297-8403-906

DMS-100 Family

TOPS Internet Protocol (TOPS-IP)

User's Guide

TOPS15 and up Preliminary 02.03 September 2001

NORTEL NETWORKS™

DMS-100 Family

TOPS-IP

User's Guide

Publication number: 297-8403-906
Product release: TOPS15 and up
Document release: Preliminary 02.03
Date: September 2001

Publication history

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.

Note: The TOPS-IP product is not planned to be generally available; however, it may be ordered by special arrangement. TOPS-IP functionality is intended only for the North American market. For more details, contact your Nortel Networks representative.

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

TOPS15 preparatory work

Several TOPS-IP features were implemented in the TOPS15 software release in preparation for the support of TOPS Intelligent Workstation System (IWS) operator positions that have IP voice and data connectivity with the DMS switch. These positions were referred to as "IP positions." IP positions, however, will not be orderable.

Customer-visible changes that were made primarily for IP positions but which also affect OC-IP are described in this document. Visible changes that do not affect OC-IP are not included here but may be found in *Translations Guide* and in *Customer Data Schema Reference Manual*.

Software enhancements available in TOPS15

For readers of an 01.xx version of *TOPS-IP User's Guide*, this section briefly describes the enhancements provided in the TOPS15 software, with pointers to specific chapters where the changes are documented.

New way to limit the number of TOPS-IP dynamic voice trunks

Although 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. For details, refer to Chapter 2: "TOPS-IP data and voice communication," and Chapter 6: "TOPS-IP engineering guidelines."

New method for datafilling OC-IP data links

To optimize load balancing among C-side links, an earlier version of TOPS-IP software recommended datafill for eight OC-IP data links to each distant office. With TOPS15 software, only one OC-IP data link is required from each IP-XPM to each distant office. For details, refer to Chapter 3: "TOPS OC-IP application."

New engineering guideline for QMS MIS-IP data links

With TOPS15 software, an IP-XPM that supports a QMS MIS-IP data link cannot also support OC-IP data links. The IP-XPM used for MIS-IP must be a dedicated peripheral that has no 7X07AA Gateway cards installed. For details, refer to Chapter 6: "TOPS-IP engineering guidelines."

New voice codec selection

In an earlier version of TOPS-IP software, the voice codec selection was done through datafill in existing table OCHOSTQ (Operator Centralization Host Queue). In TOPS15 software, the voice codec selection is done instead through datafill in new table PKTVPROF (Packetized Voice Profile) and existing table TQCQINFO (TOPS Call Queue Information). For details, refer to Chapter 2: "TOPS-IP data and voice communication."

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 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 5: 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 6: TOPS-IP engineering guidelines

This chapter provides information on requirements for performance, capacity, and provisioning for the TOPS-IP network.

Part 5: Provisioning

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

Chapter 7: TOPS-IP data schema

This chapter describes datafill requirements for TOPS-IP.

Chapter 8: 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 9: TOPS-IP maintenance activities

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

Chapter 10: TOPS-IP CI tools

This chapter discusses related CI tools.

Chapter 11: TOPS-IP logs

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

Chapter 12: 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).

List of terms

This chapter lists terms and definitions.

Feature activity

The features listed in the following table provide the foundation and functionality of the TOPS-IP product.

TOPS-IP related features

Feature name	Activity ID
IP on XPM	59007341
TOPS-IP Data Communication	59007541
TOPS-IP Data Communication Utilities	59007546
TOPS-IP OC-IP Infrastructure	59012723
TOPS-IP OC-IP Voice	59013928
TOPS-IP OC-IP Data	59013932
TOPS-IP OC-IP Data Link Maintenance	59013936
TOPS-IP QMS MIS over IP	59007458
TOPS-IP Other DRU Changes	59007550
TOPS-IP Call Processing for IP Voice	59015863
TOPS-IP Voice Provisioning and Utilities	59022288
TOPS-IP IPGW Enhancements	59022293
TOPS-IP 7X07 Gateway Support for Voice over IP	59022821
TOPS-IP Global Support	59020499
RSI Link Selection, Version Control, Robustness	59022114
TOPS-IP Position Maintenance	59006653
TOPS-IP Position Provisioning and OPP Data	59006658

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 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*
- *TOPS QMS MIS Protocol*, Q220-1

  Note: QMS MIS Protocol is a licensed interface. To receive this document, please contact Nortel Networks Marketing.
- *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, *Coding of Speech at 8kbits/s Using Conjugate Structure Algebraic-Code-Excited-Linear-Predication (CS-ACELP)*
- ITU-T (H.225), *Media Stream Packetization and Synchronization on Non-Guaranteed Quality of Service LANs*
- ITU-T (H.323), *Packet-based Multimedia Communications Systems*
- RFC768 (STC 6) *User Datagram Protocol*
- RFC791 (STD 5) *Internet 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*
- RFC2131 *Dynamic Host Configuration Protocol*
- RFC2338 *Virtual Router Redundancy Protocol*

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:

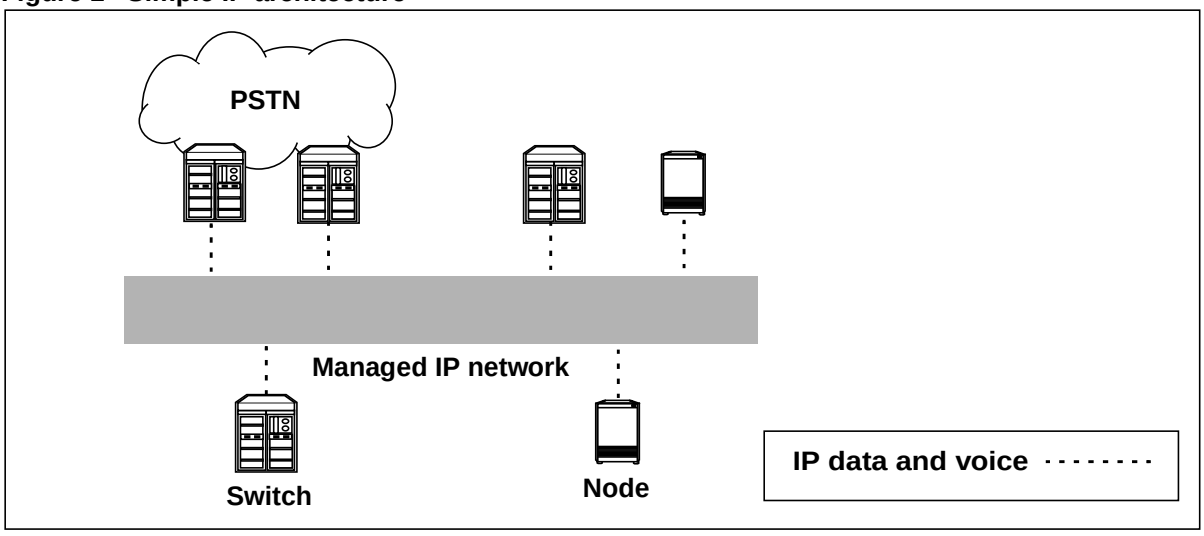
- benefits of IP networking
- components of the IP infrastructure
- capabilities of TOPS-IP

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 current 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:

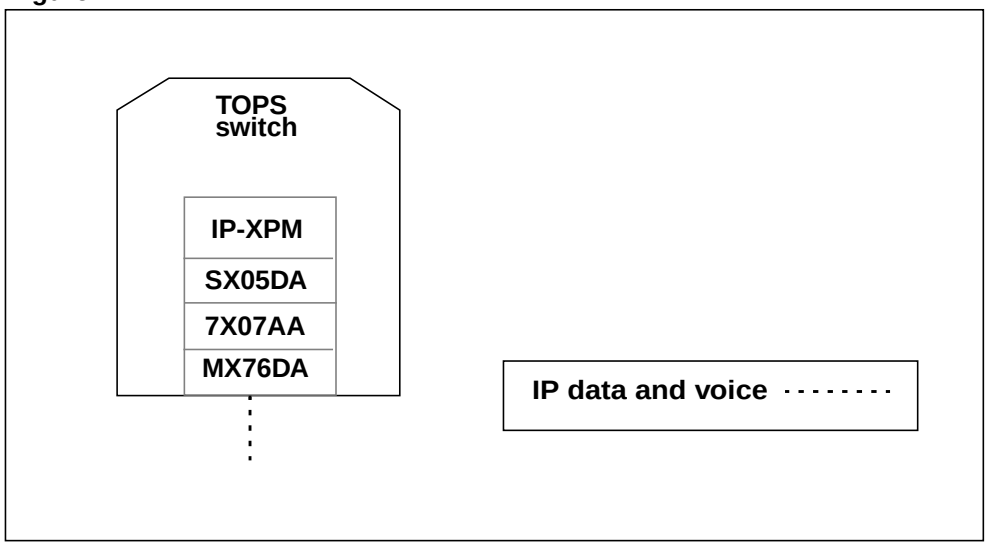
- an IP-based extended peripheral module (IP-XPM) at the DMS switch
- the managed IP network, or private intranet

This section introduces the key hardware for these two components. Chapter 2: “TOPS-IP data and voice communication” provides functional details and Chapter 6: “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 48 voice channels (in North American applications).

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 (for North American loads):

- 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 to either an Ethernet patch panel (optional) or to a compatible Ethernet switch on the LAN

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 6: "TOPS-IP engineering guidelines."

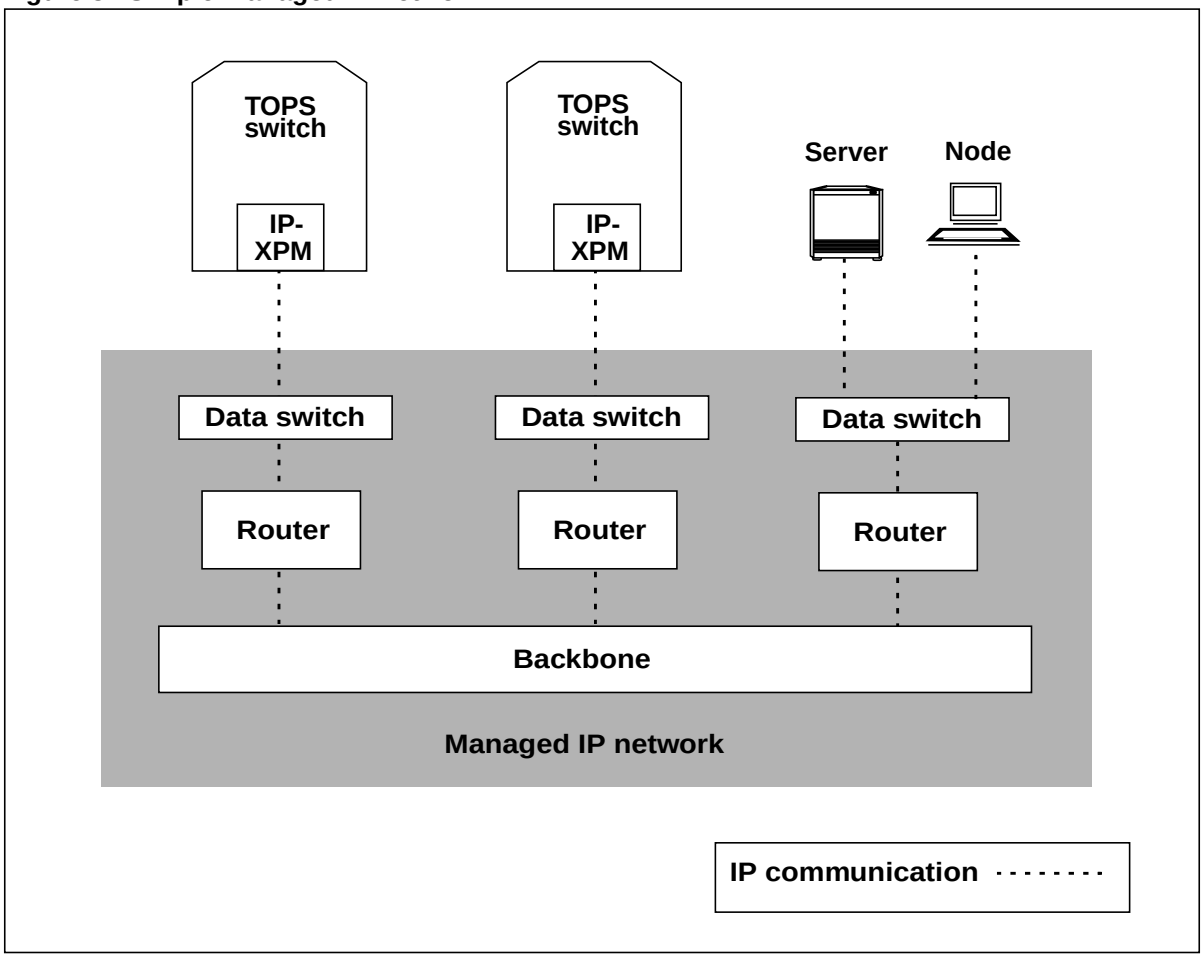
DHCP/FTP server

A Dynamic Host Configuration Protocol/File Transfer Protocol (DHCP/FTP) server (NTNX55PA, NTNX55QA, NTNX55RA) 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, 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 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 6: "TOPS-IP engineering guidelines."

