetup | Leaf | Read | Counter | The number of incoming H.225 Setup messages |
| .28.0.2.4.2.3.1.8 nnTgwH225MsgInUnknown | Leaf | Read | Counter | The number of incoming H.225 messages of unknown type. |
| .28.0.2.4.2.3.1.9 nnTgwH225MsgOutAlerting | Leaf | Read | Counter | The number of outgoing H.225 Alerting messages |
| .28.0.2.4.2.3.1.10 nnTgwH225MsgOutProceeding | Leaf | Read | Counter | The number of outgoing H.225 Call Proceeding messages |
| .28.0.2.4.2.3.1.11 nnTgwH225MsgOutConnect | Leaf | Read | Counter | The number of outgoing H.225 Connect messages |
| .28.0.2.4.2.3.1.12 nnTgwH225MsgOutFacility | Leaf | Read | Counter | The number of outgoing H.225 Facility messages |
| .28.0.2.4.2.3.1.13 nnTgwH225MsgOutUserInfo | Leaf | Read | Counter | The number of outgoing H.225 User Information messages |
| .28.0.2.4.2.3.1.14 nnTgwH225MsgOutRLC | Leaf | Read | Counter | The number of outgoing H.225 Release Complete messages |
| .28.0.2.4.2.3.1.15 nnTgwH225MsgOutSetup | Leaf | Read | Counter | The number of outgoing H.225 Setup messages |
| .28.0.2.4.2.3.1.16 nnTgwH225MsgOutUnknown | Leaf | Read | Counter | The number of outgoing H.225 messages of unknown type |
| **.28.0.2.4.2.3.2 nnTgwH225RASStats** | Node | None | None | The H.225 RAS message stats group |
| .28.0.2.4.2.3.2.1 nnTgwH225RASincoming | Leaf | Read | Counter | The number of incoming H.225 RAS messages |
| .28.0.2.4.2.3.2.2 nnTgwH225RASoutgoing | Leaf | Read | Counter | The number of outgoing H.225 RAS messages |
| **.28.0.2.4.2.3.3 nnTgwH245MsgStats** | Node | None | None | The H.245 messaging stats group |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.2.3.3.1 nnTgwH245MsgInDet | Leaf | Read | Counter | The number of incoming H.245 Determination messages |
| .28.0.2.4.2.3.3.2 nnTgwH245MsgInCapSet | Leaf | Read | Counter | The number of incoming H.245 Capability Set messages |
| .28.0.2.4.2.3.3.3 nnTgwH245MsgInOLC | Leaf | Read | Counter | The number of incoming H.245 Open Logical Channel messages |
| .28.0.2.4.2.3.3.4 nnTgwH245MsgInOLCAck | Leaf | Read | Counter | The number of incoming H.245 OLC Ack messages |
| .28.0.2.4.2.3.3.5 nnTgwH245MsgInOLCRej | Leaf | Read | Counter | The number of incoming H.245 OLC Reject messages |
| .28.0.2.4.2.3.3.6 nnTgwH245MsgInCLC | Leaf | Read | Counter | The number of incoming H.245 Close Logical Channel messages |
| .28.0.2.4.2.3.3.7 nnTgwH245MsgInCLCAck | Leaf | Read | Counter | The number of incoming H.245 CLC Ack messages |
| .28.0.2.4.2.3.3.8 nnTgwH245MsgInSendTerm CapSet | Leaf | Read | Counter | The number of incoming H.245 Send Term Capability Set messages |
| .28.0.2.4.2.3.3.9 nnTgwH245MsgInEndSession | Leaf | Read | Counter | The number of incoming H.245 EndSession messages |
| .28.0.2.4.2.3.3.10 nnTgwH245MsgInUnknown | Leaf | Read | Counter | The number of incoming H.245 messages of unknown type |
| .28.0.2.4.2.3.3.11 nnTgwH245MsgOutDet | Leaf | Read | Counter | The number of outgoing H.245 Determination messages |
| .28.0.2.4.2.3.3.12 nnTgwH245MsgOutCapSet | Leaf | Read | Counter | The number of outgoing H.245 Capability Set messages |
| .28.0.2.4.2.3.3.13 nnTgwH245MsgOutOLC | Leaf | Read | Counter | The number of outgoing H.245 Open Logical Channel messages |
| .28.0.2.4.2.3.3.14 nnTgwH245MsgOutOLCAck | Leaf | Read | Counter | The number of outgoing H.245 OLC Ack messages |
| .28.0.2.4.2.3.3.15 nnTgwH245MsgOutOLCRej | Leaf | Read | Counter | The number of outgoing H.245 OLC Reject messages |
| .28.0.2.4.2.3.3.16 nnTgwH245MsgOutCLC | Leaf | Read | Counter | The number of outgoing H.245 Close Logical Channel messages |
| .28.0.2.4.2.3.3.17 nnTgwH245MsgOutCLCAck | Leaf | Read | Counter | The number of outgoing H.245 CLC Ack messages |
| .28.0.2.4.2.3.3.18 nnTgwH245MsgOutSendTerm CapSet | Leaf | Read | Counter | The number of outgoing H.245 Send Term Capability Set messages |
| .28.0.2.4.2.3.3.19 nnTgwH245MsgOutEndSession | Leaf | Read | Counter | The number of outgoing H.245 EndSession messages |
| .28.0.2.4.2.3.3.20 nnTgwH245MsgOutUnknown | Leaf | Read | Counter | The number of outgoing H.245 messages of unknown type |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.4.2.3.4 nnTgwH323SockStats** | Node | None | None | The H.323 socket stats group |
| .28.0.2.4.2.3.4.1 nnTgwH323SockConnectAtt | Leaf | Read | Counter | The number of H.323 (H.225, H.245) connect attempts |
| .28.0.2.4.2.3.4.2 nnTgwH323SockConnectSucc | Leaf | Read | Counter | The number of successful H.323 (H.225, H.245) connects |
| .28.0.2.4.2.3.4.3 nnTgwH323SockConnectFail | Leaf | Read | Counter | The number of failed H.323 (H.225, H.245) connects |
| **.28.0.2.4.2.4 nnTgwCallAgentSummary** | Node | None | None | This node is parent to the Call Agent Summary table |
| **.28.0.2.4.2.4.1 nnTgwCaSummaryTable** | Node | None | None | This table summarizes the Gateway's call agent messaging totals |
| **.28.0.2.4.2.4.1.1 nnTgwCaEntry** | Node | None | None | A table entry containing messaging totals for a single Gateway call agent |
| .28.0.2.4.2.4.1.1.1 nnTgwCaIndex | Leaf | Read | Integer 32 | Table index, 1...n, where n is the number of Gateway call agents |
| .28.0.2.4.2.4.1.1.2 nnTgwCaName | Leaf | Read | Display String | The name of an individual Gateway call agent |
| .28.0.2.4.2.4.1.1.3 nnTgwCaTotalMsgsIn | Leaf | Read | Integer 32 | The total number of incoming messages for this call agent |
| .28.0.2.4.2.4.1.1.4 nnTgwCaTotalMsgsOut | Leaf | Read | Integer 32 | The total number of outgoing messages for this call agent |
| .28.0.2.4.2.4.1.1.5 nnTgwCaPercentMsgs | Leaf | Read | Integer | This call agent's percentage of the total message count |
| **.28.0.2.4.3 nnTgwSystem** | Node | None | None | The System group for the TOPS Gateway |
| .28.0.2.4.3.1 nnTgwReboot | Leaf | Read Write | Integer | Reboot the Gateway card immediately. This variable triggers an action, has no default and will always read 0.<br>0–noAction<br>1–reboot |
| .28.0.2.4.3.2 nnTgwClearSwLogs | Leaf | Read Write | Integer | Clears the Gateway log buffer. Note: This variable triggers an action, has no default and will always read 0.<br>0–noAction<br>1–clear |
| .28.0.2.4.3.3 nnTgwClearSwTraps | Leaf | Read Write | Integer | Clears the Gateway trap buffer.Note: This variable triggers an action, has no default and will always read 0.<br>0–noAction<br>1–clear |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.3.4<br>nnTgwSwLogThresh | Leaf | Read<br>Write | Integer | The number of logs per 15-minute period at which the Gateway temporarily suspends sending log notifications. Range is 0 to 30. The default setting is 15.<br><br>***Note:*** A threshold of 0 disables log notifications. |
| .28.0.2.4.3.5<br>nnTgwSwTrapThresh | Leaf | Read<br>Write | Integer | The number of traps per 15-minute period at which the Gateway temporarily suspends sending trap (exception) notifications. Range is 0 to 30. The default setting is 15.<br><br>***Note:*** A threshold of 0 disables trap notifications. |
| .28.0.2.4.3.6<br>nnTgwDtmfInterDigitTime | Leaf | Read<br>Write | Integer | The interdigit time for DTMF generated by the Gateway. Range is 10 to 250 ms. The default setting is 10.<br><br>***Note:*** This parameter is not used by TOPS-IP Gateway applications. |
| .28.0.2.4.3.7<br>nnTgwDtmfVolume | Leaf | Read<br>Write | Integer | The power level in -dBm of DTMF generated by the Gateway. Range is 0 to 31. 31 = 0dBm. The default setting is 24 which corresponds to -7 dBm.<br><br>***Note:*** This parameter is not used by TOPS-IP Gateway applications. |
| .28.0.2.4.3.8<br>nnTgwClearCAStats | Leaf | Read<br>Write | Integer | Clear all call agent messaging stats on the Gateway.<br>0–noAction<br>1–set<br><br>***Note:*** This variable triggers an action, has no default, and will always read 0. |
| **.28.0.2.4.3.9**<br>**nnTgwLogTable** | Node | None | None | This table contains the current Gateway logs |
| **.28.0.2.4.3.9.1**<br>**nnTgwLogTabEntry** | Node | None | None | A table entry containing a single Gateway log |
| .28.0.2.4.3.9.1.1<br>nnTgwLogIndex | Leaf | Read | Integer 32 | Table index, 1...n, where n is the number of logs in the table |
| .28.0.2.4.3.9.1.2<br>nnTgwSysName | Leaf | Read | Display String | The system name of the Gateway issuing a log<br><br>***Note:*** This name is taken from the RFC1213 MIB's System group sysName variable. |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.3.9.1.3<br>nnTgwLogType | Leaf | Read | Integer | The type of log:<br>0–swerr<br>1–info<br>2–note |
| .28.0.2.4.3.9.1.4<br>nnTgwLogTimeStamp | Leaf | Read | Display String | The timestamp of the log |
| .28.0.2.4.3.9.1.5<br>nnTgwTask | Leaf | Read | Display String | The name of the task producing the log |
| .28.0.2.4.3.9.1.6<br>nnTgwLogText | Leaf | Read | Display String | A text description of this log |
| .28.0.2.4.3.9.1.7<br>nnTgwLogTraceback | Leaf | Read | Display String | The function traceback for this log |
| **.28.0.2.4.3.10<br>nnTgwExcTable** | Node | None | None | This table contains the current Gateway exceptions (traps) |
| **.28.0.2.4.3.10.1<br>nnTgwExcTabEntry** | Node | None | None | A table entry containing a single Gateway trap |
| .28.0.2.4.3.10.1.1<br>nnTgwExcIndex | Leaf | Read | Integer 32 | Table index, 1...n, where n is the number of traps in the table |
| .28.0.2.4.3.10.1.2<br>nnTgwExcSysName | Leaf | Read | Display String | The system name of the Gateway issuing a trap<br><br>***Note:*** This name is taken from the RFC1213 MIB's System group sysName variable. |
| .28.0.2.4.3.10.1.3<br>nnTgwExcTimeStamp | Leaf | Read | Display String | The timestamp of the trap |
| .28.0.2.4.3.10.1.4<br>nnTgwExcTask | Leaf | Read | Display String | The name of the task producing the trap |
| .28.0.2.4.3.10.1.5<br>nnTgwExcVecNum | Leaf | Read | Integer 32 | The exception vector number of the trap |
| .28.0.2.4.3.10.1.6<br>nnTgwExcPC | Leaf | Read | Display String | The Program Counter of the task producing the trap |
| .28.0.2.4.3.10.1.7<br>nnTgwExcMSR | Leaf | Read | Display String | The Machine State Register of the task producing the trap |
| .28.0.2.4.3.10.1.8<br>nnTgwExcCR | Leaf | Read | Display String | The Condition Register of the task producing the trap |
| .28.0.2.4.3.10.1.9<br>nnTgwExcTraceback | Leaf | Read | Display String | The function traceback for this trap |
| **.28.0.2.4.3.11<br>nnTgwMtcInfo** | Node | None | None | The Maintenance Info group |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.3.11.1<br>nnTgwStatus | Leaf | Read | Display String | The sparing status of the Gateway (Primary, Spare, Nil)<br><br>***Note:*** Gateway sparing is not supported, so Primary is the only sparing status reported by the Gateway. |
| .28.0.2.4.3.11.2<br>nnTgwState | Leaf | Read | Display String | The current maintenance state of the Gateway. The possible states are:<br>Reset Booting<br>ROM Critical Fail 1<br>ROM Critical Fail 2<br>ROM Critical Fail 3<br>Offline<br>Busy<br>In-Service<br>Reserved<br>Unknown |
| .28.0.2.4.3.11.3<br>nnTgwLogNodeNum | Leaf | Read | Integer 32 | The logical node number of the Gateway |
| .28.0.2.4.3.11.4<br>nnTgwPhysNodeNum | Leaf | Read | Integer 32 | The physical node number of the Gateway |
| .28.0.2.4.3.11.5<br>nnTgwVariant | Leaf | Read | Integer 32 | The type of Gateway (Toll Bypass, Centrex IP, TOPS) |
| .28.0.2.4.3.11.6<br>nnTgwAppVersion | Leaf | Read | Display String | The software version of the Gateway |
| .28.0.2.4.3.11.7<br>nnTgwBSPVersion | Leaf | Read | Display String | The BSP software version of the Gateway |
| .28.0.2.4.3.11.8<br>nnTgwCurrentTime | Leaf | Read | Display String | The current time on the Gateway |
| .28.0.2.4.3.11.9<br>nnTgwCmBcsRelease | Leaf | Read | Integer 32 | The CM BCS Release number |
| .28.0.2.4.3.11.10<br>nnTgwXpmBcsRelease | Leaf | Read | Integer 32 | The XPM BCS Release number |
| .28.0.2.4.3.11.11<br>nnTgwHdlcLinkState | Leaf | Read | Display String | The state of the XPM-GW HDLC link |
| .28.0.2.4.3.11.12<br>nnTgwFpgaVersion | Leaf | Read | Display String | The version of the Gateway FPGA |
| .28.0.2.4.3.11.13<br>nnTgwBootRomVer0 | Leaf | Read | Display String | The version of the Gateway BootRom 0 |
| .28.0.2.4.3.11.14<br>nnTgwBootRomVer1 | Leaf | Read | Display String | The version of the Gateway BootRom 1 |
| **.28.0.2.4.3.12<br>nnTgwDhcpInfo** | Node | None | None | The DHCP Info group |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.3.12.1<br>nnTgwBootFile | Leaf | Read | Display String | The name of this Gateway's boot file |
| .28.0.2.4.3.12.2<br>nnTgwDhcpClient | Leaf | Read | Display String | The DHCP client name of this Gateway |
| .28.0.2.4.3.12.3<br>nnTgwDnsDomain | Leaf | Read | Display String | The DNS domain name in which this Gateway resides |
| .28.0.2.4.3.12.4<br>nnTgwDhcpServerIpAddr | Leaf | Read | IP Address | The IP address of this Gateway's DHCP Server |
| **.28.0.2.4.3.13<br>nnTgwHostInfo** | Node | None | None | The Host Info group |
| .28.0.2.4.3.13.1<br>nnTgwVxTargetIpAddr | Leaf | Read | IP Address | The IP address of this TOPS-IP Gateway |
| .28.0.2.4.3.13.2<br>nnTgwLocalHostIpAddr | Leaf | Read | IP Address | The loopback IP address of the local host |
| .28.0.2.4.3.13.3<br>nnTgwBootHostIpAddr | Leaf | Read | IP Address | The IP address of the boot host for this TOPS-IP Gateway |
| **.28.0.2.4.3.14<br>nnTgwNotifications** | Node | None | None | SNMP trap definitions |
| .28.0.2.4.3.14.1<br>nnTgwNSysName | Leaf | Notification Element | Display String | The system name of the Gateway issuing a log<br><br>***Note:*** This name is taken from the RFC1213 MIB's System group sysName variable. |
| .28.0.2.4.3.14.2<br>nnTgwNLogType | Leaf | Notification Element | Integer | The type of log:<br>0–swerr<br>1–info<br>2–note |
| .28.0.2.4.3.14.3<br>nnTgwNTimeStamp | Leaf | Notification Element | Display String | The timestamp of the log |
| .28.0.2.4.3.14.4<br>nnTgwNTask | Leaf | Notification Element | Display String | The name of the task producing the log |
| .28.0.2.4.3.14.5<br>nnTgwNLogText | Leaf | Notification Element | Display String | A text description of this log |
| .28.0.2.4.3.14.6<br>nnTgwNTraceback | Leaf | Notification Element | Display String | The function traceback for this log |
| **.28.0.2.4.3.14.7<br>nnTgwLogNotification** | Node | Notification | | A Gateway log notification |
| .28.0.2.4.3.14.8<br>nnTgwNExcVecNum | Leaf | Notification Element | Integer 32 | The exception vector number of the trap |
| .28.0.2.4.3.14.9<br>nnTgwNExcPC | Leaf | Notification Element | Display String | The Program Counter of the task producing the trap |
| .28.0.2.4.3.14.10<br>nnTgwNExcMSR | Leaf | Notification Element | Display String | The Machine State Register of the task producing the trap |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.3.14.11 nnTgwNExcCR | Leaf | Notification Element | Display String | The Condition Register of the task producing the trap |
| **.28.0.2.4.3.14.12 nnTgwExcNotification** | Node | Notification | | A Gateway exception notification |
| **.28.0.2.4.3.14.13 nnTgwNodeBusy** | Node | Notification | | Indicates a Gateway transition to a busy state. The corresponding DMS map states are ManB or SysB. |
| **.28.0.2.4.3.14.14 nnTgwNodeInservice** | Node | Notification | | Indicates a Gateway transition to an inservice state. The corresponding DMS MAP state is InSv. |
| **.28.0.2.4.4 nnTgwPerformance** | Node | None | None | This node is parent to the Gateway performance groups |
| **.28.0.2.4.4.1 nnTgwMsgQStats** | Node | None | None | The Message Queue stats group |
| .28.0.2.4.4.1.1 nnTgwMsgQCallpCurrent | Leaf | Read | Integer | The current number of messages in the call processing queue. Range is 0 to 120. |
| .28.0.2.4.4.1.2 nnTgwMsgQCallpHighWater | Leaf | Read | Integer | The highest number of messages in the call processing queue. Range is 0 to 120. |
| **.28.0.2.4.4.2 nnTgwTaskSummary** | Node | None | None | This node is parent to the Task Summary table |
| **.28.0.2.4.4.2.1 nnTgwTaskSummaryTable** | Node | None | None | This table contains information on all tasks in the Gateway |
| **.28.0.2.4.4.2.1.1 nnTgwTaskSummEntry** | Node | None | None | A table entry containing info on a single Gateway task |
| .28.0.2.4.4.2.1.1.1 nnTgwTaskIndex | Leaf | Read | Integer 32 | Table index, 1...n, where n is the number of tasks in the Gateway |
| .28.0.2.4.4.2.1.1.2 nnTgwTaskName | Leaf | Read | Display String | The name of an individual Gateway task |
| .28.0.2.4.4.2.1.1.3 nnTgwTaskCode | Leaf | Read | Display String | The task entry |
| .28.0.2.4.4.2.1.1.4 nnTgwTaskId | Leaf | Read | Display String | The task ID number |
| .28.0.2.4.4.2.1.1.5 nnTgwTaskPrio | Leaf | Read | Integer 32 | The task priority |
| .28.0.2.4.4.2.1.1.6 nnTgwTaskStatus | Leaf | Read | Display String | The task status |
| .28.0.2.4.4.2.1.1.7 nnTgwTaskPC | Leaf | Read | Display String | The task program counter |
| .28.0.2.4.4.2.1.1.8 nnTgwTaskSP | Leaf | Read | Display String | The task stack pointer |