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. Two TOPS-IP applications use the IP infrastructure:

- Operator Centralization (OC-IP)
- 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.

TOPS OC-IP application

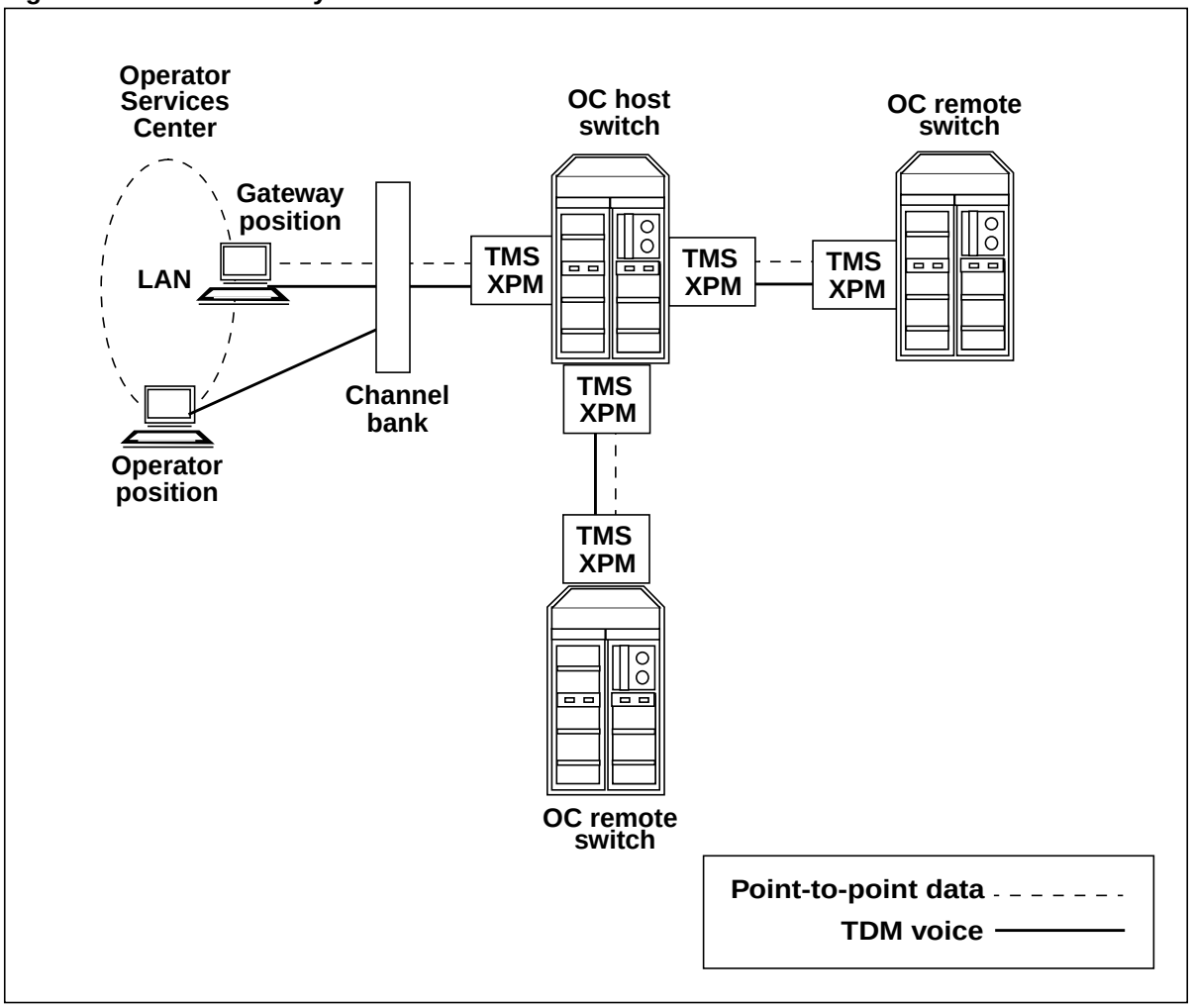
In a centralized operator network, a number of TOPS remote switches share the operator positions provided by a TOPS host switch. Calls originate in a remote switch, which is responsible for call control. The host switch provides the operator positions and is responsible for call and agent queue management,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

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

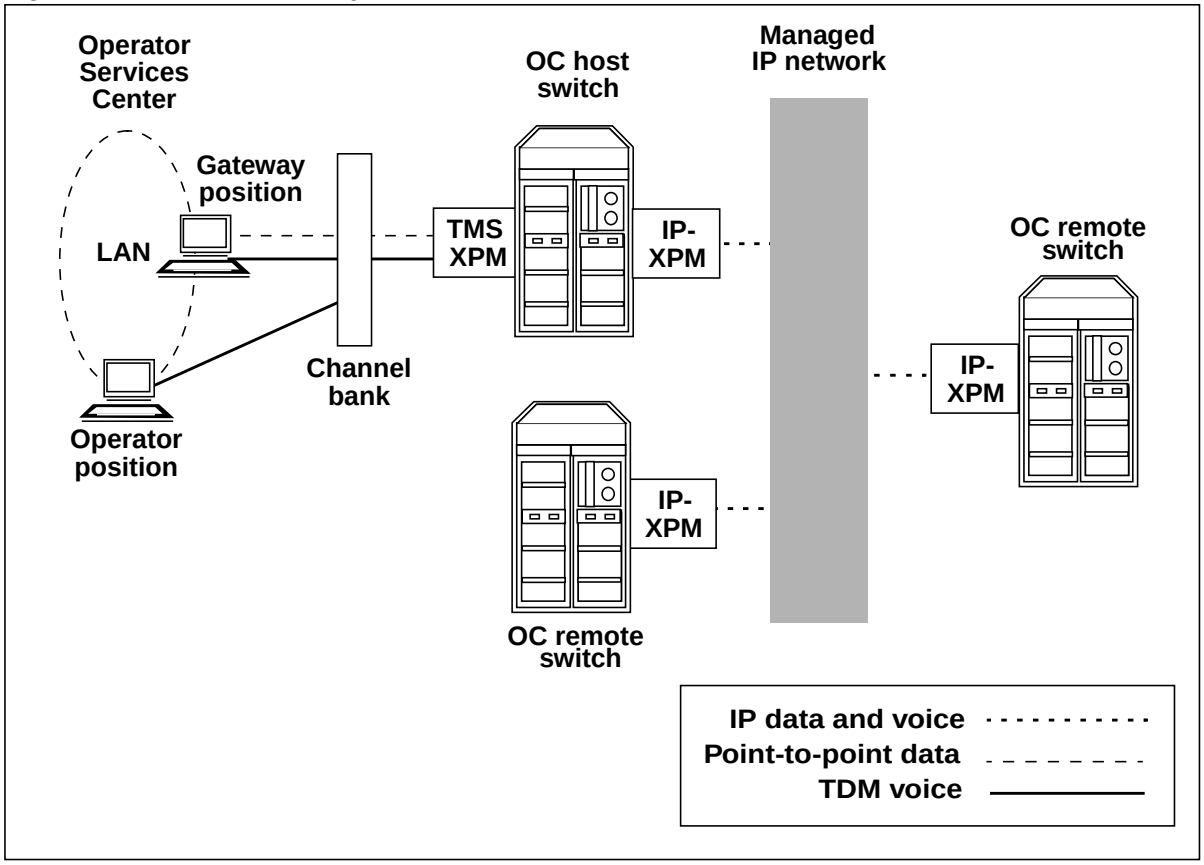


Note: Although not shown in the figure, the three TOPS switches are also connected to the PSTN in the traditional way.

OC connectivity with TOPS-IP

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 with TOPS-IP



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.

TOPS QMS MIS-IP application

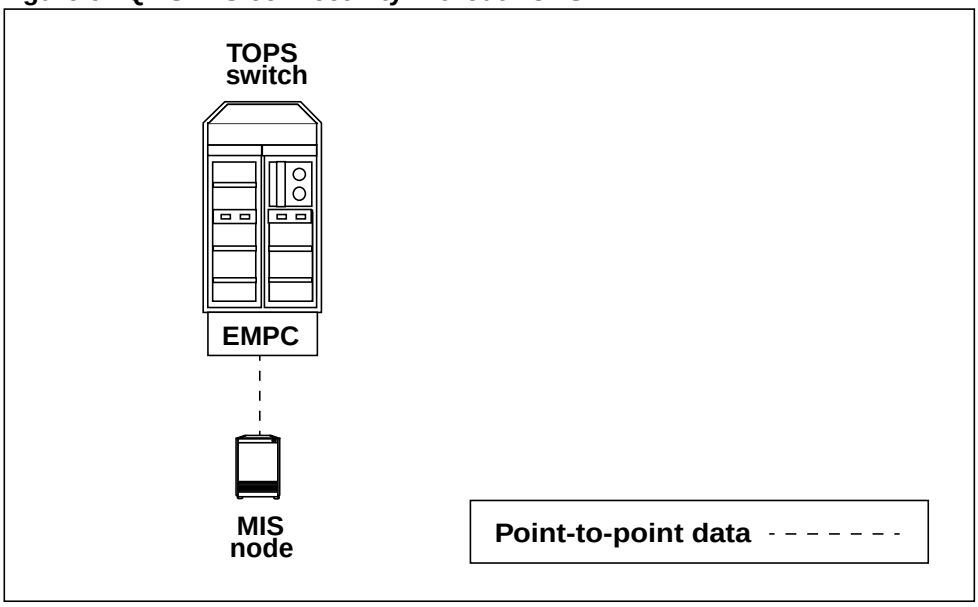
TOPS QMS MIS is a switch application that collects event-driven data about TOPS calls. The switch sends this data to an external reporting facility, such as an MIS vendor node. The data is used to report statistics on TOPS QMS call queues and operator positions.

Note: The flow of QMS MIS data is one-way only, from the switch to the MIS node.

QMS MIS connectivity without TOPS-IP

Figure 6 shows an example of the traditional connectivity for TOPS QMS MIS. In the figure, TOPS QMS MIS data is through a point-to-point (X.25) interface and an enhanced multiprotocol controller (EMPC) card.

Figure 6 QMS MIS connectivity without TOPS-IP

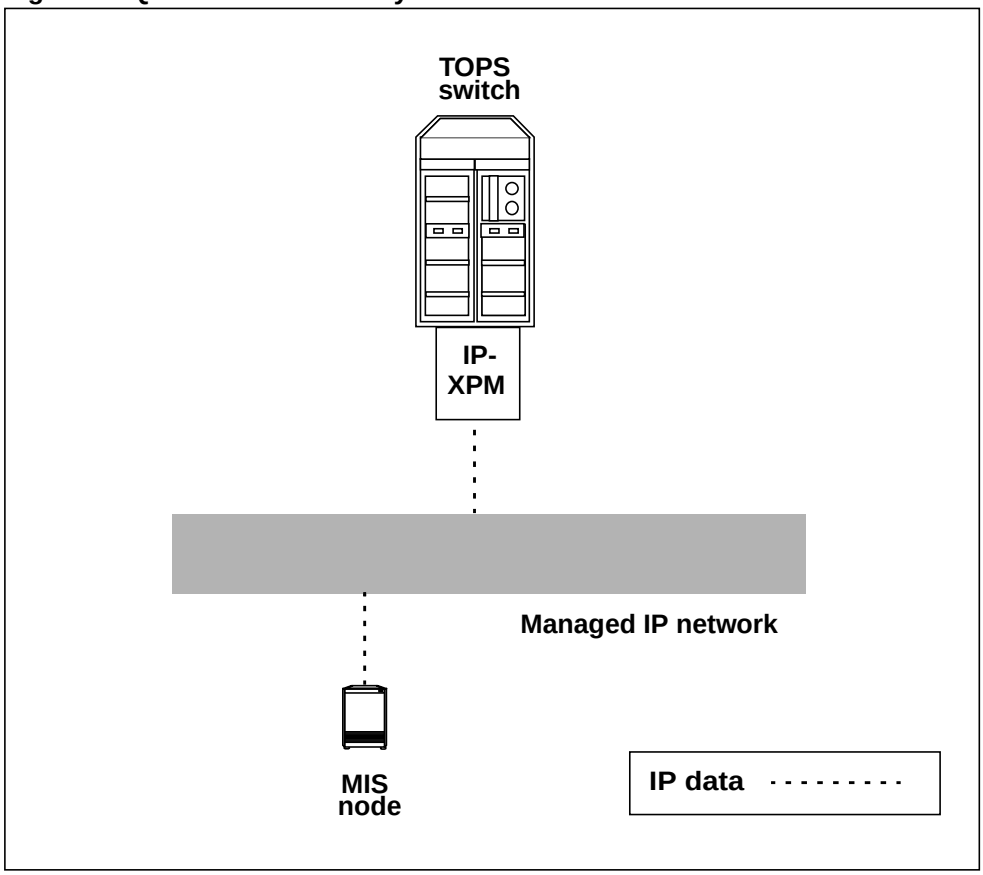


Note: TOPS QMS MIS connectivity differs from OSSAIN QMS MIS connectivity, which is through an Ethernet interface and a peripheral module equipped with an Ethernet interface unit (EIU). For TOPS15, provisioning of Ethernet data for the OSSAIN MIS application is unchanged.