**Table 169 TOPSIPGW.MIB description**

| OID and name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.4.2.1.1.9 nnTgwTaskErrno | Leaf | Read | Display String | The task error number |
| .28.0.2.4.4.2.1.1.10 nnTgwTaskDelay | Leaf | Read | Integer 32 | The task delay |
| **.28.0.2.4.4.3 nnTgwResourcePool** | Node | None | None | This node is parent to the Resource Pool table |
| **.28.0.2.4.4.3.1 nnTgwResPoolTable** | Node | None | None | This table contains information about various Gateway resources |
| **.28.0.2.4.4.3.1.1 nnTgwResourceEntry** | Node | None | None | A table entry containing info on a single Gateway resource |
| .28.0.2.4.4.3.1.1.1 nnTgwResIndex | Leaf | Read | Integer 32 | Table index, 1...n, where n is the number of resources in the table |
| .28.0.2.4.4.3.1.1.2 nnTgwResType | Leaf | Read | Display String | The name of an individual Gateway resource |
| .28.0.2.4.4.3.1.1.3 nnTgwResAvail | Leaf | Read | Integer 32 | The available instances of a Gateway resource type |
| .28.0.2.4.4.3.1.1.4 nnTgwResInUse | Leaf | Read | Integer 32 | The instances currently in use of a Gateway resource type |
| .28.0.2.4.4.3.1.1.5 nnTgwResHighWater | Leaf | Read | Integer 32 | The high water mark usage of a Gateway resource type |
| .28.0.2.4.4.3.1.1.6 nnTgwResPercentUsed | Leaf | Read | Integer | The percentage of a Gateway resource type currently in use |

### Additional information on TOPSIPGW.MIB

Please note the following information:

- All categories of messaging stats represent the Gateway's in-service totals that have accumulated from the time the Gateway came into service following the last reboot. The counters for each message type increment up to a maximum count of 4,294,967,295 before rolling over to 0. After roll-over, the count continues to increment from 0.
- The messaging stats for the nnTgwISUPMsgStats group apply to both OC-IP and IP Position calls.
- The messaging stats for the nnTgwIGIPMsgStats group only apply to OC-IP calls.
- The messaging stats for the nnTgwH225MsgStats and nnTgwH245MsgStats groups only apply to IP Position calls.