QMS MIS connectivity with TOPS-IP

Figure 7 shows an example of QMS MIS-IP connectivity in a TOPS-IP network. The IP-XPM that supports QMS MIS-IP must be a dedicated peripheral that does not contain 7X07 Gateway cards (used only for voice over IP applications). In the figure, a common IP infrastructure replaces the provisioning of X.25 data for the TOPS QMS MIS-IP application.

Figure 7 QMS MIS connectivity with TOPS-IP



Note: The QMS MIS-IP peripheral cannot be used to support the OC-IP application.

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 TOPS QMS MIS-IP application.
- Chapter 5 discusses the limitations and restrictions for TOPS-IP capabilities in the network.
- Chapter 6 provides information on planning and engineering for TOPS-IP, focusing on requirements for performance, capacity, and provisioning.
- Chapter 7 describes datafill requirements for TOPS-IP, focusing on the CM datafill needed to provision the IP infrastructure and TOPS-IP applications.
- Chapter 8 discusses ordering codes for the TOPS-IP product.
- Chapter 9 describes DMS switch maintenance activities associated with TOPS-IP applications.
- Chapter 10 describes related command interface (CI) tools.
- Chapter 11 shows examples of switch log reports.
- Chapter 12 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).

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 *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, *Coding of Speech at 8kbits/s Using Conjugate Structure Algebraic-Code-Excited-Linear-Predication (CS-ACELP)*
  - ITU-T (H.225), *Media Stream Packetization and Synchronization on Non-Guaranteed Quality of Service LANs*
  - 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*
  - 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*

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

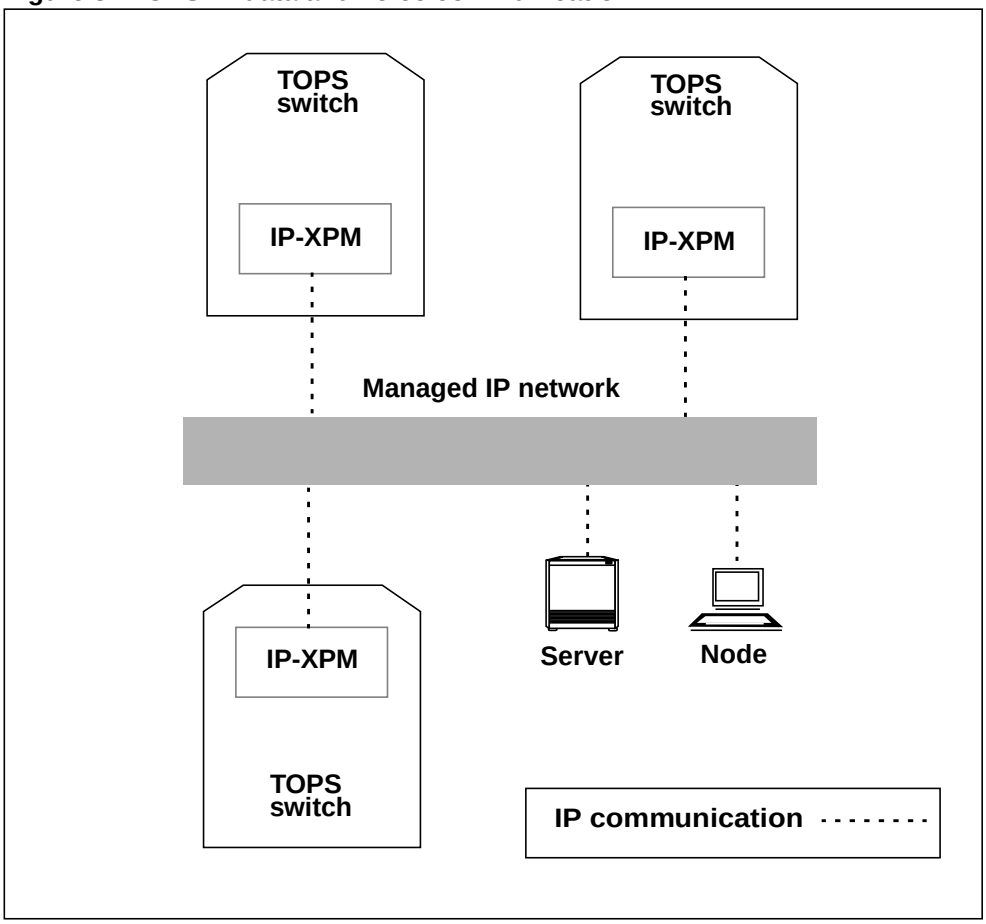
Part 2: Functional description

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 8 for a simple topology.

Figure 8 TOPS-IP data and voice communication



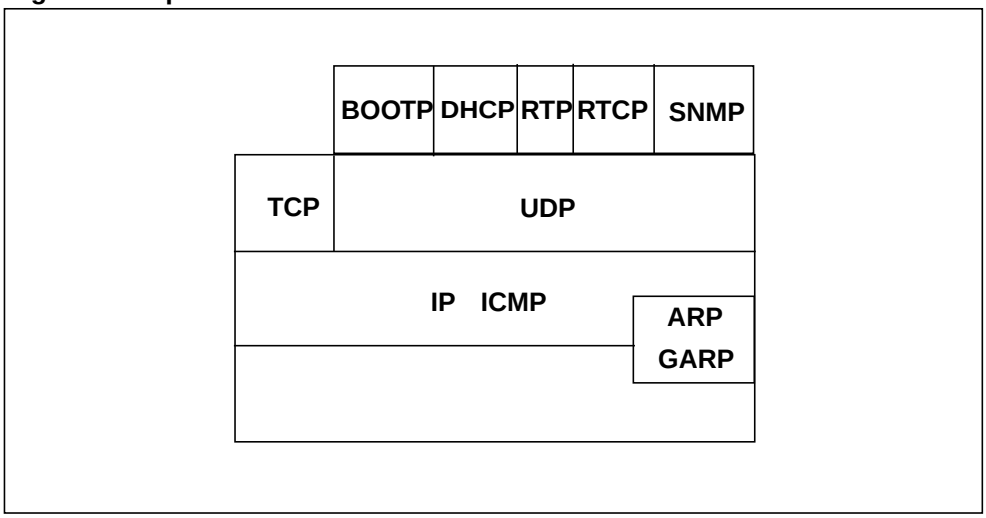
This chapter discusses how the IP-XPM provides data and voice communication, focusing on the following areas:

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

Figure 9 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).
- 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) and Gratuitous ARP (GARP) are 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.

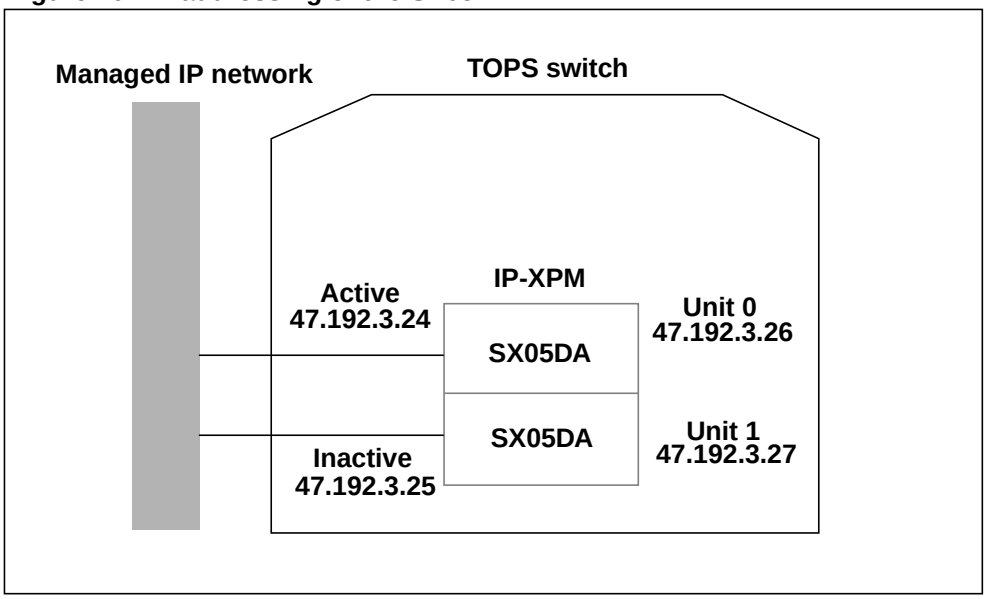
IP addressing of the SX05DA card

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.The CM does not use an IP address; rather, a CM IP application uses the IP address of the SX05DA as its IP address.

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 10 shows IP addressing of the SX05DA cards.

Figure 10 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

GARP 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 GARP 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 different applications. Refer to Chapter 6: “TOPS-IP engineering guidelines” for 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, 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 55 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 "Redundancy in the managed IP network" on page 144.

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, port numbers, and protocols, 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. The operation of RSI is transparent to 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 any of three industry-standard codecs.
- It can support up to 480 simultaneous voice connections on each IP-XPM (North American applications).

  Note: C-side link capacity, however, may not allow use of all 480 connections for OC-IP calls. Details are in Chapter 6: “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.

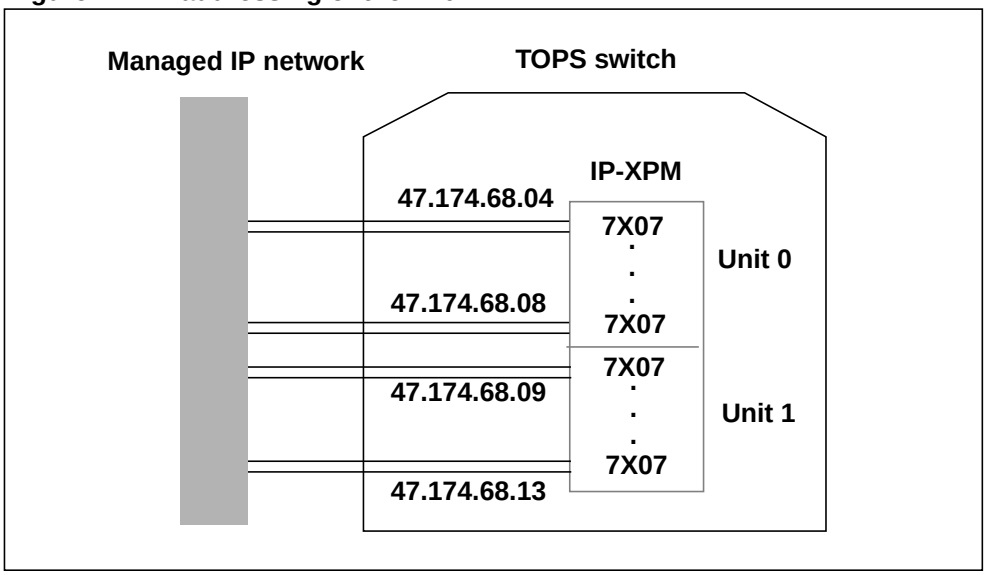
As with the 6X50 interface cards, all 7X07 Gateway cards provisioned in an IP-XPM are used by the active unit regardless of the physical unit location of the cards. They perform the following functions for the IP-XPM:

- They provide packetized voice over the network.
- They provide call setup signaling associated with the voice channels between Gateways 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 11 shows IP addressing of the 7X07AA cards.

Figure 11 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 6: “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 the IP-XPM with the loadfile name and the IP addresses of all the Gateway cards. 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 “Redundancy in the managed IP network” on page 144.

H.323 protocol suite

H.323 specifies a set of standard interfaces for data, voice, and video communication among a diverse set of cooperating terminals in a packet-switched network. From these interfaces, the 7X07 Gateway card uses RTP and RTPC for the media stream and its associated control packets. For call signaling, the 7X07 uses a proprietary protocol that incorporates elements of both H.323 and ISUP. This protocol is referred to as IGIP (ISUP Gateway Interworking Protocol).

Voice encoding

For voice encoding, the 7X07 uses codecs from the H.323 standards. Codecs are algorithms used to convert between TDM voice and packetized voice. A codec takes a sample of voice, converts it according to the appropriate algorithm, and surrounds it with additional information required by an IP packet.