- The incoming messaging stats for the nnTgwH225RASStats group will peg when another node in the network specifically directs RAS messages intended for a Gatekeeper to the TOPS Gateway. This will happen if another node is mistakenly configured to consider the TOPS Gateway to be it's Gatekeeper. This group will not peg incoming RAS messages when routine Gatekeeper discovery messages (GRQ) are received by the TOPS Gateway.
- When the nnTgwSystem group's nnTgwReboot variable is set to 1 (reboot), the SNMP manager will see a timeout occur since the Gateway is immediately rebooted and does not send a response. Note that an SNMP reboot is not the preferred way to reboot a Gateway. The preferred method is to use the DMS MAP interface to drain calls from a Gateway before issuing a PMRESET command at the MAP to reboot the Gateway. The SNMP reboot option is provided to give network administrators a way to recover a Gateway. It is acceptable to do an SNMP reboot of a Gateway that is in a MANB (busy) state at the DMS MAP.
- The writable variables in this MIB produce a Gateway log when they are changed. The value of these variables will survive a Gateway reboot, PMRESET or even a software upgrade. However, they are reset to default values if the 7X07 pack is reseated.
- The nnTgwSystem group's nnTgwSwLogThresh and nnTgwSwTrapThresh variables can be set to 0 to disable SNMP trap notifications of Gateway logs and exceptions. Other values affect the threshold at which these notifications are suspended during a 15-minute period.
- The system name used in the log and exception tables and in the log and trap notifications is the name maintained in the RFC1213 System group's sysName variable. The default value is "vxTarget" which is a default provided by the Gateway's VxWorks operating system. This variable, as well as sysContact and sysLocation are writable variables that can be set to appropriate values by a network administrator.
- All of the trap notifications defined in this MIB will be sent to the default SNMP management node and any additional SNMP management nodes configured through the Gateway's PMDEBUG SNMP COnfigmgrs interface.

## TOPSQOS.MIB

The TOPSQOS.MIB displays QoS information for the Gateway in nnTgwQosCumulativeTable. This MIB also defines trap notifications that are sent to SNMP management nodes when a call ends with one or more of the QoS metrics exceeding a specified threshold. The supported metrics are average roundtrip network latency, highest average roundtrip network latency, average jitter, highest average jitter, and percent packet loss.

The QosCumulative table defines 10 cells (rows) for each QoS metric. The number in each cell represents the number of calls whose calculated metric value at call end falls within the cell boundaries. The cell boundaries (base, width) are set for each metric via the nnTgwQosCumSettings group. The default values for each metric's cell bounds are given in the OID table.

Table 170 shows an example of the QoS table layout. Using the base and width values given in the column heading for average network latency, cell1 represents from 0-24 ms of latency, cell2 from 25-49ms and on up to 225-249ms for cell10. When a call ends, the average roundtrip network latency is computed and the appropriate cell count is incremented by 1.

In this example, if the computed average roundtrip network latency at call end is 85ms, then the count for cell4 is incremented. If the highest average roundtrip network latency seen during this call was 190ms, then the count for cell8 for this metric is incremented. The jitter and packet loss metrics work in a similar fashion. The table's appearance is determined by the SNMP tools used to display the table and does not include the metric base and width settings.

**Table 170 Example QoS table**

| **Cell index** | **Average latency**<br>Base=0 ms<br>Width=25 ms | **High average latency**<br>Base=0 ms<br>Width=25 ms | **Average jitter**<br>Base=0 ms<br>Width=5 ms | **High average jitter**<br>Base=0 ms<br>Width=5 ms | **Percent packet loss**<br>Base=0%<br>Width=1% |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 276 | 7 | 30058 |
| 2 | 378 | 57 | 3428 | 1271 | 1245 |
| 3 | 8456 | 1699 | 3893 | 2287 | 4 |
| 4 | 15343 | 2076 | 2358 | 2665 | 0 |
| 5 | 6786 | 7986 | 4275 | 1822 | 3 |
| 6 | 223 | 879 | 8672 | 4554 | 0 |
| 7 | 67 | 6833 | 5674 | 6284 | 0 |
| 8 | 6 | 10093 | 547 | 9350 | 0 |
| 9 | 8 | 1006 | 601 | 2614 | 0 |
| 10 | 0 | 678 | 1583 | 453 | 0 |

The latency and jitter characteristics of a specific customer network may require that the metric base and width defaults be changed in order to better display the performance distribution of each QoS metric. The roundtrip network latency metrics are reported in milliseconds and computed using information in RTCP sender and receiver reports. These computed values only reflect roundtrip network latency and do not include any systemic DMS or Gateway latency. The jitter metrics are also reported in milliseconds and are computed per RFC1889 algorithm A.8 using information in RTCP receiver reports. The highest average latency and jitter metrics represent the highest values computed during a call.

The cell values accumulated in the QoS table are cumulative since the Gateway came in-service or since the table data was last cleared. Anytime the base or width setting for a QoS metric is changed or rewritten, the data in all 10 cells for that metric is reset to 0. The entire table can be cleared by rewriting the base value for each QoS metric in the nnTgwQosCumSettings group.

Table 171 lists the OIDs in the TOPSQOS.MIB.

**Table 171 TOPSQOS.MIB description**

| OID and Name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| **.28.0.2.4.4.4 gwTOPSQosMib** | Node | None | None | This MIB allows a TOPS-IP Gateway to provide QOS information to a network management node |
| **.28.0.2.4.4.4.1 nnTgwQosCumulative** | Node | None | None | |
| **.28.0.2.4.4.4.1.1 nnTgwQosCumulativeTable** | Node | None | None | This table contains the cumulative distribution of calls for each of five QoS metrics. The nnTgwQosCumSettings group contains the base and width variables that define the cells for each QoS metric. |
| **.28.0.2.4.4.4.1.1.1 nnTgwQosCumulativeEntry** | Node | None | None | |
| .28.0.2.4.4.4.1.1.1.1 nnTgwQosCumulativeIndex | Leaf | Read | Integer | The QosCumulative table index–identifies cells 1-10 |
| .28.0.2.4.4.4.1.1.1.2 nnTgwQosCumAvgLatency | Leaf | Read | Counter 32 | The number of calls with the average roundtrip network latency within the bounds of cells 1-10 |
| .28.0.2.4.4.4.1.1.1.3 nnTgwQosCumHiAvgLatency | Leaf | Read | Counter 32 | The number of calls with the highest average roundtrip network latency within the bounds of cells 1-10 |
| .28.0.2.4.4.4.1.1.1.4 nnTgwQosCumAvgJitter | Leaf | Read | Counter 32 | The number of calls with the average jitter within the bounds of cells 1-10 |
| .28.0.2.4.4.4.1.1.1.5 nnTgwQosCumHiAvgJitter | Leaf | Read | Counter 32 | The number of calls with the highest average jitter within the bounds of cells 1-10 |

**Table 171 TOPSQOS.MIB description**

| OID and Name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.4.4.1.1.1.6 nnTgwQosCumPacketLoss | Leaf | Read | Counter 32 | The number of calls with the percentage packet loss within the bounds of cells 1-10 |
| **.28.0.2.4.4.4.2 nnTgwQosCumSettings** | Node | None | None | |
| .28.0.2.4.4.4.2.1 nnTgwQosAvgLatencyBase | Leaf | Read Write | Integer | The cell base for the average roundtrip network latency distribution. The default setting is 0 ms. (See Note.) |
| .28.0.2.4.4.4.2.2 nnTgwQosAvgLatencyWidth | Leaf | Read Write | Integer | The cell width for the average roundtrip network latency distribution. The default setting is 50 ms. (See Note.) |
| .28.0.2.4.4.4.2.3 nnTgwQosHiAvgLatencyBase | Leaf | Read Write | Integer | The cell base for the highest average roundtrip network latency distribution. The default setting is 0 ms. (See Note.) |
| .28.0.2.4.4.4.2.4 nnTgwQosHiAvgLatencyWidth | Leaf | Read Write | Integer | The cell width for the highest average roundtrip network latency distribution. The default setting is 50 ms. (See Note.) |
| .28.0.2.4.4.4.2.5 nnTgwQosAvgJitterBase | Leaf | Read Write | Integer | The cell base for the average jitter distribution. The default setting is 0 ms. (See Note.) |
| .28.0.2.4.4.4.2.6 nnTgwQosAvgJitterWidth | Leaf | Read Write | Integer | The cell width for the average jitter distribution. The default setting is 5 ms. (See Note.) |
| .28.0.2.4.4.4.2.7 nnTgwQosHiAvgJitterBase | Leaf | Read Write | Integer | The cell base for the highest average jitter distribution. The default setting is 0 ms. (See Note.) |
| .28.0.2.4.4.4.2.8 nnTgwQosHiAvgJitterWidth | Leaf | Read Write | Integer | The cell width for the highest average jitter distribution. The default setting is 5 ms. (See Note.) |
| .28.0.2.4.4.4.2.9 nnTgwQosPacketLossBase | Leaf | Read Write | Integer | The cell base for the percent packet loss distribution. The default setting is 0%. (See Note.) |
| .28.0.2.4.4.4.2.10 nnTgwQosPacketLossWidth | Leaf | Read Write | Integer | The cell width for the percent packet loss distribution. The default setting is 1%. (See Note.) |
| **.28.0.2.4.4.4.3 nnTgwQosThresholds** | Node | None | None | |
| .28.0.2.4.4.4.3.1 nnTgwQosThresholdAverage Latency | Leaf | Read Write | Integer | The threshold value for average roundtrip network latency in milliseconds. The default setting is 250 ms. |
| .28.0.2.4.4.4.3.2 nnTgwQosThresholdHighest Latency | Leaf | Read Write | Integer | The threshold value for highest average roundtrip network latency in milliseconds. The default setting is 450 ms. |

**Table 171 TOPSQOS.MIB description**

| OID and Name | Type | Access | Syntax | Description |
|---|---|---|---|---|
| .28.0.2.4.4.4.3.3 nnTgwQosThresholdAverage Jitter | Leaf | Read Write | Integer | The threshold value for average jitter in milliseconds. The default setting is 50 ms. |
| .28.0.2.4.4.4.3.4 nnTgwQosThresholdHighestJitter | Leaf | Read Write | Integer | The threshold value for highest average jitter in milliseconds. The default setting is 70 ms. |
| .28.0.2.4.4.4.3.5 nnTgwQosThresholdAverage PacketLoss | Leaf | Read Write | Integer | The threshold value for packet loss in percent. The default setting is 4%. |
| .28.0.2.4.4.4.3.6 nnTgwQosThresholdsEnabled | Leaf | Read Write | Integer | The current state of threshold detection. When this is set to enabled, the QoS metrics are compared to the thresholds at the end of each call and an SNMP trap is generated if any of the thresholds are exceeded. The default setting is disabled:<br>1–enabled<br>2–disabled |
| **.28.0.2.4.4.4.4 nnTgwQosNotifications** | Node | None | None | |
| .28.0.2.4.4.4.4.1 nnTgwQosAverageLatency | Leaf | Notification Element | Integer | The average packet roundtrip network delay in milliseconds. This value is the average of all the latency values reported in RTCP Sender Reports during the entire call. |
| .28.0.2.4.4.4.4.2 nnTgwQosHighestLatency | Leaf | Notification Element | Integer | The highest average packet roundtrip network delay in milliseconds. This value is the highest latency value reported in RTCP Sender Reports during the entire call. |
| .28.0.2.4.4.4.4.3 nnTgwQosAverageJitter | Leaf | Notification Element | Integer | The average jitter in milliseconds. This value is the average of all the jitter values reported in RTCP Sender Reports during the entire call. |
| .28.0.2.4.4.4.4.4 nnTgwQosHighestJitter | Leaf | Notification Element | Integer | The highest average jitter in milliseconds. This value is the highest jitter value reported in RTCP Sender Reports during the entire call. |
| .28.0.2.4.4.4.4.5 nnTgwQosAveragePacketLoss | Leaf | Notification Element | Integer | The percentage of packets which are lost. This value is the number of packets lost during the entire call divided by the total number of packets expected during the entire call, expressed in percent. |
| .28.0.2.4.4.4.4.6 nnTgwQosRemoteAddress | Leaf | Notification Element | IP Address | Indicates the remote RTP transport address |
| **.28.0.2.4.4.4.4.7 nnTgwQosThreshold Exceeded** | Node | None | Notification | Signifies that a QoS threshold has been exceeded |
| ***Note:*** Setting this element also clears the ten associated cell counts. | | | | |

### Additional information on TOPSQOS.MIB

Please note the following information:

- To enable SNMP trap notification for calls exceeding QoS thresholds, set the nnTgwQosThresholdsEnabled variable to 1.
- The writable variables in this MIB produce a Gateway log when they are changed. The value of these variables will survive a Gateway reboot, PMRESET or even a software upgrade, but are reset to default values if the 7X07 pack is reseated.
- Since the Gateway's QoS software relies upon RTCP reports that are only issued periodically, large numbers of unusually short duration calls can reduce the accuracy of the reported latency and jitter.
- All of the trap notifications defined in this MIB will be sent to the default SNMP management node and any additional SNMP management nodes configured through the Gateway's PMDEBUG SNMP COnfigmgrs interface.