Codecs supported

Although codec selection is determined by CM datafill, the 7X07 Gateway card supports all the following codecs:

- G.711 Mu-law 64K
- G.729A with no silence suppression
- G.729A with silence suppression per G.729 Annex B

An uncompressed voice stream uses the G.711 codec and provides carrier-grade voice quality at the expense of increased bandwidth. A compressed voice stream uses the G.729A codec and consumes less bandwidth, but provides lower voice quality. Both codecs use UDP at the transport layer.

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 card 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. This task is achieved by automatically datafilling blocks of trunk members when the Gateway card is datafilled. Manual additions and deletions to individual trunk members are *not* allowed for 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 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 9: "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 number of available dynamic trunks" on page 69 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 9: "TOPS-IP maintenance activities."

ISUP call processing

Dynamic trunking applications use ISUP signaling internally at the switch between the CM and the XPM. TOPS-IP applications convert both the ISUP call control and the voice (bearer) into IP messages, whereas other applications use the existing SS7 network for call control and either IP or ATM for bearer. TOPS-IP applications do not use the SS7 network.

Overview of datafill for IP data and voice

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: Details on how a particular TOPS-IP application uses these tables (and other application-specific tables) are in the individual chapter that discusses the application. Details on table dependencies and the range of valid datafill for every table affected by TOPS-IP are in Chapter 7: "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)
   - TQCQINFO (TOPS Call Queue Information)

LTCINV

Table LTCINV specifies hardware inventory information for each XPM (excluding the P-side link assignments). Datafill values include the IP-XPM type and number and other data associated with its processors 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 QD715 load)
- OPTCARD (for the messaging card)
- TONESET (for North America)

  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 (for IP-XPM firmware load)
- OPTATTR (for CCS7)

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

The following example shows three IP-XPMs, DTC 10, DTC 11, and DTC 20.

Figure 12 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  QD715XX (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         SXFWAG04     (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0    6X02AF   QD715XX (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          SXFWAG04    (CCS7) $
       6X40FC    N
DTC 20  1002   LTE    0    51    0     C   0    6X02AF   QD715XX (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          SXFWAG04    (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 (for DTCs)
- TMPLTNM (for 7X07 Gateway cards)
- 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

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

Figure 13 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).

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 222.

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

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 an MIS-IP data link). No Gateway cards are installed, so the P-side links remain NILTYPE.

Figure 14 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) $

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 card. A gateway router is a component of the managed IP network and is used to forward IP packets to other networks.

When the CM method is used to configure the SX05DA (specified in table XPMIPMAP, page 61), the switch downloads appropriate router information 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 6: "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 15 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 16 MAP display example for table XPMIPMAP

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

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 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 "GARP broadcast message" on page 49.)

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 222.

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 local IP transport service names. Each service name represents a software port and transport protocol. The service name is referenced by table IPCOMID.

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

Figure 17 MAP display example for table IPSVCS

```
SERVICE            PORT       PROTOCOL
-------------------------------------------------------------------
FREEPORT           0          TCP_UDP
OCIPSVC            8600       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: Each TOPS-IP application has its own recommendation for port values; details are in the separate chapter that describes each application.

PROTOCOL field

PROTOCOL specifies the type of IP 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.

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 TOPS-IP applications. 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.

The following example shows datafill for four COMIDs. DTC 10 is used for two COMIDs, and DTC 11 is used for one. Both DTC 10 and DTC 11 support the port and protocol identified by OCIPSVC. DTC 20 supports the port and protocol for QMSMIS. A brief description of each field follows the example.

Figure 18 MAP display example for table IPCOMID

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

COMID field

COMID identifies the tuple. The COMID is referenced by other 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. (For details on how an application datafills the COMID, refer to the separate application chapters in this book.)

SERVICE field

SERVICE specifies the tuple in table IPSVCS, which identifies the port and protocol. Multiple COMIDs may use the same service name as long as the associated port is on a different XPM.

XPMNAME field

XPMNAME specifies the IP-XPM datafilled in table XPMIPMAP that is used for the particular COMID.

CLLI

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

Figure 19 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, member selection algorithm, and translations and screening attributes for a given trunk group. Dynamic trunks use the IT (intertoll) trunk group type. Table TRKOPTS, where trunk groups are defined as dynamic, enforces this restriction.

Note: The direction of the dynamic trunk group is important for TOPS-IP voice communication. Outgoing (OG) trunk groups are used exclusively to communicate with offices that are defined as OC hosts, whereas two-way (2W) trunk groups are used to communicate with OC remotes. For more information, refer to Chapter 3: "TOPS OC-IP application."

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

Figure 20 MAP display example for table TRKGRP

```
GRPKEY         GRPINFO
-------------------------------------------------------------------
OCIPTOREMOTE   IT 0 TLD NCTC 2W IA MIDL 000 NPRT NSCR 619 619 000 N N $
OCIPTOHOST     IT 0 TLD NCTC OG IA 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

The following example shows datafill for the two trunk groups.

Figure 21 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
```

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)

The following example shows datafill for the two trunk groups.

Figure 22 MAP display example for table TRKOPTS

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

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 Gateway name is referenced by table IPINV as well as by application-specific tables.

Note: Gateway does not refer to a gateway router.

The following example shows datafill for the TGWY site name, which uses six Gateway cards. 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 23 MAP display example for table SITE

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

IPINV

Table IPINV defines the individual 7X07 Gateways at the CM. Datafill values include the site name, the XPM name, P-side port, and Gateway type and refinements.

The following example shows the TGWY site datafilled with a total of six Gateway cards. Two trunk groups, OCIPTOREMOTE and OCIPTOHOST, are datafilled across two IP-XPMs (DTC 10 and DTC 11). Each trunk group supports 144 members. A brief description of each field follows the example.

Figure 24 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
```

IPNO field

IPNO associates the name of the site (datafilled in table SITE) with a unique Gateway frame and unit number pair. (For details on a numbering method for Gateways, refer to page 186.)

PMTYPE field

PMTYPE specifies the XPM type 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. 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 details, refer to “LTCPSINV-to-IPINV port mapping” on page 186.

IPZONE field

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

Note: TOPS Gateways require the correct IP address in the IPZONE field. In an OC host switch, 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. Refer to Chapter 3: "TOPS OC-IP application" for details on IPZONE.

GWTYPE field

GWTYPE defines the type of Gateway. Datafill also includes refinements based on the Gateway type, such as trunk group and starting range of trunk members. The example datafill shown in Figure 24 is as follows:

- TOPS represents a TOPS-IP application, such as OC-IP.
- OCIPTOREMOTE and OCIPTOHOST represent the CLLIs of the dynamic trunk groups.
- 0 represents the *start* of the trunk members 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.

After datafilling the Gateway cards, table IPINV automatically datafills the trunk members in table TRKMEM.

Note 1: Removing TOPS entries in 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: 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 3: Refer to table TOPSTOPT 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, table IPINV *automatically* datafills table TRKMEM, so manual datafill is not allowed. The following example shows partial datafill for the dynamic trunk groups.

Figure 25 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 47       0    DTC 10 7 24
 . . . . . .
OCIPTOHOST 96         0    DTC 11 10 1
OCIPTOHOST 97         0    DTC 11 10 2
OCIPTOHOST 98         0    DTC 11 10 3
 . . . . . .
OCIPTOHOST 143        0    DTC 11 11 24
```

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 total number of dynamic trunks that are available for call processing.

Limiting the number of available dynamic trunks

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.

Each Gateway card supports 48 trunk members. When a maximum is datafilled in MAXCONNS, the switch loops over all in-service Gateway cards for the affected trunk group and calculates a member limit for each card. This allows the maximum specified to be distributed across all in-service Gateway cards. So, for example, if MAXCONNS is set to 100, and three Gateway cards are associated with the trunk group, the first card is limited to 34 members and the second and third cards are limited to 33 each. The system automatically adjusts this distribution as Gateway cards go into and out of service.

Note 1: Additional information in table TOPSTOPT is not used for dynamic trunks and should be datafilled with default values.

Note 2: For details on how the switch makes trunks unavailable for call processing, refer to "Limiting the use of dynamic voice links" in Chapter 9: "TOPS-IP maintenance activities."

Note 3: For details on capacity engineering, refer to Chapter 6: "TOPS-IP engineering guidelines."

The following example shows datafill for the two trunk groups.

Figure 26 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. 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: Any change in the value of this parameter requires the Gateway to be reloaded.

- NUMPERMEXT allocates data structures for calls. For TOPS-IP voice applications, this value should be incremented by one for each member of a dynamic trunk group that has a direction of OG (outgoing) in table TRKGRP.

  Note: For members of host trunk groups (defined with a direction of 2W in TRKGRP), this parameter should not be incremented.

- 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. (TOPS-IP does not change the use of this parameter.)

- 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. (TOPS-IP does not change the use of this parameter.)

The following example shows datafill for these OFCENG parameters.

Figure 27 MAP display example for table OFCENG

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

PKTVPROF

Table PKTVPROF defines profiles used for packetized voice. The profile index specifies a voice codec and is referenced in table TQCQINFO by call queue. The codecs supported are G.711 and G.729. If G.729 is datafilled, silence suppression may also be specified. The use of silence suppression discontinues the codec output if it detects parts of a signal where there is no speech. NOSILSUP (default) specifies no silence suppression; SILSUP specifies silence suppression.

Note 1: Datafilling the G.729 codec is not recommended if carrier-grade voice is required.

Note 2: Table PKTVPROF contains two default tuples, 0 and 1.

The following example shows datafill for three packetized voice profiles.

Figure 28 MAP display example for table PKTVPROF

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

TQCQINFO

Table TQCQINFO defines TOPS call queues, including the packetized voice profile index that applies to the call queue. The following example shows datafill for three packetized voice profile indexes against call queues.

Figure 29 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         1
CQ133  TOPS_TA  500    1000   VACT    N         2
```

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

OC background

In the 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.

OC data and voice connectivity

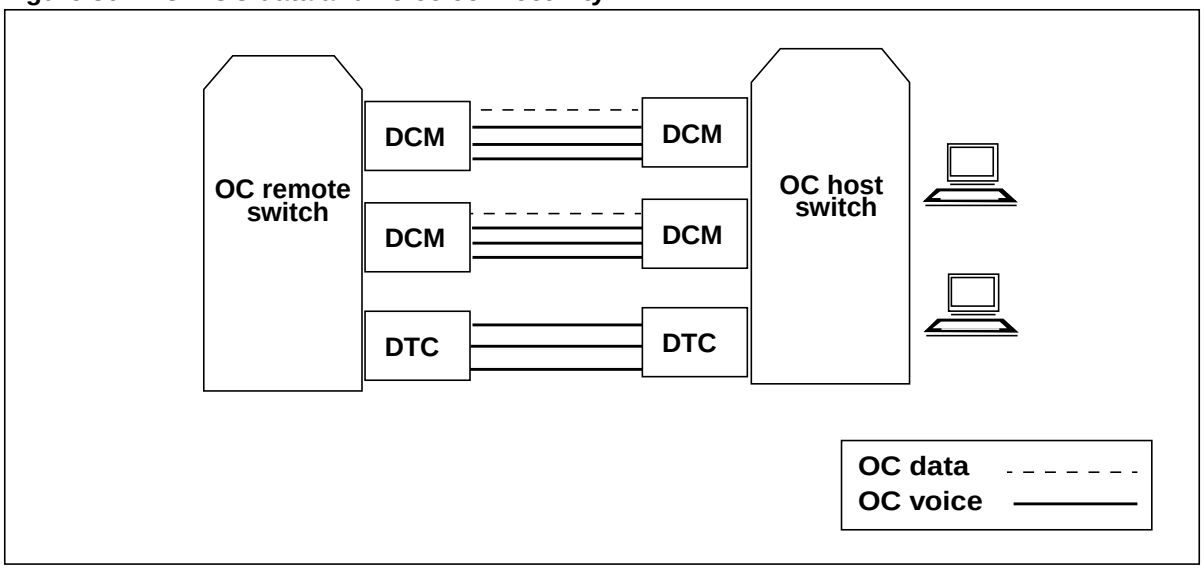
The OC data links are used for call control messages, key function messages, and screen update messages. One data link can be shared by many calls in progress. In a traditional OC configuration, the data links can be provisioned on either Digital Carrier Module (DCM) or Enhanced TOPS Message Switch (ETMS)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

The OC voice links 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 traditional 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 30 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 30 DCM OC data and voice connectivity



Note: DCM OC, the original TOPS OC product, is still supported in TOPS15, although DCMs are no longer manufactured or sold.

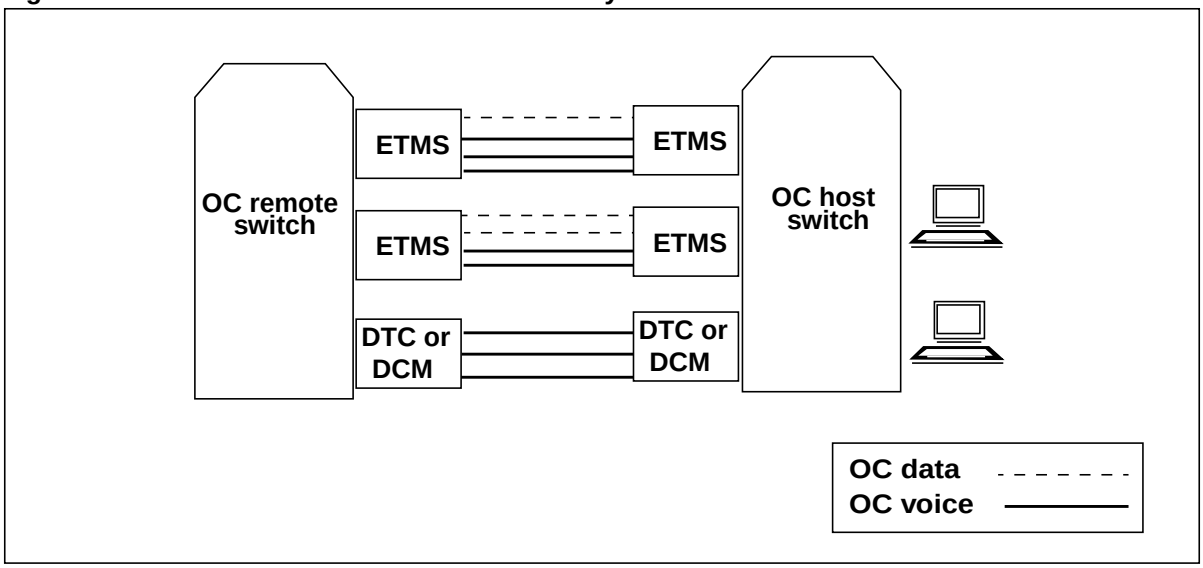
ETMS OC connectivity

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 31 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.

Figure 31 ETMS OC data and voice connectivity



Traditional OC call flow

Figure 32 shows an example of a traditional OC call flow that illustrates the use of voice and data links. The arrows represent data messages sent and received on the data links. The data messages describe both OC data and OPP data. Use of voice links is described in the text.

Figure 32 Example of traditional OC call flow

OC remote switch events and processing	OC host switch events and processing	Position events and processing
A call arrives on a TOPS-supported trunk in the remote and is routed to TOPS.		
The remote selects an OC data link and sends to the host an OC Request Operator message.		
OC message: Request Operator →		
	The host selects an operator, selects an OC voice link, and connects the OC voice link to the TDM position voice link.	
	The host sends to the remote an OC Got Operator message.	
← *OC message: Got Operator*		
The remote allocates a CF3P circuit and connects the operator and the caller.		

OC remote switch events and processing	OC host switch events and processing	Position events and processing
The remote sends to the host an OPP Call Begin message and some OPP Call Update messages in a series of OC screen update messages.		
OC message: OPP Call Begin → . . . *OC message: OPP Call Updates* →		
The remote sends call arrival tones to the operator over the OC voice link. (These tones are not heard by the caller.)		
	The host forwards the screen update messages to the operator position.	
	OPP message: Call Begin → . . . *OPP message: Call Updates* →	
The call is established and data messages are processed.		The caller and operator begin conversation.
When the call is complete, the remote releases its end of the OC voice link. The remote sends to the host an OC Release Operator message.		
OC message: Release Operator →		
	The host sends to the remote an OC Release Operator Acknowledgment message. The host also sends to the position an OPP Call End message.	
OC message: Release Operator Ack ←		
		OPP message: Call End →
	The host releases the voice link and places the position in the idle queue.	
	The host generates an AMA record.	

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 secondary 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.

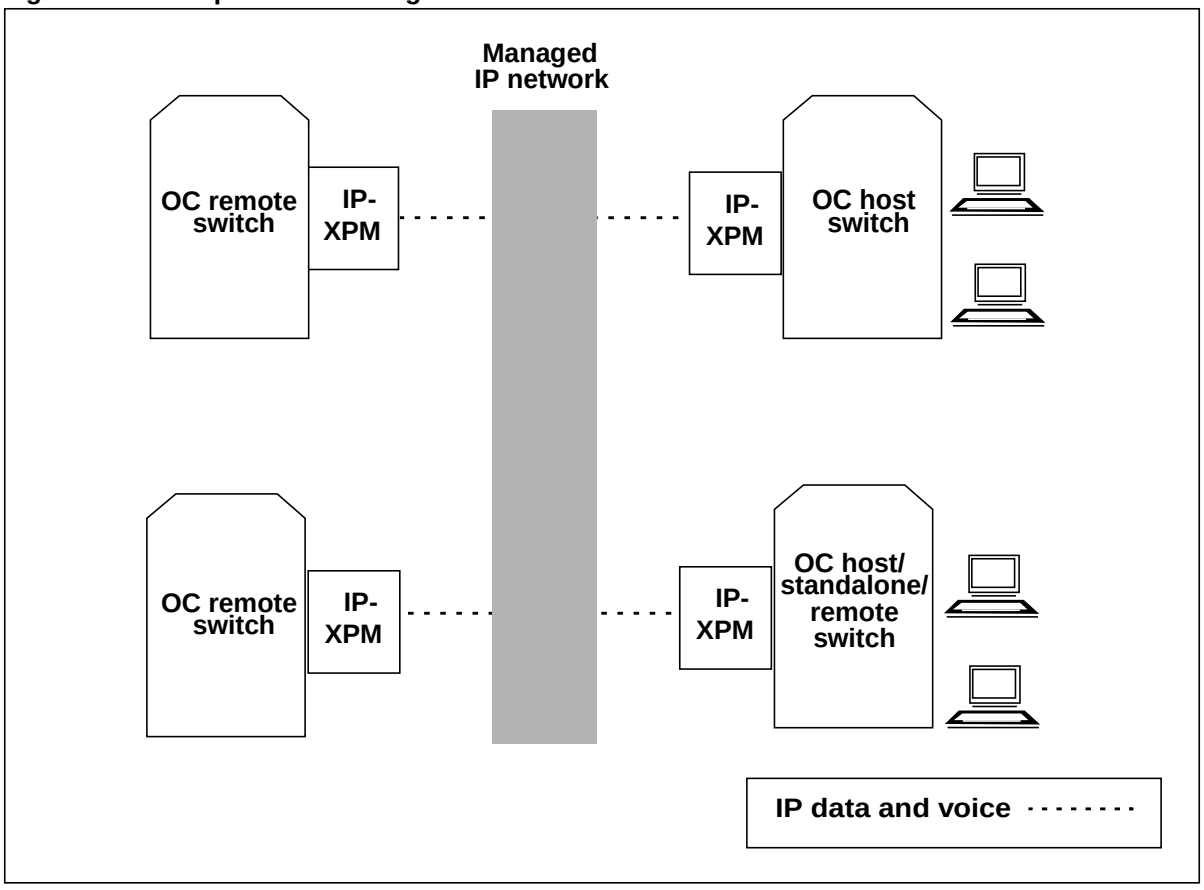
OC-IP introduction

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 data and voice traffic for OC calls 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 in the call 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.

Figure 33 shows an example OC-IP configuration.

Figure 33 Example OC-IP configuration



OC-IP data communication

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

IP-XPM data interface

The SX05DA processor card provides OC-IP data communication, which is used for call control, key function, and screen update messaging between the OC host switch and the OC remote switch.

OC-IP data links

The OC-IP application does not have a 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-IP data link uses the P-side Ethernet LAN connection in the IP-XPM instead of using a P-side DS1 port. Therefore, a data link no longer represents any particular *physical path* to the distant switch. Depending on how the 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 for both of the connection endpoints—the local end and the distant end—of each data link it uses.

An IP connection endpoint is represented by a socket, which is a software entity identified by an IP address and a port. IP addresses are used to route IP packets to the correct node on the network. For OC-IP data links, this means routing call control, key function, and screen update messages to the correct IP-XPM at the correct distant TOPS switch.

Ports are used in routing messages to the correct application after the correct node on the network has been reached. For OC-IP data links, this means routing OC data link messages from the IP-XPM to the switch CM software that “knows” about that particular data link. These are software ports, and they are unrelated to any hardware port.

The local 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. Each OC-IP data link is associated through datafill with a unique COMID.

Related switch datafill

The switch datafill for the local connection endpoint of an OC-IP data link identifies the IP-XPM whose SX05DA provides the data link LAN connectivity. Datafill also identifies a local port number that distinguishes this data link on the IP-XPM from any other data links or applications that might be using the XPM for IP connectivity. Datafilling the IP-XPM specifies its active IP address indirectly.

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 IP-XPM 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 PINs and calling card numbers.

OC-IP voice communication

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

IP-XPM voice interface

The 7X07AA Gateway card 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.

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.

The IP-XPM handles OC-IP calls differently from SS7 ISUP calls. With OC-IP, the CM includes proprietary information such as terminal identifiers (TID) in the IAM message used to establish the voice connection. Traditional ISUP call processing routes and receives messages from the SS7 network through the LIU7, whereas OC-IP ISUP call processing routes and receives messages through the IP-XPM. The 7X07 Gateway card in the IP-XPM then converts both the ISUP call control and the voice into data packets for the managed IP network.

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

Voice signaling

To set up voice connections between Gateways across the managed IP network, OC-IP uses a proprietary protocol, IGIP, that incorporates elements of both H.323 and ISUP. Gatekeepers are not used.

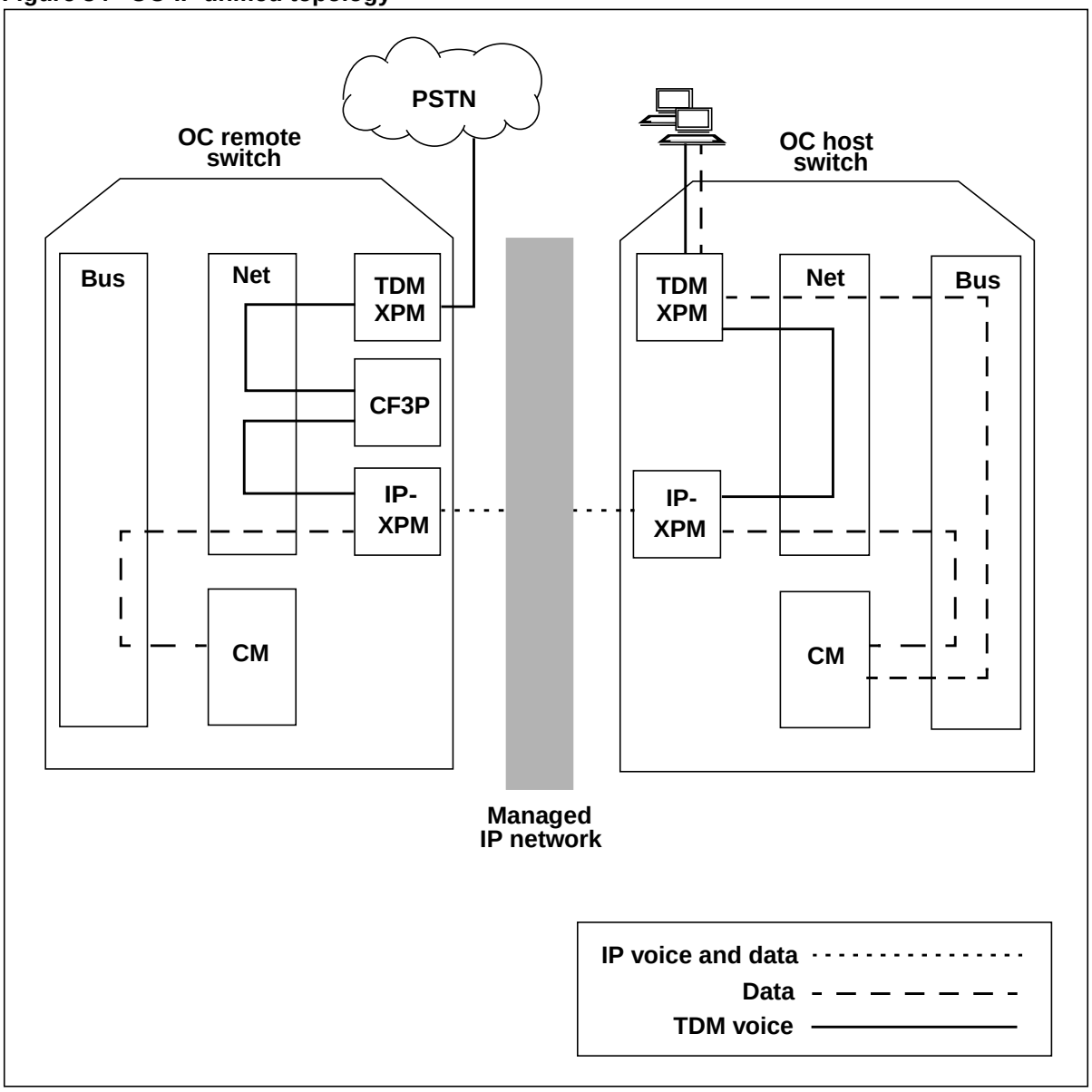
Voice encoding

The G.711 and G.729A codecs, also from the H.323 protocols, are used for voice encoding. G.711 provides uncompressed voice and G.729A provides compressed voice. An uncompressed voice stream provides carrier-grade voice quality at the expense of increased bandwidth; whereas compressed voice consumes less bandwidth but provides lower voice quality. Both codecs use the UDP data transport.