## SNMP security for the Gateway

Since the MIBs supported by the 7X07 Gateway card define a number of objects having write access, the Gateway provides additional security enhancements beyond the security features of SNMPv1 or SNMPv2.

This section describes the following SNMP security topics:

- Gateway access through Telnet
- Gateway password changes
- Gateway password resets
- Adding recognized SNMP network management nodes
- Disabling Set operations
- Source screening for Set operations
- Persistence of security configuration data
- Increased IP-XPM security through SNMP

### Gateway access through Telnet

The Gateway supports access through Telnet, which is present and enabled on deployed 7X07AAs. As of SN09, Telnet may be disabled using an office parameter in Table OFCENG.

***Note:*** Telnet on a 7X07AA is always disabled following an upgrade from a pre-SN09 (TOPS22) load to an SN09 or higher load.

The only reasons to access the Gateway through Telnet are:

- to change the default Gateway Telnet password (page 561)

- to configure the Gateway to recognize additional SNMP network managers beyond the one manager that can now be distilled in the core (IPGW_SNMP_MANAGER) (page 564)
- to change the SNMP security settings (page 566)

### Draining and busying the Gateway card

Telnet access should *only* be performed when the Gateway is not in an in-service state. The following steps describe how to take the Gateway out of service at the DMS MAP:

1 Enter the MAPCI;MTC;PM level.

2 Post the Gateway by typing: POST IPGW <IPNO> (IPNO field datafilled in table IPINV for the Gateway). For example, `POST IPGW TGWY 10 3`.

3 Issue the BSY DRAIN command. Draining allows calls in progress on a Gateway to remain up until completion, while preventing future call origination.

4 After draining, the Gateway transitions to a MANB state at the MAP.

***Note:*** For more information on the IPGW level and other Gateway maintenance, refer to Chapter 10: "TOPS-IP maintenance activities."

### Enabling/disabling Telnet access

If the telco is not using Telnet on the 7X07, this parameter should be set to N to avoid inadvertent outages or tampering.

The IPGW_TELNET_ENABLED parameter in Table OFCENG allows the craftsperson to enable or disable Telnet on the 7X07AA by selecting "Y" or "N". The parameter defaults to N meaning Telnet is disabled. The Telnet enabled/disabled status does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level.

The new setting applies only to 7X07AAs datafilled for TOPS usage in existing Table IPINV (field GW_TYPE is set to TOPS).

To verify the change, the craftsperson can attempt to Telnet onto the changed 7X07AAs. If the craftsperson receives the login prompt, Telnet is enabled. If the attempt times out, Telnet is disabled.

## Changing the default Gateway Telnet password

By default, the Gateway Telnet password is the same as the Gateway loadfile user access password set in Windows NT at the DHCP server. However, the Gateway stores and handles them as two separate passwords. The Gateway loadfile user password *must not* be changed in Windows NT. And since it is unsafe to Telnet to a Gateway that is processing calls, users may want to change the Gateway Telnet password from its default after installation. This change does not affect the Gateway loadfile user access password.

The PMDEBUG utility at the Gateway card allows users to change the default Telnet password. The user login name is *gateway* and the default password is *tazmanian*.

The following steps describe how to change the password:

1 Manually busy (BSY DRAIN) the Gateway at the MAP.

2 Telnet to the Gateway card. Enter the user login name and password.

3 Type PMDEBUG to enter the PMDEBUG utility. Figure 269 shows an example of the PMDEBUG level at the Gateway.

**Figure 269 Example of Gateway PMDEBUG level commands**

```
Debug/ Network/ Vxworks/ Password/ PErformance/ Maintenance/ MEdia/ DIag/
Eventtracker/ Snmp/ Time Load
[NT7X07]
```

4 Type P to enter the Password level.

5 Type Instructions to display password help information. Use the following syntax to change the default password:

```
Change tazmanian <new_password> <new_password>
```

6 Type Quit to exit PMDEBUG.

7 Type Logout to close the Telnet connection to the Gateway.

***Note:*** When typing a command, users may enter just the capitalized portion of the command name.

## Resetting the default Gateway Telnet password

The Gateway Telnet password is maintained across any type of software reset, including a PMRESET and across software upgrades. Also, the password survives a reseating of the Gateway card at the IP-XPM. Should the password be forgotten, it is not possible to enter the Gateway through Telnet to set a new password. And since the Gateway password is completely persistent, no type of reboot will restore the default password. The only way to restore the password is to use the PMDEBUG utility at the Gateway's host DTC peripheral.

***Note 1:*** Access to the Gateway by DMS PMDEBUG should *never* be used to enter an in-service Gateway. This means of Gateway access uses the DTC's internal HDLC link to communicate with the Gateway and can adversely affect a Gateway that is in service and handling calls. Refer to "Draining and busying the Gateway card" on page 561.

***Note 2:*** For details on the persistence of Gateway data, refer to "Summary of persistence of user-configured Gateway data" on page 569.

The following steps describe how to restore the password to *tazmanian*:

1 Manually busy (BSY DRAIN) the Gateway at the MAP.

2 Issue the QUERYPM command and note the node number displayed in the Node_No field. This number is used in Step 6 to cross-reference the DTC's internal node table to determine the internal node number of the Gateway.

3 Issue the QUIT ALL command to leave the maintenance MAP level.

4 Type PMDEBUG DTC <nn>, where nn is the number of the DTC that hosts the Gateway card (PMNO field datafilled in table IPINV for the Gateway).

5 Navigate to the top command level of PMDEBUG (by entering *). Figure 270 shows an example of the top-level PMDEBUG commands.

**Figure 270 Example of DTC PMDEBUG level commands**

```
TIme,Load,Xprompt,CHEaptmr,DAtadump,TAsk,Debug,BPMonitor,Swerr,C++monitor,Ipc,
Verreg,Patches,Msg6x69,C14msg,Uartimc,Newmsging,Flq,MTs,NWmsgtrc,Tps,MSGTr,
CHnls,CDm,DYnamic,Opf,MX76dbg,MTC,OMUnsol,Rcvrmon,DIagnose,TCpip,RSi,FLAsh,
Audit,MAtediag,CAudit,PRfm,PErcall,SChnls,DS1,UTr,XBert,TOnes,ECHOCan,Bigfoot,
Gwmon,MSGMx76,TKdata,GDt,TRmtrc,CP,CALl,ISom,DDmgr,GSm,C7tbls,PRTcvs,TRUnks,
IPGateway,ICot,ECHO,IPTRunk.
LTCUP>
```

6 Type CHnls Prot Node to display the node table that maps internal and external node numbers. Figure 271 shows a portion of such a table.

**Figure 271 Example node table**

```
------------------------------------------------------ . . .
NODE TABLE
------------------------------------------------------ . . .
      Node        | Description  |   Msg  |   Port    | . . .
------------------------------------------------------ . . .
 Int External Host|  Node      PM|Protocol|# Start End| . . .
      dec hex    #|  Type    Type|Relation|           | . . .
------------------------------------------------------ . . .
   1  177 0B1    1 LTC:0B  DTC:13 ds30:1 S 16    0  15  . . .
   2   14 00E    1 PGW:21 IPGW:7D hdlc:5 M  2   16  17  . . .
   3   15 00F    1 PGW:21 IPGW:7D hdlc:5 M  2   18  19  . . .
   4   26 01A    1 PGW:21 IPGW:7D hdlc:5 M  2   20  21  . . .
------------------------------------------------------ . . .
```

Using the external node number obtained in Step 2, look at its corresponding internal node number in the table. For example, an external node number of 15 corresponds to an internal node number of 3 in Figure 271.

7 Navigate to the top command level of PMDEBUG again.

8 Type IPG IPGW to enter the IPGW level.

9 At the `Enter IPGW Node Number:` prompt, enter the internal node number (3, in the example).

10 The PMDEBUG command level at the Gateway is displayed, as shown in Figure 272.

**Figure 272 Example of Gateway PMDEBUG level commands**

```
Debug/ Network/ Vxworks/ Password/ PErformance/ Maintenance/ MEdia/ DIag/
Eventtracker/ Snmp/ Time Load
[NT7X07]
```

11 Type P to enter the Password level.

12 Type Instructions to display password help information. Use the following syntax to reset to the default password:

```
Reset tazmanian
```

13 Now use the following syntax to change `tazmanian` to a new, non-default password:

```
Change tazmanian <new_password> <new_password>
```

14 Type Up to exit the Gateway PMDEBUG level.

15 Type Quit to exit the DTC PMDEBUG level.

## Adding recognized SNMP network management nodes

The DHCP server provides the IP address of the default SNMP network management node when the Gateway card comes into service. This IP address can be changed only at the DHCP server (MobileIP Home Agents option). If the Gateway is expected to deal only with this one SNMP manager, then no further configuration work is required.

However, if more than one SNMP manager is expected, up to three more can be added. This is done through the SNMP level of the PMDEBUG utility on the Gateway. The following steps describe how to add the IP address of another SNMP manager:

1 Manually busy (BSY DRAIN) the Gateway at the MAP.

2 Telnet to the Gateway card. Enter the user login name and password.

3 Type PMDEBUG. Figure 273 shows an example of the PMDEBUG commands.

**Figure 273 Example of Gateway PMDEBUG level commands**

```
Debug/ Network/ Vxworks/ Password/ PErformance/ Maintenance/ MEdia/ DIag/
Eventtracker/ Snmp/ Time Load
[NT7X07]
```

4 Type S to enter the SNMP level. Figure 274 shows an example of the SNMP commands. The commands in bold are described after the figure.

**Figure 274 Example of Gateway SNMP level commands**

```
Dispparms Pegbucket Initbucket Chgstart CHGWidth INDbucket DEfmgr
DISPMgrs COnfigmgrs Setoptions
[Snmp]
```

— DEfmgr displays the IP address of the default SNMP manager. This IP address can never be cleared.

— DISPMgrs displays the list of configured SNMP managers.

— COnfigmgrs allows up to three more managers to be recognized by the Gateway.

5 Type CO to configure the IP address or addresses. Figure 275 shows an example of this command level.

**Figure 275 Example of Gateway COnfigmgrs level commands**

```
This command level allows an administrator to enter
the IP addresses of up to 3 additional SNMP Management
Nodes for this gateway. This configuration will
over-write all such previous configurations. The
default SNMP Management Node's IP address is obtained
via DHCP and is unaffected by any operation at this level.

Enter the number of Mgmt Nodes to be added (Max:3) :

Enter IP Address 1
```

6 At the `Enter the number of Mgmt Nodes to be added (Max:3):` prompt, enter the number of nodes to add (1, 2, or 3).

7 At the `Enter IP Address 1` prompt, enter the first IP address. After entering an IP address for each added node, users are returned to the SNMP command level.

8 Type DISPM to display the default and the configured IP addresses.

9 Type Quit to exit PMDEBUG.

10 Type Logout to close the Telnet connection to the Gateway.

***Note 1:*** These Gateway security enhancements place no limits on who can retrieve data from the Gateway with SNMP.

***Note 2:*** When multiple SNMP management nodes are configured, any SNMP trap notifications produced by the Gateway will be sent to each configured manager.

## Disabling Set operations

In addition to source screening for Set operations, the Gateway also provides a command interface that allows Set operations to be fully or partially enabled or disabled. The ability to enable or disable an SNMP-requested reboot is provided independently of the ability to collectively enable or disable Set operations against all other write-accessible objects.

By default, SNMP-requested reboot is disabled and Set operations on all other writable objects are enabled. A network administrator desiring a more restrictive SNMP environment must logon to the Gateway and disable the appropriate Set Enable options. When a Set operation is attempted against a disabled variable, the SNMP manager will receive no indication that the operation failed. The Set request is "silently" refused.

***Note:*** Write-accessible SNMP variables defined by the RFC1213 and RFC1643 MIBs are not included in this security enhancement. This enhancement applies to the private Nortel TOPS-IP Gateway MIBs.

The following steps describe how to disable Set operations:

1 Manually busy (BSY DRAIN) the Gateway at the MAP.

2 Telnet to the Gateway card. Enter the user login name and password.

3 Type PMDEBUG to enter the utility.

4 Type S to enter the SNMP level. Figure 276 shows an example of the SNMP commands.

**Figure 276 Example of Gateway SNMP level commands**

```
Dispparms Pegbucket Initbucket Chgstart CHGWidth INDbucket DEfmgr
DISPMgrs COnfigmgrs Setoptions
[Snmp]
```

5 Type S to enter the Setoptions level. Figure 277 shows an example of this command level.

**Figure 277 Example of Gateway Setoptions level commands**

```
This command level allows an administrator to control whether
SNMP Set operations can be used to reboot the gateway or modify
other settable MIB objects. A separate enable is provided for
SNMP reboot. The other settable objects are grouped together
under another enable.

Current setting for SNMP Reboot Enable is: Disabled.
Current setting for SNMP Set Enable is: Enabled.

SNMP Reboot: Enter 0 to disable, 1 to enable, -1 to abort.
```

The two Set Enable options are:

— `SNMP Reboot Enable` affects the ability to set the nnTgwReboot variable.

— `SNMP Set Enable` affects the ability to set all other variables in the private Nortel MIBs.

The command interface walks the user through setting the two options. Entering 0 disables a Set Enable option. Entering 1 enables that category of Set operation. Entering -1 leaves the Set Enable option unchanged.

6 After entering the desired setting for the two options, type Quit to exit PMDEBUG.

7 Type Logout to close the Telnet connection to the Gateway.

## Source screening for Set operations

When an SNMP Set Request is received by the Gateway's SNMP agent, the source IP address is compared to the list of IP addresses of recognized (configured) network management nodes. If a match occurs, the Set Request is processed normally.

As described previously, users can display the list of configured management nodes with the DISPMgrs command. If the source IP address is not in the list of management nodes, the Set Request is not executed. In such a case, the Set Response sent back to the sending node provides a "GenError" indication. A Gateway log is issued to note this situation. The log includes the IP address of the source node. Figure 278 shows an example log report.

**Figure 278 Example log report for SNMP Set validation failure**

```
Info SUN JAN 04 19:32:34 2001 - Current Load
Task name: tSnmpd
Text: SNMP set validation failed. Src ipaddr is 47.245.1.18
Data: eeee eeee eeee eeee eeee eeee eeee eeee eeee eeee
```

## Persistence of security configuration data

The IP addresses of any additional SNMP managers that have been configured, as well as the state of the Set Enable options, are stored in such a manner as to persist across the following events:

- Gateway-initiated reboot
- SNMP-initiated reboot
- PMRESET from the DMS MAP
- Software upgrade

Reseating the Gateway card will clear the list of configured SNMP managers and reset the Set Enable options to default values.

## Increased IP-XPM security through SNMP

SNMP allows IP hosts to monitor, modify behavior, and receive unsolicited management information from other IP hosts. The monitoring host is termed the SNMP manager and the monitored host is termed the SNMP element.

***Note:*** The SNMP settings are datafilled in the Succession core, but the new settings do not take effect until the data is downloaded to the 7X07AA. The craftsperson must perform a PMRESET on each 7X07AA to download the SNMP settings.

Three settings are introduced in SN09 to provide this increased security. They include:

- SNMP community name
- SNMP manager
- SNMP enable/disable

***Note 1:*** SX05DA support is limited to the Community Name and SNMP enable/disable. Refer to page 536 for additional information.

***Note 2:*** These settings apply only to TOPS 7X07AAs datafilled in existing Table IPINV (field GW_TYPE is set to TOPS). The settings are added as individual office parameters in Table OFCENG.

### SNMP community name

The community name is used for reading and writing SNMP data. It is also used when the IP-XPM sends traps (unsolicited SNMP information) to an SNMP manager.

The community name may be set to some other value than “public.” This increases security since hackers must guess the community name (through repeated attempts) or break into the secure network in order to use a sniffer to detect the SNMP community name.

Many IP hosts allow configuration of different community names for SNMP reads, writes, and traps. For example, many users might need read access to a device while only a few need write access, so separate read and write names are defined. For TOPS-IP, SNMP support is limited, and it is not anticipated that many users will need access to SX05DAs and 7X07AAs. As a result only one community name can be defined.

For the SX07AA, the datafilled community name is validated for incoming read and write requests, and is also sent in trap messages.

### SNMP manager

The SNMP manager is also called the trap manager, since it is the host to whom traps are reported. Allowing specification of an SNMP manager by IP address increases security, since the IP-XPM will reject SNMP write attempts from unauthorized remote hosts.

Up to five SNMP managers can be configured on a 7X07AA card. One is obtained via DHCP and up to three more can be configured using PMDEBUG on each card. A fifth SNMP manager can be configured in the Succession core. When SNMP write requests arrive, the 7X07AA ensures the originating IP address is present in the allowed SNMP manager list. If not, the 7X07AA rejects the write operation.

### SNMP enable/disable

A Y/N parameter indicating whether the IP-XPM supports any incoming SNMP requests, or sends out any traps.

By setting this parameter to N, the 7X07AA will ignore all incoming SNMP requests and will not send any traps.

## Summary of persistence of user-configured Gateway data

The Gateway has some user-configured data that is maintained through SNMP and Telnet access to the Gateway as discussed previously. Table 172 summarizes the persistence of this data in the Gateway with respect to a DMS PMRESET, a Gateway reboot, and reseating or replacing the 7X07 Gateway circuit pack. The affected data includes writable variables in SNMP MIBs, configurable SNMP security settings, and the Gateway password.

**Table 172 Summary of persistence of user-configured Gateway data**

| Gateway resident data | Survives PMRESET | Survives Gateway reboot | Survives software upgrade | Survives reseat of 7X07 pack | Survives replacement of 7X07 pack |
|---|---|---|---|---|---|
| RFC1213 MIB: System group variables, sysName, sysLocation, sysContact | No | No | No | No | No |
| AUDIOCODES.MIB writable variables | Yes | Yes | Yes | No | No |
| TOPSIPGW.MIB writable variables | Yes | Yes | Yes | No | No |
| TOPSQOS.MIB writable variables | Yes | Yes | Yes | No | No |
| Table of additional SNMP management nodes maintained in Gateway PMDEBUG, SNMP level, COnfigmgrs sublevel | Yes | Yes | Yes | No | No |
| Category-enabled SNMP Set operation override flags maintained in Gateway PMDEBUG, SNMP level, Setoptions sublevel | Yes | Yes | Yes | No | No |
| Gateway password | Yes | Yes | Yes | Yes | No |

***Note 1:*** Data in the writable variables in the RFC1213 MIB are reinitialized to default values over any type of reboot or when the 7X07 pack is reseated. Sites that make use of the System group's variables, such as sysName, will need to manually restore these values after any reboot or 7X07 pack reseat.

***Note 2:*** Data in the writable variables in the private Nortel MIBs (AUDIOCODES.MIB, TOPSIPGW.MIB, and TOPSQOS.MIB) as well as data supporting SNMP security enhancements, is retained over any type of reboot and over a software upgrade. This data is lost, however, if the 7X07 pack is reseated or replaced for any reason (such as troubleshooting). Some of this data, such as the jitter buffer settings, can greatly affect Gateway performance. This data must be manually restored after the 7X07 is replaced before the Gateway is brought back into service.

# Appendix C: TOPS-IP Network Configuration

This appendix is intended to assist in planning and configuring the TOPS-IP data network. It focuses on the following areas:

- TOPS-IP network requirements
- Network management considerations
- Network equipment considerations
- Example network topologies

## TOPS-IP network requirements

This section discusses considerations in meeting TOPS-IP network requirements for quality of service (QoS), DHCP servers, network management station, and security.

### Quality of service

Any LAN/WAN network utilized to provide TOPS-IP transport must meet specified performance levels as defined in "TOPS-IP data network requirements" beginning on page 204. This will ensure the level of performance and reliability that is required for TOPS-IP applications.

Data packet prioritization should be considered in the selection of the router and WAN equipment. If QoS cannot be differentiated, the network must meet the most stringent requirements in each area (latency, jitter, and packet loss).

### DHCP network servers

Two DHCP network servers are required to be provisioned somewhere within the secure TOPS-IP LAN/WAN network. These servers each require a 100 Mbps connection.

The network is expected to support forwarding of Network Server requests as unicast relays for a specific server (DHCP forwarding).

### Network management

The network must be provisioned with an SNMPv1 or SNMPv2 based network management system in order to utilize the MIBs provided by the IP-XPM and other network equipment.

### Network security

Firewall and/or router filtering protection should be implemented to ensure that only transactions from within the Directory and Operator Services network can reach the TOPS-IP LAN subnets and DHCP servers. The network is assumed by the TOPS-IP application to provide mechanisms to ensure that it is secure.

***Note:*** An IWS position and its host switch must be in the same IP address space. If IP positions are used with OC-IP, the OC remote switch must also be in the same address space. IP routes between these networks must exist. It is not possible to place IP positions, their host switch or OC remote switch behind a server that performs network address translation.

## TOPS-IP network management considerations

Implementation of a managed IP Network will vary from customer to customer based on existing network equipment, locations, policies and practices. In addition to the network requirements, the following are important considerations while developing plans for TOPS-IP network.

### IP address plan

Plans and practices should be developed to manage the IP Address space in the TOPS-IP network. Careful planning is important to avoid routing problems address conflicts and service outages. Addresses should be reserved for IP-XPM's, IP positions, DHCP servers, network management servers and network equipment (Ethernet switches, routers, etc.).

### Directory database access

Installation or migration of positions to a TOPS-IP network should be coordinated with directory database administrators.

### Internet access during installation of Windows XP

Licence key registration of Windows XP is required at installation. This is usually accomplished by performing the installation on a network that has Internet access and then moving the position to the destination subnet in the OSC.

## TOPS-IP Network Equipment Considerations

This section provides information about LAN connection media, Ethernet switches, routers, and WAN equipment. It is intended to help with planning and initial setup of the equipment.