OC-IP unified topology

Figure 34 illustrates the paths for voice and data in the OC-IP unified topology. A description follows the figure.

Figure 34 OC-IP unified topology



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 switch. The OC voice link connects to the same CF3P and terminates to the C-side of the IP-XPM 7X07 Gateway card. The IP-XPM converts TDM voice to either G.711 or G.729A packetized voice and presents the voice stream to the managed IP network. The IP-XPM also converts between ISUP call control signaling on the CM side and IGIP signaling on the managed IP network side.

Mixing OC-IP and traditional OC

OC-IP and traditional DCM or ETMS OC can coexist in the same switch. For example, an OC host can use IP voice and data with one of its remotes, and ETMS OC with another remote. It is also possible, between a single host-remote pair, for some call queues to use OC-IP voice and data and for other call queues to use traditional OC voice and data. (This is accomplished by using HRNQT, and by having each switch assign two different office names to the other switch in table OCOFC.)

Note: For any OC office datafilled in table OCOFC, IP connectivity must be used for *both* OC voice and OC data, or for neither. A call cannot use traditional TDM-based OC voice links and OC-IP data, or vice versa.

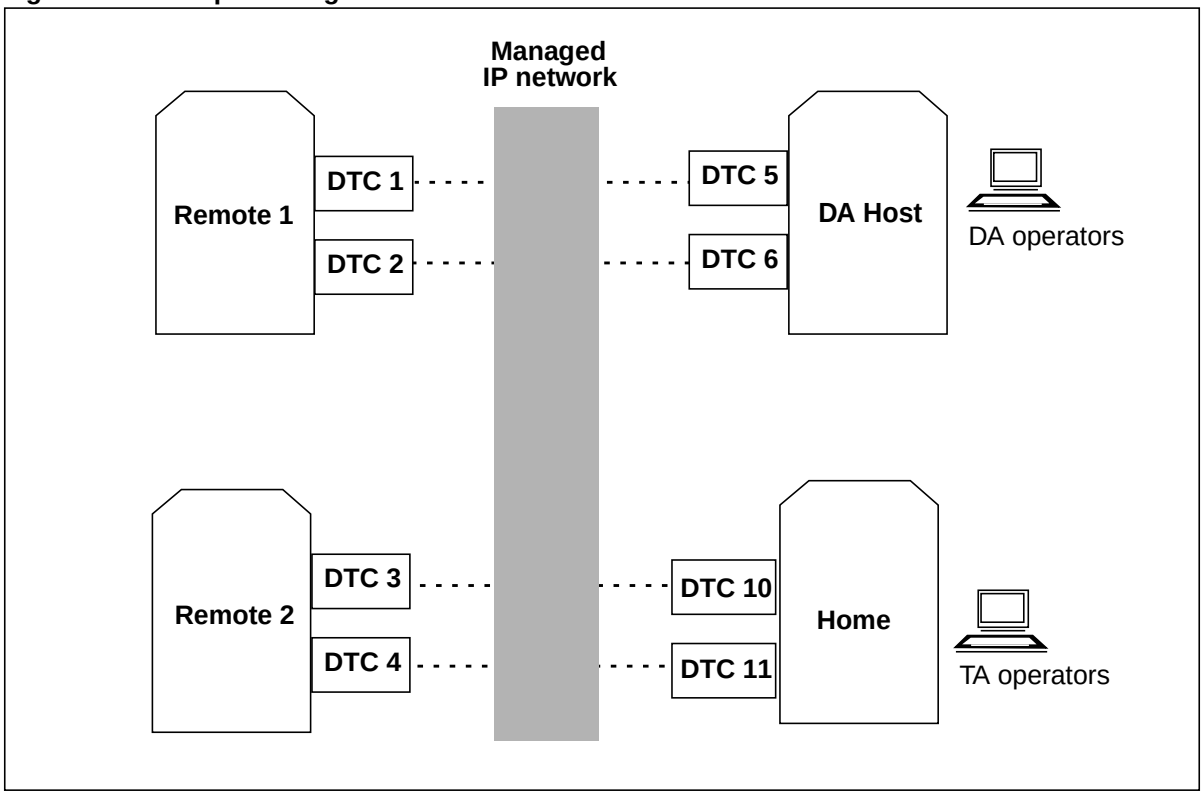
Overview of datafill for OC-IP data links

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 35.

Note 1: The OC-IP application does not affect the datafill for TDM positions. However, table TOPSPOS was modified in TOPS15 as part of the preparatory work for IP positions.

Note 2: Details on the range of valid datafill for every table affected by TOPS-IP are in Chapter 7: "TOPS-IP data schema."

Figure 35 Example configuration for OC-IP data communication



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.

In addition to the OC data-related tables, the base IP infrastructure data-related tables are shown in this discussion for completeness. 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)

LTCINV

Table LTCINV contains the inventory datafill for the SX05DA used for OC-IP data link connectivity. In the following example, the Home switch datafills DTC 10 and DTC 11 with the QD715 load name and SX05DA circuits.

Figure 36 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  QD715XX (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         SXFWAG04     (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0     6X02AF   QD715XX (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         SXFWAG04     (CCS7) $
       6X40FC    N
```

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.

Note: When the CM method is used to configure the SX05DA, the switch downloads appropriate gateway information to the XPM when it is brought into service. This information corresponds to the router indexes that are datafilled in table XPMIPMAP. When the DHCP method is used to configure the SX05DA, datafill in table XPMIPGWY is never used.

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

Figure 37 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
```

XPMIPMAP

Table XPMIPMAP specifies IP information for the IP-XPMs. Datafill values include Ethernet speed, subnet mask, and the configuration method used to configure the XPM. When CM is datafilled as the method, this table also specifies the IP addresses of each XPM unit and any router indexes into table XPMIPGWY. When DHCP is datafilled as the method, no further datafill in this table is required, and no datafill in table XPMIPGWY is used.

In the following example, the Home switch datafills the DHCP method for DTC 10 and DTC 11.