### LAN connection media

The engineering requirements and cable lengths will play a role in the types of connections to be used between ethernet switches, routers, and other wide area network equipment.

#### Cables from IWS positions to Ethernet switches

CAT-5 (or better) cabling of less than 100 meters must be used.

### Connections from Ethernet switches to routers

The engineering requirements, cable lengths and the available equipment interface options will play a role in the types of connections to be used between ethernet switches, routers.

- CAT-5 cabling is used for 100BASE-TX connections less than 100 meters.
- Multimode fiber is used for 100BASE-FX connections up to 2 km or Gigabit interfaces up to 550 meters.
- Single mode fiber is used for Gigabit interfaces for distances greater than 550 meters.

## Ethernet switches

For existing IWS installations the token ring and/or Ethernet hubs will be replaced by Ethernet switches. We recommend that an ethernet switch like the Nortel Networks Business Policy Switch (BPS) 2000 or an equivalent be utilized to allow customers to maintain TOPS network requirements and allow the greatest flexibility in implementing new services. The BPS 2000 can be configured to prioritize IP traffic and could be a valuable aid in maintaining network service levels as enhanced services are implemented. For example, voice and call setup packets could be given a higher priority in an environment where file transfers or http traffic are contending for bandwidth.

***WARNING***: Routing interfaces present in the SX05DA subnet must have the spanning tree algorithm disabled. Failure to disable spanning tree could result in the inability to bring the SX05DA in service or to keep both units of the IP-XPM in service.

### Configuring the BPS2000

The Business Policy Switch begins switching as soon as you attach network devices and connect the switch to power. To manage the switch using SNMP or to perform TFTP operations, you must set certain IP parameters. In addition, if you are connecting Business Policy Switches into a stack configuration, you must supply additional parameters to properly set up the stack.

The BPS 2000 user guides are available on the nortelnetworks.com web site. The current releases are:

- *Business Policy Switch 2000 Installation Instructions,* part number 209319-A
- *Using the Business Policy Switch 2000 Software Version 2.5,* part number 208700-D
- *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5,* part number 209570-D

The following sections should assist with the initial configuration:

- Initial switch setup
- Setting the stack operational mode
- How to set passwords

### Initial switch setup

Setting IP parameters For the initial setup of a standalone switch or a stack configuration, you must set the following IP parameters:

- IP address of the switch or the stack
- subnet mask
- gateway address.

To set the IP parameters:

1 Connect a terminal to the Console port on the switch.

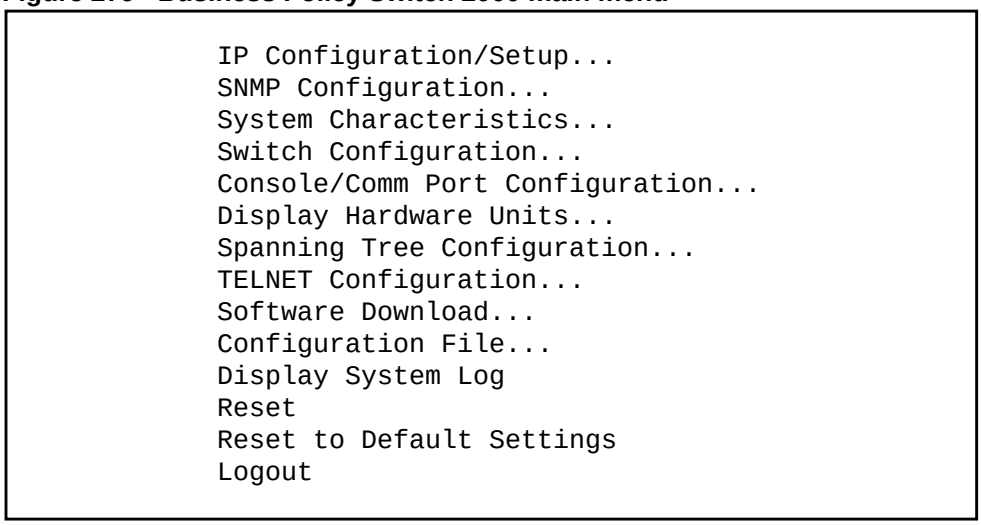
2 Set the terminal protocol as described in *Using the Business Policy Switch 2000*.

3 Connect the switch to power.

4 After the Nortel Networks logo is displayed, press [Ctrl]-Y to display the Main Menu. At first the screen displays the Main Menu for a standalone switch. Then, if the switch is part of a stack configuration, the screen is refreshed within 20 seconds to show the Main Menu for a stack configuration.

5 Select IP Configuration/Setup (or press i) to display the IP Configuration/ Setup menu.

**Figure 279 Business Policy Switch 2000 main menu**




Use arrow keys to highlight option, press <Return> or <Enter> to select option.

6 Enter the switch or stack IP address, in dotted-decimal notation:

— For a standalone switch, in the In-Band Switch IP Address field, enter the IP address of the switch.

— For a stack configuration, in the In-Band Stack IP Address field, enter the Stack IP address.

***Note 1:*** The In-Band Switch IP Address field allows this switch to operate as a standalone switch. However, this field is not required for the operation of the stack. You cannot enter the same IP address in both fields.

***Note 2:*** If the In-Band Subnet Mask field does not already contain a value when you enter the IP address in the In-Band IP Address field, the switch software provides an in-use default value for the In-Band Subnet Mask field. This value is based on the class of the entered IP address.

7 In the In-Band Subnet Mask field, enter the IP subnet mask address.

8 In the Default Gateway field, enter the default gateway address.

### Setting the stack operation mode

You can stack the BPS 2000 up to 8 units high. There are two types of stacks, Pure BPS 2000 and Hybrid. For more details on stacking and interoperability please refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

Stack operation limitations include:

— A BPS 2000 in standalone mode must indicate the stack operational mode as Pure BPS 2000 Mode, not Hybrid Mode;

— All BPS 2000 switches in the stack must be running the identical version of software;

— All the BayStack switches must be running the identical version of software;

— Mixed stacks must have identical Interoperability Software Version Numbers (ISVN). If the ISVNs are not the same, the stack does not operate.

To set the stack operation mode:

1 From the Main Menu, choose Switch Configuration > Stack Operation Mode.

2 On the Stack Operation Mode menu, select Hybrid Stack as the Next stack operational mode.

3 Press Ctrl-C to return to the Main Menu.

4 From the Main Menu, press R to reset the switch.

Refer to *Using the Business Policy Switch 2000* for detailed descriptions of the menus and screens you can use to customize your configuration.

***Note:*** In a hybrid or mixed stack, one (and only one) Business Policy Switch must be set as the base unit.

### How to set passwords for a BPS2000

Caution: If you change the system-supplied default passwords, be sure to write the new passwords down and keep them in a safe place. If you forget the new passwords, you cannot access the console interface. In that case, contact Nortel Networks for help.

1 Enter Ctrl-Y to begin.

The Main Menu will appear. Use arrow keys to highlight an option.

2 Select Console/Comm Port Configuration...

3 Enter the *types* of password for Console and Telnet (none, Local or Radius)

Telnet Switch Password Type: [Local Password]

4 If Local Password was chosen as the password type, then fill in values for the Console Read-Only and Console Read-Write. Telnet and http will use these values also. In this example, the Read-Only password is set to "user" and the Read-Write password is set to "setup".

Console Read-Only Switch Password: [user]

Console Read-Write Switch Password: [setup]

***Note 1:*** Access level via the console and telnet is determined by the password supplied. If the Read-Write password is entered, that session will have read-write capabilities.

***Note 2:*** Access via http will prompt you for a user ID and password. The Read-Only user ID is "RO" without the quotes and must be upper case. The Read-Write user ID is "RW" without the quotes and must be upper case.

## Routers

Routers will be required to connect to directory database services and to interconnect the OSC networks with DMS switch IP-XPM networks. Routers should detect network faults and reconverge within 2 seconds using VRRP or a similar router redundancy scheme, to ensure that no single network failure isolates nodes.

It is important that the routers be capable of implementing QoS mechanisms. Protocol prioritization, traffic filters and other standards-based mechanisms are needed to ensure network requirements are maintained. Refer to Table 4, "Ports and protocols used for TOPS-IP data packets," on page 206 for the IP port numbers used by TOPS-IP.

### Wide area network equipment

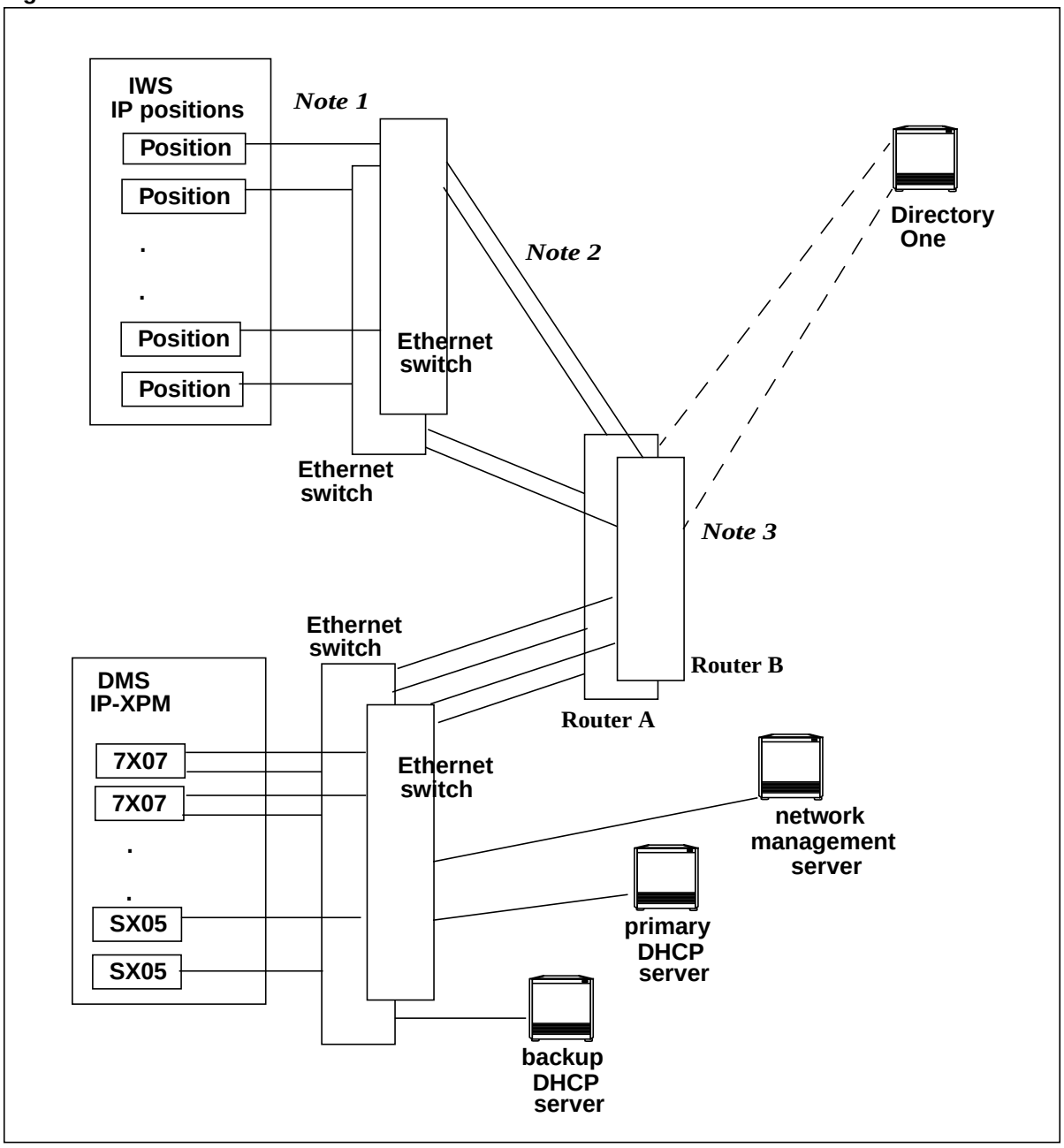
Wide area network implementation will vary from customer to customer. Detailed descriptions of options and configurations is beyond the scope of this document. Customers are encouraged to implement a fault-tolerant network and utilize network management tools for rapid network fault detection.

In some cases the Operator Service Center (OSC) network will be co-located with the DMS IP-XPM network, eliminating the need for WAN equipment and connections other than the existing links to directory databases.

## Example TOPS-IP network topologies

This section shows two example TOPS-IP network topologies. In the first example, the OSC is co-located with its host DMS switch, so WAN facilities are not needed. In the second topology, the OSC and its host DMS are not co-located, so they are connected via a WAN.

**Figure 280 Minimum TOPS-IP network: OSC co-located with IP-XPM**

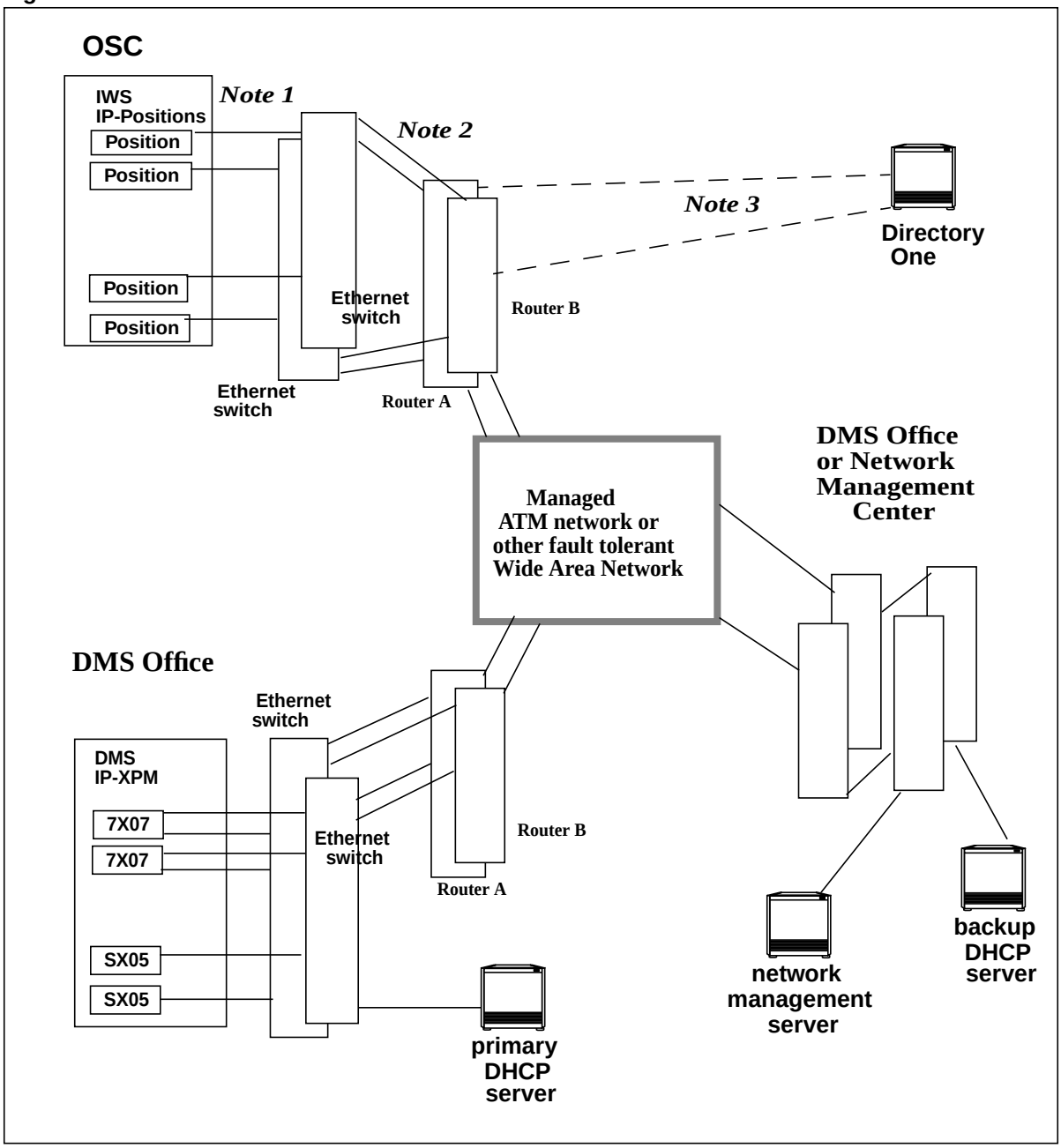



***Note 1:*** CAT-5 cabling from positions to Ethernet switches not to exceed 100 meters.

***Note 2:*** The speed and type of media between Ethernet switches and routers depends on the engineering requirements and the physical distances (cable lengths).

***Note 3:*** Router(s) are required to access directory databases. Directory database connectivity is typically T1.

**Figure 281 TOPS-IP network: OSC connected to DMS office via WAN**




***Note 1:*** CAT-5 cabling from positions to Ethernet switches not to exceed 100 meters.

***Note 2:*** The speed and media between Ethernet switches and routers depends on the engineering requirements and distances.

***Note 3:*** Directory One connectivity is typically T1.

# Appendix D: IWS IP datafill quick reference

This appendix is a quick reference for IWS configuration information that is mentioned in this book. Some of the configuration data must be parallel between the switch and the IWS, and other IWS data affects switch functionality even though the datafill is not parallel.

***Note:*** The information in this appendix applies only to the IWS17.1 software release. Furthermore, it is by no means a complete description of IWS datafill or even of parallel datafill requirements for the IWS. Refer to *TOPS IWS Base Platform User's Guide* and other standard IWS documentation for more information.

**Table 173 Quick reference for IWS17.1 datafill mentioned in this book**

| Data item | IWS configuration parameter | Corresponding switch datafill or functionality |
|---|---|---|
| position number | C:\windows\posinfo.ini<br>[PosIPConfig] PosNumber | index to table TOPSPOS |
| position IP address | Windows Start->Settings->Control Panel->Network Connections->Local Area Connections->Properties->Internet Protocol->Properties->IP address | Not datafilled in switch. Switch learns position IP address from its in-service request message. |
| position port for data from switch | C:\windows\mpxnet.ini<br>[IPConfig] DMSPortIn | Not datafilled in switch. Switch learns position port from its in-service request message. |
| switch IP address | C:\windows\mpxnet.ini<br>Datafill a host name for the switch (such as "dmsnode") against [IPConfig] DMSNode<br>C:\windows\system32\drivers\etc\hosts<br>Datafill the same switch host name (from mpxnet.ini) against the switch IP address | Table TOPSPOS field IPCOMID indexes table IPCOMID.<br>Table IPCOMID field XPMNAME specifies the IP-XPM (a DTC), which indexes table XPMIPMAP.<br>IPCONFIG selector in XPMIPMAP specifies CM or DHCP.<br>If IPCONFIG=CM, ACTADDR field contains the IP address to datafill in the IWS.<br>If IPCONFIG=DHCP, the IWS datafill must match the host IP address that is datafilled in the DHCP server against the MAC address of unit 0 of the IP-XPM (see Step of "Configure NetID," on page 521). |

| Data item | IWS configuration parameter | Corresponding switch datafill or functionality |
|---|---|---|
| switch port for data from position | C:\windows\mpxnet.ini<br>[IPConfig] DMSPortOut | Table TOPSPOS field IPCOMID indexes table IPCOMID.<br>Table IPCOMID field SERVICE indexes table IPSVCS. PORT field in IPSVCS tuple must be datafilled in IWS. |
| option to send DA link alarms to switch | C:\windows\posinfo.ini<br>[IPConfig] SendExtLinkAlarm<br>C:\windows\ntdaini.ini<br>Link_Alarm_Service | Table TQMSSERV lists TOPS QMS services. Datafill the service that the position normally logs into, and should send alarms for, in IWS parameter Link_Alarm_Service.<br>Switch functionality related to SendExtLinkAlarm: TPExDB alarm (see page 366) and TOPS136 log (see page 465). |

# List of terms

**%OCC**

percent occupancy

**10 base T**

A standard for Ethernet data transmission over twisted pair at 10 megabits per second.

**100 base T**

A standard for Ethernet data transmission over twisted pair at 100 megabits per second.

**7X07 card**

An NT7X07 IP Gateway circuit used for voice communication over the managed IP network. The 7X07 has its own Ethernet interface and is responsible for conversion between circuit-switched voice and packet-switched voice. Also referred to as the “Gateway card.”

**Address Resolution Protocol (ARP)**

A protocol used by the IP routing service to translate IP addresses into Ethernet addresses.

**ARP**

Address Resolution Protocol

**ATM**

Asynchronous Transfer Mode

**BOOTP**

Bootstrap Protocol

### BPS

Business Policy Switch

### Bootstrap Protocol (BOOTP)

Part of the TCP/IP suite of protocols used to dynamically assign IP addresses and other configuration information to networked computers. BOOTP is the predecessor of DHCP.

### central office (CO)

A central office arranged for terminating subscriber lines and provided with switching equipment trunks for establishing connections to and from other switching offices.

### central processing unit (CPU)

The hardware unit of a computing system that contains the circuits that control and perform the execution of instructions.

### CI

command interpreter

### CM

computing module

### CO

central office

### COMID

communication identifier

### command interface (CI)

A component in the DMS-100 Family switch operating system that functions as the main interface between the machine and the user.

### communication identifier (COMID)

A number that embodies local data connectivity information for switch CM applications that use an Ethernet-equipped SX05 XPM. *See also* IP-XPM.

**computing module (CM)**

The processor and memory of the dual-plane combined core used by the DMS SuperNode. Each CM consists of a pair of CPUs with associated memory that operate in a synchronous matched mode on two separate planes. Only one plane is active; it maintains overall control of the system while the other plane is on standby.

**CPU**

central processing unit

**CRES**

Connected Restricted Idle. The maintenance state of an in-service IP position that is not accepting calls.

**CSE**

Customer Assistance Service Enhancements

**DoIP**

Data over IP

**DCM**

Digital Carrier Module

**DHCP**

Dynamic Host Configuration Protocol

**Digital Carrier Module (DCM)**

A peripheral module that provides a traditional operator centralization data link interface.

**Digital Trunk Controller (DTC)**

An XPM that connects DS30 links from the network with digital trunk circuits.

**DMS**

Digital Multiplex System

**DMS SuperNode**

A central control complex for the DMS-100 Family switch. The two major components of the DMS SuperNode are the computing module and the message switch. Both are compatible with the network module, the input/output controller, and XPMs.

### DS-0

A protocol for data transmission that represents one channel in a 24-channel DS-1 trunk.

### DS-1

A 24-channel 1.544-Mb/s digital signaling format used for digital trunks in in North America. Each DS-1 channel (DS-0) transmits 64 kb/s.

### DS30

A 32-channel 2.048-Mb/s speech-signaling and message-signaling link used in the DMS-100 Family switches.