Figure 38 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
```

IPSVCS

Table IPSVCS defines local IP transport services. Each service name represents a software port and transport protocol. Tuples in IPSVCS used for OC-IP data links may not be used by another application, such as QMS MIS-IP. Also, each OC-IP data link associated with a particular IP-XPM must use a different IPSVCS tuple. However, two data links associated with different IP-XPMs may use the same IPSVCS tuple.

In the following example, the Home switch defines 8 IP transport services for OC-IP data links.

Figure 39 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: It is recommended that OC-IP data links assign port numbers in the range 8600 to 8899. The managed IP network should be designed with these port numbers in mind to minimize loss of data link messages. For more details, refer to Chapter 6: "TOPS-IP engineering guidelines."

Note 2: The OC-IP application does not allow the PROTOCOL value to be set to anything except UDP if the IP transport service is datafilled against a COMID that is used for an OC-IP data link. Neither does it allow PORT to be changed unless the data link is offline.

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. The COMID represents local connectivity information for each data link. The COMID is referenced by table OCIPDL, which associates a data link with it. The service name matches a tuple in table IPSVCS, and so it indirectly specifies a local software port number and transport protocol for the COMID and its associated data link. The XPM name identifies the SX05DA at the Home switch that provides LAN connectivity for the COMID and its associated data link.

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.

Figure 40 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 1: 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).

Note 2: Two different COMIDs may be associated with the same service name only if they are on different IP-XPMs, and two COMIDs may use the same IP-XPM only if they are associated with different service names.

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 41 MAP display example for table OCOFC

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

OCGRP

Table OCGRP identifies each distant office referenced in table OCOFC as a host or remote. Table OCGRP is also used by traditional OC, but has some OC-IP-specific datafill. Datafill values include the office type and the IP voice link groups associated with the distant offices. The data link overlay field includes a selector for IP data connectivity used with a particular office.

Note: IP data connectivity can be used only when IP voice connectivity is used (and vice versa). A call cannot use traditional TDM-based OC voice links and OC-IP data, nor traditional TDM-based data links and OC-IP voice.

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.

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

Figure 42 MAP display example for table OCGRP

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

Note: 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 if some of the OC traffic uses OC-IP and some of it uses traditional OC.

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.

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

Figure 43 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 9: “TOPS-IP maintenance activities.”

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

Figure 44 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 each OC switch is aware of the data links used for IP transport services, so 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:

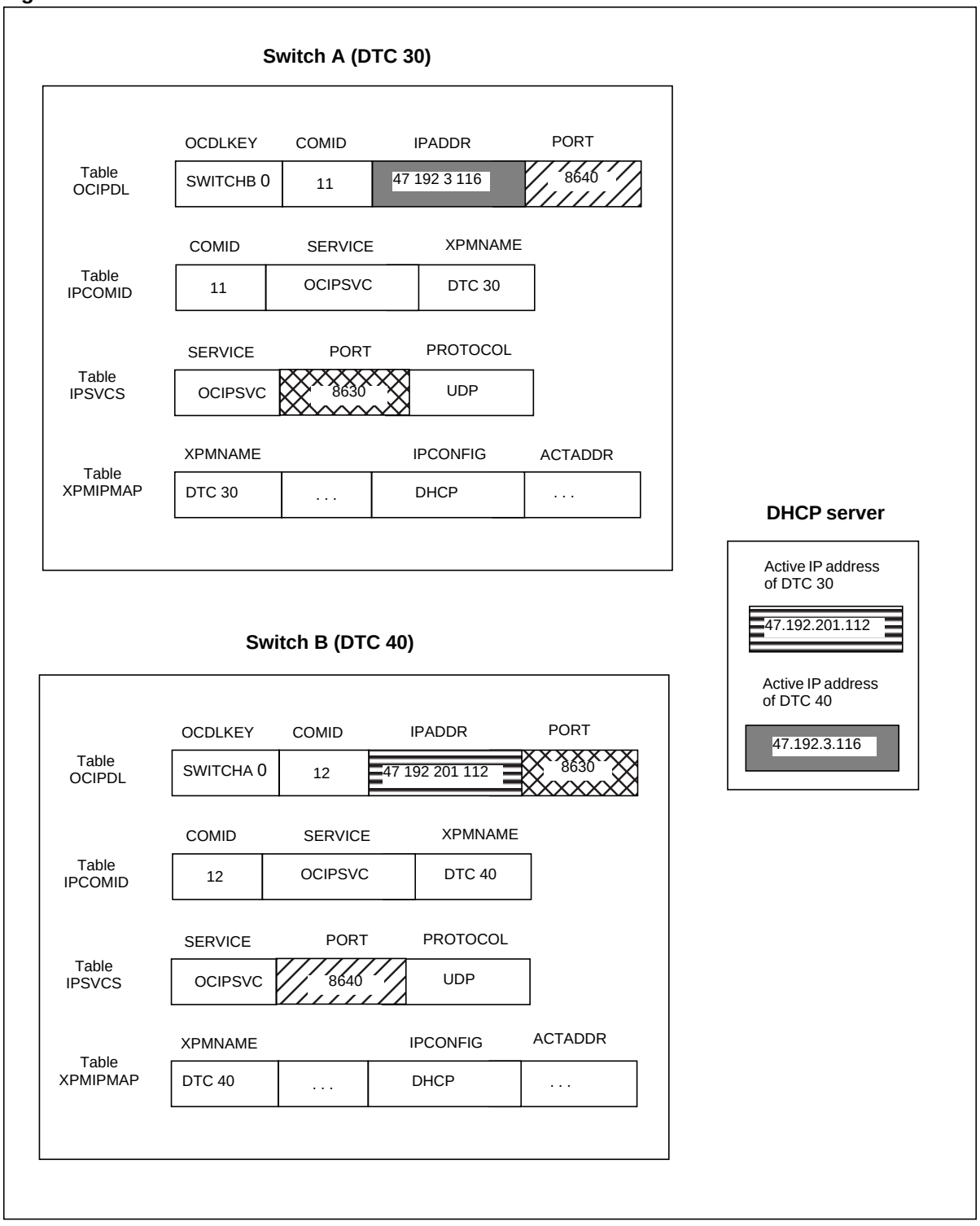
- network method (DHCP)
- CM method

Network method

When using the DHCP method, the IP-XPM receives its active IP address from a DHCP server in the network. Figure 45 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 45 Parallel datafill for OC-IP data links—network method

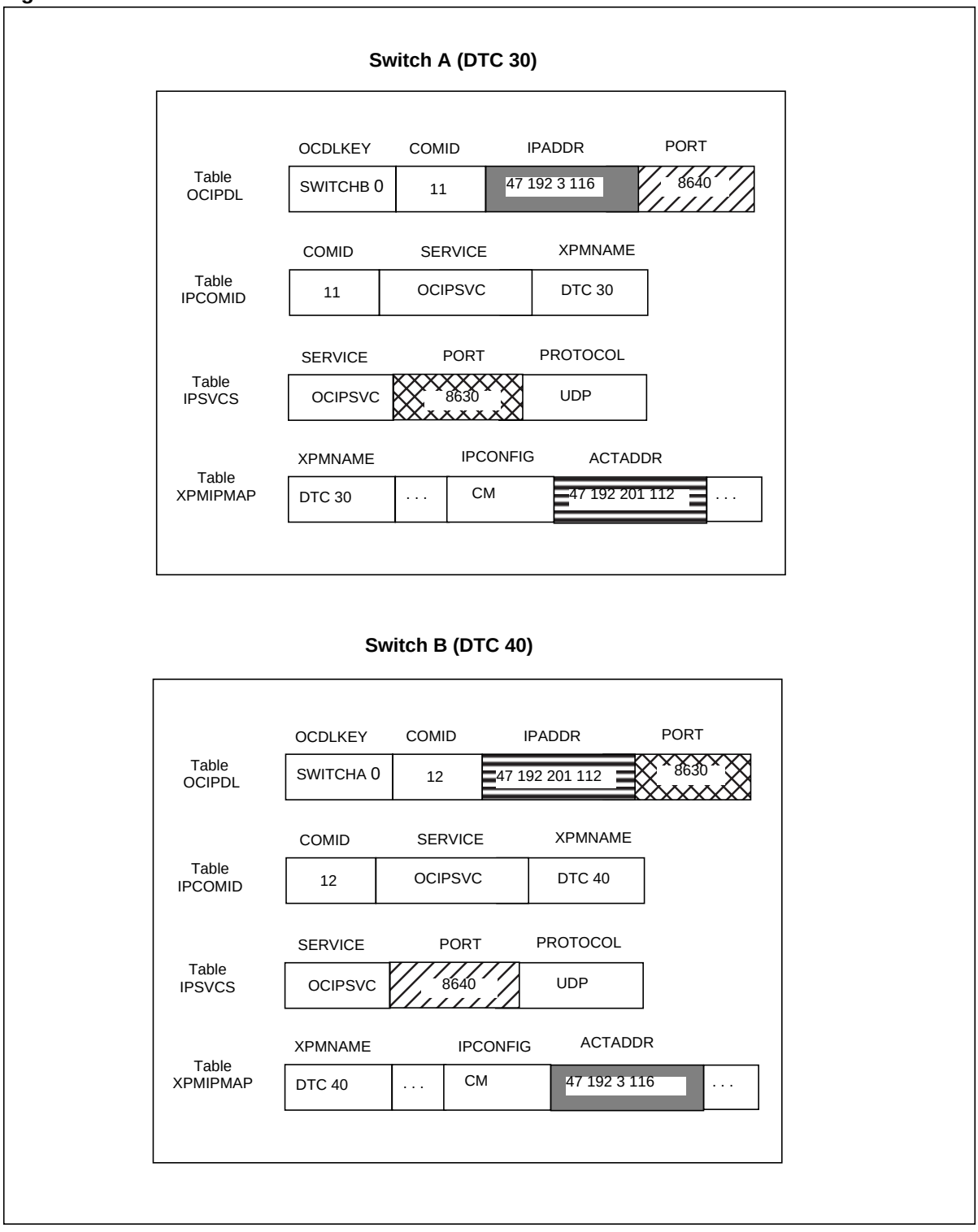


CM method

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 46 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 46 Parallel datafill for OC-IP data links—CM method

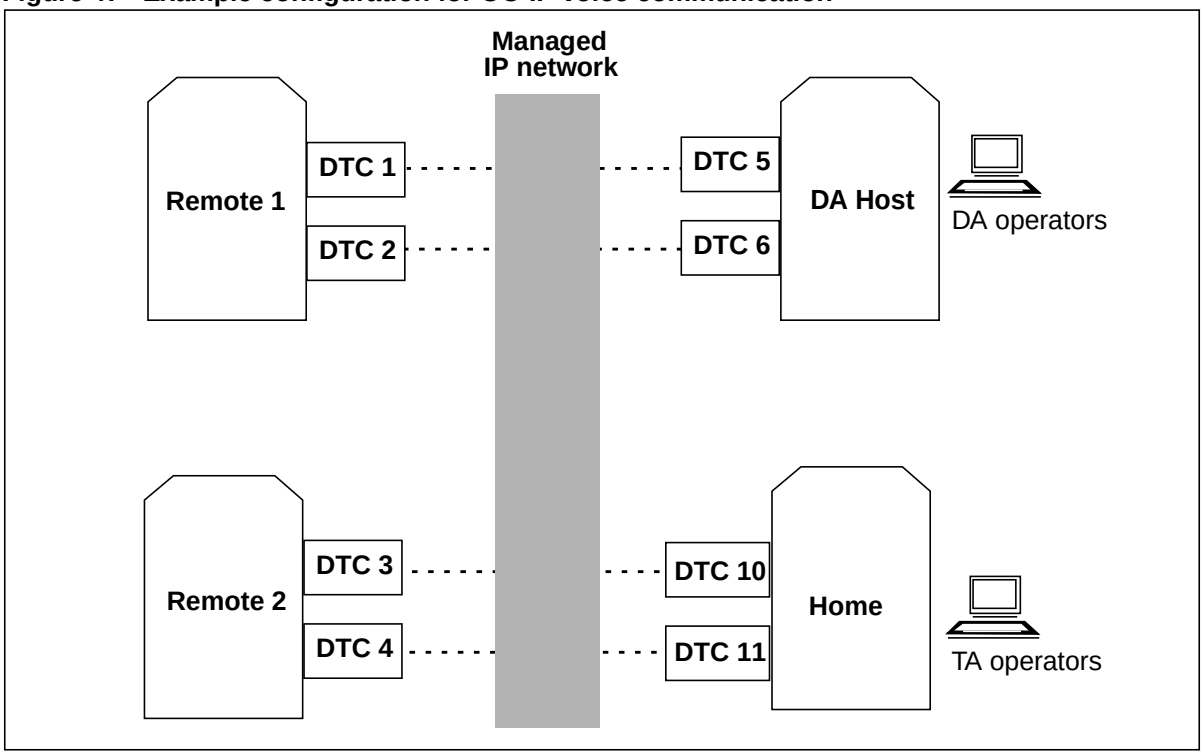


Overview of datafill for OC-IP voice links

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 47.

Note: Details on the range of valid datafill for every table affected by TOPS-IP are in Chapter 7: “TOPS-IP data schema.”

Figure 47 Example configuration for OC-IP voice communication



In addition to the OC voice-related tables, the base IP infrastructure voice-related tables are shown in this discussion for completeness. 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)
- OCFENG (Office Engineering)
- PKTVPROF (Packetized Voice Profile)
- TQCQINFO (TOPS Call Queue Information)
- OCGRP (Operator Centralization Group)

LTCINV

Table LTCINV contains the inventory datafill for the IP-XPM associated with the 7X07 Gateway cards. In the following example, the Home switch datafills DTC 10 and DTC 11 with the North American toneset.

Note: The NORTHAA value is required only to satisfy table control and diagnostics. The IP-XPM does not use this toneset to generate tones.

Figure 48 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  QD715XX (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         SXFWAG04     (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0    6X02AF   QD715XX (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         SXFWAG04     (CCS7) $
       6X40FC    N
```

CARRMTC

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

Figure 49 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 P-side link assignments for the 7X07 Gateway cards in DTC 10 and DTC 11.

Note: 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 222.

In the following example, the Home switch datafills P-side links 6 through 11 for each DTC. These links correspond to the TGWY Gateway ports defined in table IPINV (page 100).

Figure 50 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 the trunk group names and the maximum number of members in any given trunk group. 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 trunk groups, it is not recommended because of its impact on sparing. As described in Chapter 6: “TOPS-IP engineering guidelines,” N+1 redundancy of 7X07 Gateway cards is needed for each trunk group.

In the following example, the Home switch datafills two trunk groups, OCIPTOREMOTE and OCIPTOHOST.

Figure 51 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 a given trunk group. IP trunks use the IT (intertoll) trunk group type. Table TRKOPTS, where trunk groups are defined as IP, enforces this restriction.

The direction of the trunk group is important for voice communication between OC switches. Outgoing (OG) trunk groups are used exclusively to communicate with offices that are defined as OC hosts, whereas two-way (2W) trunk groups are used to communicate with OC remotes. Table OCGRP, where voice trunks are associated with offices, enforces this restriction.

The selection sequence should specify MIDL (most idle). Translations and screening information in TRKGRP is not used for OC-IP voice trunks and should be datafilled with default values.

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

Figure 52 MAP display example for table TRKGRP

```
GRPKEY         GRPINFO
-----------------------------------------------------------------
OCIPTOREMOTE   IT 0 TLD NCTC 2W IA MIDL 000 NPRT NSCR 619 000 N N $
OCIPTOHOST     IT 0 TLD NCTC OG IA MIDL 000 NPRT NSCR 619 000 N N $
```

TRKSGRP

Table TRKSGRP defines additional trunk group information such as signaling. Because OC-IP voice trunks use dynamic trunking (ISUP trunks), the following datafill must be present:

- 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

Table TRKOPTS enforces these restrictions. Additional information in TRKSGRP is not used for OC-IP voice trunks and should be datafilled with default values.

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

Figure 53 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
```

TRKOPTS

Table TRKOPTS specifies additional trunk group options, including the dynamic option required by OC-IP voice trunks. Datafill in TRKOPTS is used to define entire trunk groups as IP trunks. For OC-IP voice trunks, 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 name set to OC

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

Figure 54 MAP display example for table TRKOPTS

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

SITE

Table SITE identifies a site name associated with the 7X07 Gateway cards datafilled at the switch. This name is referenced by table IPINV. Datafill also includes the number of Gateways in the switch.

Additional information in table SITE is not used and can be datafilled with default values. In the following example, the Home switch datafills the site name TGWY.

Note: After table IPINV is datafilled, the system automatically updates the MODCOUNT field to reflect the number of Gateway cards on the site.

Figure 55 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 and secondary IP addresses; the type of Gateway (such as TOPS); and Gateway-specific refinements, such as the associated trunk group and the starting trunk member number.

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

Figure 56 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
```

P-side port numbers

Each DTC P-side 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 the OC-IP application.

Note: P-side links must first be assigned in table LTCPSINV (page 97). For information on port mapping, see “LTCPSINV-to-IPINV port mapping” on page 186.

IP addresses

In the OC host, the primary IP address must be the same as the IP address assigned to the Gateway by the DHCP server in the network. Any mismatch between DHCP datafill and CM datafill for a Gateway will not allow the Gateway to come into service. The secondary IP address is unused and should be datafilled with 0 0 0 0. In the OC remote, datafill in the IPZONE subfields is for informational purposes only.

Datafilling trunk members

After a Gateway card is defined in table IPINV, this table *automatically* allocates 48 trunk members in table TRKMEM. So, the starting trunk member in IPINV must be 0 or a multiple of 48. The maximum number of trunk group members is limited to 2016 instead of 2048 for OC-IP trunk groups, since 2016 is the highest multiple of 48 that is less than 2048.

The example datafill shown Figure 56 causes the 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 1: Removing TOPS entries in table IPINV automatically removes the associated TRKMEM members. Table TRKMEM does not allow individual 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: Refer to table TOPSTOPT 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, no manual datafill in TRKMEM is allowed because tuples are automatically datafilled by table IPINV.

The following example shows partial Home switch datafill for the OCIPTOREMOTE and OCIPTOHOST trunk groups.

Figure 57 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 47       0    DTC 10 7 24
 . . . . . .
OCIPTOHOST 96         0    DTC 11 10 1
OCIPTOHOST 97         0    DTC 11 10 2
OCIPTOHOST 98         0    DTC 11 10 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. Additional information in TOPSTOPT is not used for dynamic voice trunks and should be datafilled with default values.

In the following example, the Home switch datafills the trunk groups with a MAXCONNS value of 60 trunks.

Figure 58 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. In the following example, the Home switch increases the existing value of NUMPERMEXT from 100 to 244 to account for the 144 members in the OCIPTOHOST trunk group (OG).

Note: The values for TOPS_NUM_OC_EXT and TOPS_OC_ENVIRONMENT are unchanged by TOPS-IP.