### DTC

Digital Trunk Controller

### Dynamic Host Configuration Protocol (DHCP)

Part of the TCP/IP suite of protocols used to dynamically assign IP addresses and other configuration information to networked computers. DHCP is the successor of BOOTP.

### EIU

Ethernet interface unit

### end office (EO)

A switching office arranged for terminating subscriber lines and provided with trunks for establishing connections to and from other switching offices.

### ENET

Enhanced Network

### Enhanced Network (ENET)

A channel-matrixed time switch that provides PCM voice and data connections between peripheral modules.

### Enhanced TOPS Message Switch (ETMS)

An XPM used by TOPS to provide non-IP voice and data for operator centralization.

### EO

end office

### Ethernet interface unit (EIU)

A circuit that connects the DMS SuperNode to the local area network. The EIU is not used by TOPS-IP applications.

### ETMS

Enhanced TOPS Message Switch

### extended peripheral module (XPM)

The generic name for peripheral modules that use the Motorola 68000 microprocessor.

### file transfer protocol (FTP)

A protocol used to transfer files, such as load files and patch files, across the Ethernet local area network facility.

### FM

force management

### FTP

file transfer protocol

### Gateway card

*See* 7X07 card.

### H.323

A protocol that specifies a set of standard interfaces for data, voice, and video communication among a diverse set of cooperating terminals in a packet-switched network. Functionality is roughly comparable to that of SIP.

### HDLC

high-level data link control

### high-level data link control

The channel that carries high-level control messages from central control between the IP-XPM (DTC) and the Gateway card.

### HMI

human-machine interface

### Host Remote Networking by Queue Type (HRNQT)

An operator centralization (OC) feature that allows remote calls to be routed to different hosts depending on the call queue. A single switch can serve as an OC host for some queues and as a remote for other queues.

### HRNQT

Host Remote Networking by Queue Type

### human-machine interface (HMI)

The series of commands and responses used by operating company personnel to communicate with DMS-100 Family switches. Communication takes place through the MAP terminal and other input/output devices.

### ICMP

Internet Control Message Protocol

### IDLT

idle time

### IETF

Internet Engineering Task Force

### IGIP

ISUP Gateway Interworking Protocol

### initial program load (IPL)

The initialization procedure that causes a computer operating system to start operation.

### integrated services digital network (ISDN)

A set of standards proposed by the CCITT to establish compatibility between the telephone network and various data terminals and device. ISDN is a fully digital network, in general evolving from a telephone integrated digital network. It provides end-to-end connectivity to support a wide range of services, including circuit-switched voice, circuit-switched data, and packet-switched data over the same local facility.

### Internet addressing

Physical or subnet addressing used by the Internet Protocol (IP) in which each host is assigned a unique integer address, written in the form of decimal notation. The address is referred to as IP address.

**Internet Protocol (IP)**

A suite of protocols used at the network layer in data communication across the Ethernet local area network (LAN). IP is used in the public Internet and private intranets.

**IP**

Internet Protocol

**IP-XPM**

Internet Protocol - extended peripheral module. A DTC (Digital Trunk Controller) peripheral equipped with several new or upgraded components that support the integrated TOPS-IP architecture.

**IPL**

initial program load

**IP-XPM**

An extended peripheral module at the DMS switch used to deliver integrated IP voice and data to the managed IP network.

**ITU-T**

**ISDN**

integrated service digital network

**ISDN user part (ISUP)**

A common channel message-based signaling protocol that acts as a transport carrier for ISDN services. ISUP provides the functionality in a CCS7 network for voice and data services.

**ISUP**

ISDN user part

**ISUP Gateway Interworking Protocol**

A proprietary protocol used by the 7X07AA Gateway card. IGIP incorporates elements of both H.323 and ISUP.

**IWS**

Intelligent Workstation

### LAN

local area network

### local area network (LAN)

A network that permits the interconnection and intercommunication of a group of computers.

### maintenance and administration position (MAP)

A group of components that provides a user interface between operating company personnel and the DMS-100 Family of switches. The interface consists of a video display unit and keyboard, a voice communications module, test facilities, and special furniture.

### managed IP network

A private, engineered network using standard IP components. The managed IP network responsible for routing and delivering data and voice traffic—in the form of packets—between nodes in the private intranet.

### management information base (MIB)

A data structure in SNMP network management that defines what is obtainable from a network device.

### MAP

maintenance and administration position

### message switch (MS)

A high-capacity communications facility that functions as the messaging hub of the dual-plane combined core of a DMS SuperNode processor. The MS controls messaging between the DMS-Bus components by concentrating and distributing messages and by allowing other DMS-STP components to communicate directly with each other.

### MIB

management information base

### MIS node

An external reporting facility that receives data, which is used to report statistics on the functioning of call queues and agents (or service node sessions). *See also* Queue Management System Management Information System (QMS MIS).

**MS**

message switch

**NCL**

non-CM load

**network module (NM)**

The basic building block of the DMS-100 Family switches. The NM accepts incoming calls and uses connection instructions from the central control complex to connect the incoming calls to the appropriate outgoing channels. Network module controllers control the activities in the NM.

**NM**

network module

**non-CM load (NCL)**

The software load for a non-computing module (CM) component, such as an extended peripheral module (XPM).

**Nortel Networks publication (NTP)**

A document that contains descriptive information about Nortel Networks hardware or software modules and performance-oriented practice for installing, testing, or maintaining the system. The document is often supplied as part of the standard documentation package provided to an operating company.

**NTP**

Nortel Networks publication

**OC**

operator centralization

**OC-IP**

The implementation of OC using integrated IP voice and data through a TOPS IP-XPM.

**OM**

operational measurement

**Open Position Protocol (OPP)**

The protocol required to communicate data between a TOPS switch and an OPP-compatible terminal, such as the TOPS IWS.

### operational measurements (OM)

The hardware and software resource of the DMS-100 Family switches that control the collection and display of measurements taken on an operating system. The OM subsystem organizes the measurement data and manages its transfer to displays and records. The OM data is used for maintenance, traffic, accounting, and provisioning decisions.

### operator centralization (OC)

A DMS TOPS functionality that allows a host switch to provide operators for calls that are processed in remote switches.

### OPP

Open Position Protocol

### OSC

operator services center

### OSSAIN

Operator Services System Advanced Intelligent Network

### PCL

product computing module load

### PCM

pulse code modulation

### PEC

product engineering code

### peripheral module (PM)

A generic term referring to all hardware modules in the DMS-100 Family switches that provide interfaces between external line, trunk, or service facilities. A PM contains peripheral processors that perform routines, thus relieving the load on the CPU.

### PM

peripheral module

### IP position

The implementation of TOPS operator positions using integrated IP voice and data through a TOPS IP-XPM.

### product computing module load (PCL)

The CM software load delivered to the operating company. A PCL contains both base and optional functionalities.

### product engineering code (PEC)

An eight-character unique identifier for each marketable hardware item manufactured by Nortel.

### PSTN

public switched telephone network

### pulse code modulation (PCM)

Representation of an analog waveform by coding and quantifying periodic samples of the signal. Each sample is encoded as a binary number.

### QMS CASE

Queue Management System Customer Assistance Service Enhancements

### QMS MIS

Queue Management System Management Information System

### QMS MIS-IP

The implementation of QMS MIS using IP data connectivity through a TOPS IP-XPM.

### Queue Management System Management Information System (QMS MIS)

A switch application that collects event-driven data about TOPS and OSSAIN calls and sends this data to an external reporting facility, or MIS node. The data is used to report statistics on the functioning of call queues and agents (or service node sessions).

### Real-Time Transport Control Protocol (RTCP)

An industry standard protocol that augments RTP to allow monitoring of data delivery and to provide minimal control and identification functionality.

### Real-Time Transport Protocol (RTP)

An industry standard protocol used to transport data with real-time characteristics, including audio and video.

**RES**

Restricted Idle. The state of a TDM position that is in service but not available for call processing. Rather than having a RES state, IP positions have URES and CRES states.

**RFC**

Request for comments.

**router**

A component of the managed IP network used to forward IP packets to other networks. A router is sometimes referred to as a gateway router.

**RTCP**

Real-Time Transport Control Protocol

**RTP**

Real-Time Transport Protocol

**RTS**

return to service

**SA**

Service Assistant

**Session Initiation Protocol (SIP)**

A protocol that specifies standard interfaces for creating, modifying and terminating sessions with one or more participants. These sessions can include Internet multimedia conferences, Internet telephone calls and multimedia distribution. Functionality is roughly comparable to that of H.323.

**Simple Network Management Protocol (SNMP)**

An industry standard protocol used to manage and monitor network activity and performance.

**SIP**

Session Initiation Protocol

**SNMP**

Simple Network Management Protocol

**SOC**

software optionality control

**software optionality control (SOC)**

A tool for controlling and monitoring the options in a product computing module load (PCL).

**state transition**

A node change from one maintenance state to another; for example, from system busy to in service.

**SX05 card**

An NTSX05 Unified Processor circuit used for data communication over the managed IP network. It serves as the main processor, replacing the MX77 Unified Processor. The SX05 has a full-duplex 10/100 Megabit per second (Mbps) Ethernet port.

**T1**

The standard 24-channel 1.544-Mb/s pulse code modulation system used in North America. This digital carrier carries a signal whose designation is a DS-1 link.

**TCP**

Transmission Control Protocol

**TDM**

time division multiplexing

**TLI**

Transport Layer Interface

**TMS**

TOPS message switch

**TOPS**

Traffic Operator Position System

**TOPS IWS**

Traffic Operator Position System Intelligent Workstation System

### Traffic Operator Position System (TOPS)

A call processing system made up of a number of operator positions. Each operator position consists of a visual display unit (VDU), a controller, a keyboard, and a headset.

### Traffic Operator Position System Intelligent Workstation System (TOPS IWS)

An integrated operator assistance, intercept, and DA position, which uses a personal computer with customized software, keyboard, and interface.

### Transmission Control Protocol (TCP)

A connection-oriented protocol that builds the underlying IP datagram delivery service. TCP adds reliability through sequencing, timeouts, and retransmissions. It provides acknowledgments and checks for missing, out-of-sequence, and duplicated packets.

### Transport Layer Interface (TLI)

A generic interface used by applications to access transport layer protocols, such as User Datagram Protocol (UDP).

### URES

Unconnected restricted idle. The maintenance state of an IP position when a socket for the position is open in the SX05DA but the position is not in service and is not known to be troubled.

### UDP

User Datagram Protocol

### User Datagram Protocol (UDP)

A connectionless protocol that permits packets to be sent with a minimum of protocol overhead. With UDP, message delivery is not guaranteed. It provides neither acknowledgments nor checks for missing, out-of-sequence, or duplicated packets.

### Virtual Router Redundancy Protocol (VRRP)

A standard router redundancy protocol that eliminates the single point of failure common in a single default router environment.

### VoIP

Voice over IP

### VRRP

Virtual Router Redundancy Protocol

**WAN**

wide area network

**wide area network**

A large-scale, high-speed communications network used primarily for interconnecting local area networks (LAN) located in different cities or nations.

**XIPVER**

An XPM IP verification CI tool that uses non-menu commands. With XIPVER, users initiate User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) transactions through the IP-XPM.

**XPM**

extended peripheral module

# Index

# E



# F



# G



# H



# I

# L

# M



# N



# O



# P



# Q



# R

## S



## T



## U



## V



## W



## X

DMS-100 Family

# TOPS-IP
# User's Guide



Publication number: 297-8403-906
Product release: SN09 and up
Document release: Standard
Date: April 2006
Printed in the United States of America

NORTEL NETWORKS™