Figure 59 MAP display example for table OFCENG

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

PKTVPROF

Table PKTVPROF defines profiles used for packetized voice. The profile index specifies a voice codec and is referenced in table TQCQINFO by call queue. When the G.729 codec is datafilled, silence suppression may also be specified. Table PKTVPROF contains two default tuples, 0 and 1.

Note: Datafilling the G.729 codec is not recommended if carrier-grade voice is required.

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

Figure 60 MAP display example for table PKTVPROF

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

TQCQINFO

Table TQCQINFO defines TOPS call queues, including the packetized voice profile index that applies to the call queue. The following example shows datafill for three packetized voice profile indexes against call queues.

Figure 61 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         1
CQ133   TOPS_TA  500    1000   VACT    N         2
```

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 62 MAP display example for table OCGRP

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

OC-IP call processing

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

Successful OC-IP call flow

Figure 63 shows an example OC-IP call flow that illustrates the use of voice and data links. The arrows represent both data link messages and call control messages used for voice link setup. For more details on the steps in the call progression, see “Detailed call progression” on page 107.

Figure 63 Example OC-IP call flow

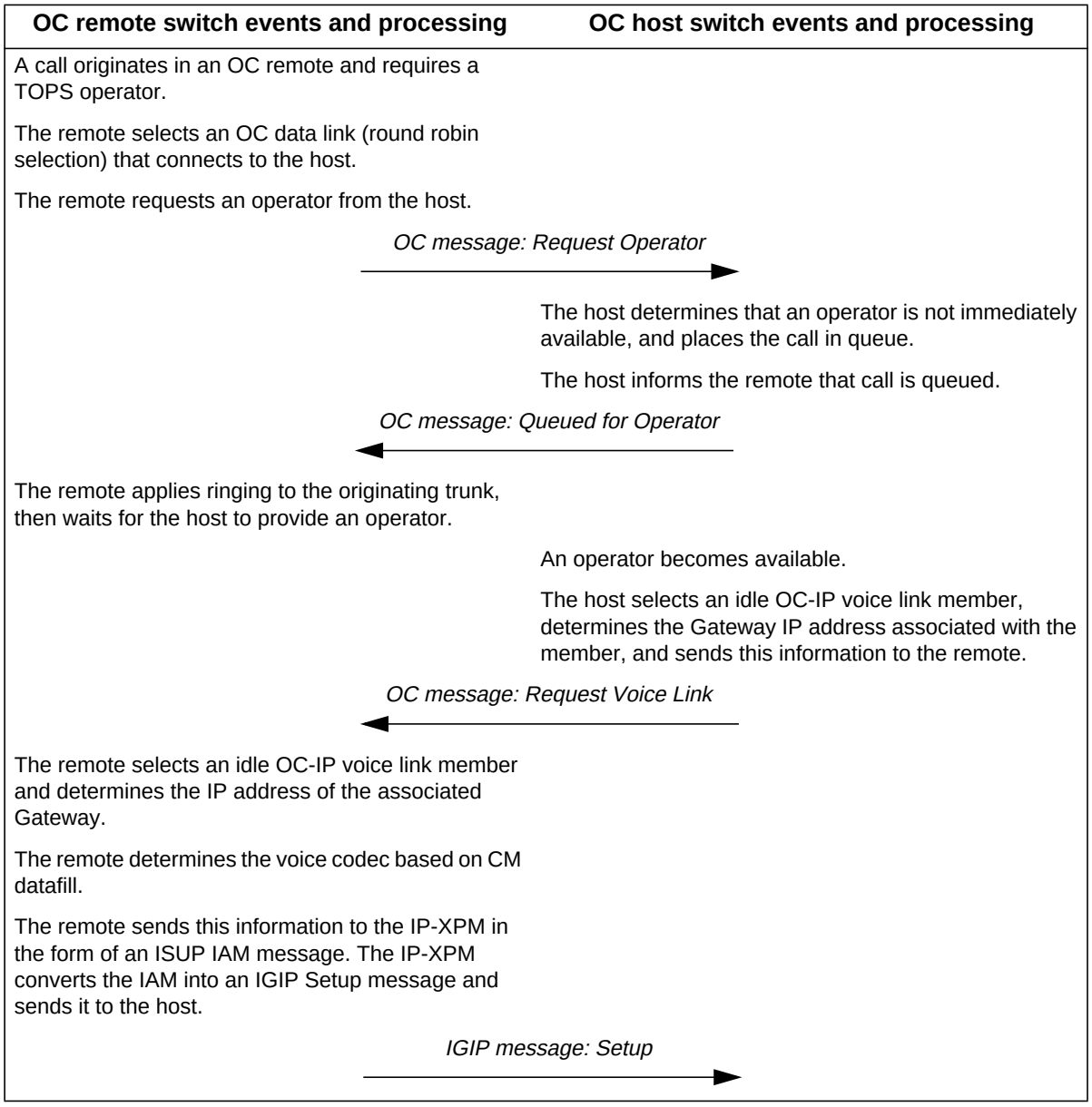
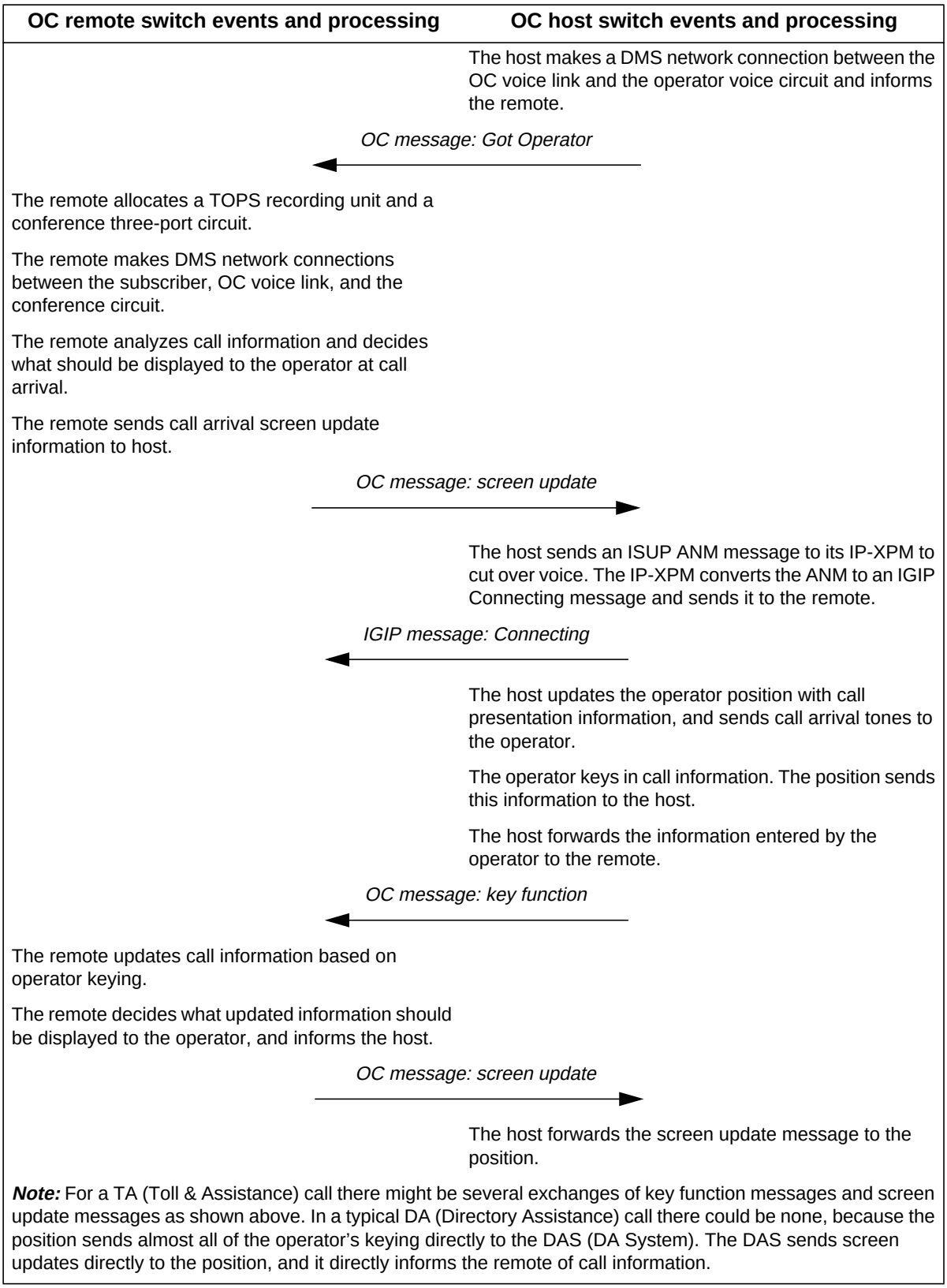
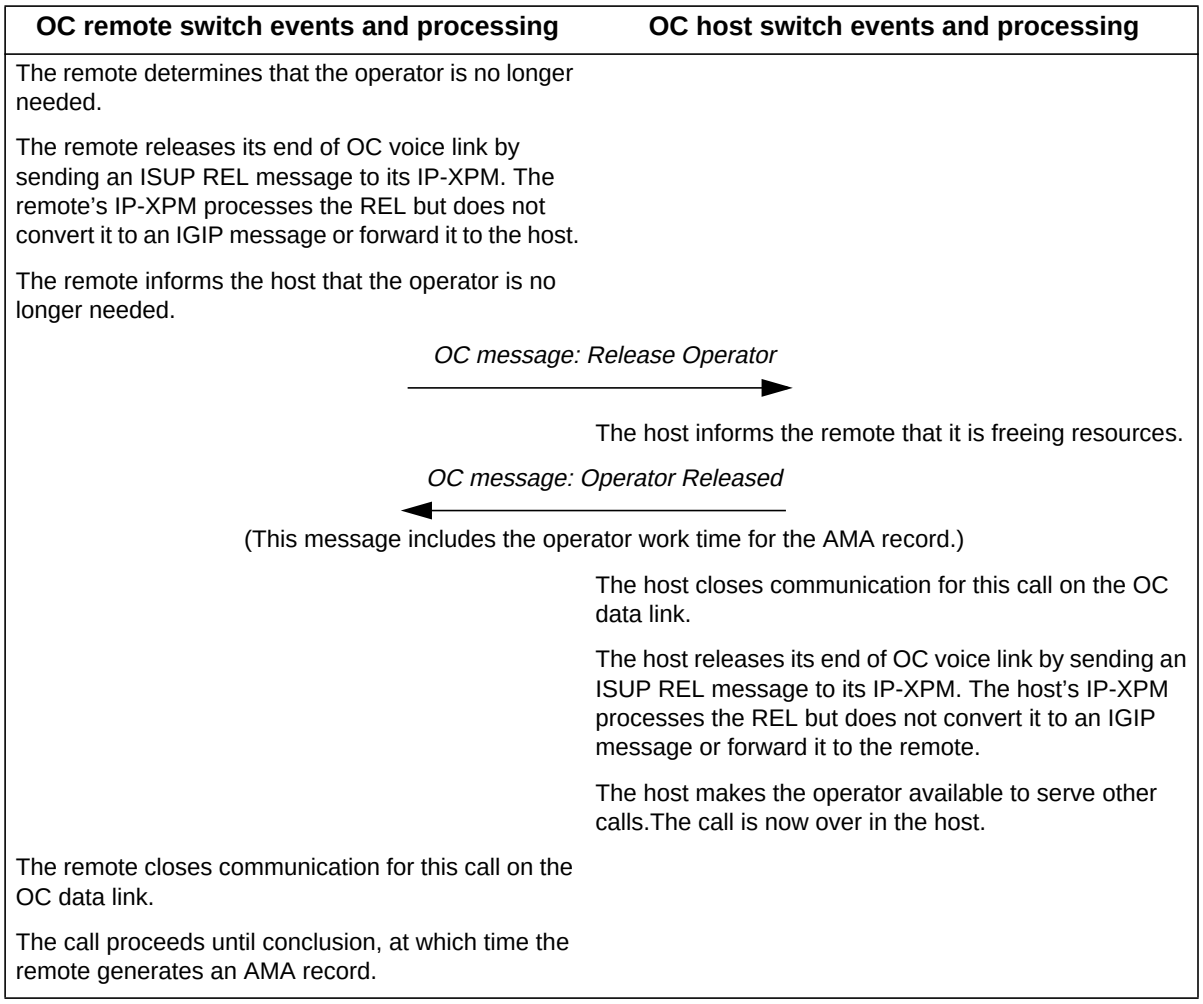


Figure 63 Example OC-IP call flow



Note: For a TA (Toll & Assistance) call there might be several exchanges of key function messages and screen update messages as shown above. In a typical DA (Directory Assistance) call there could be none, because the position sends almost all of the operator's keying directly to the DAS (DA System). The DAS sends screen updates directly to the position, and it directly informs the remote of call information.

Figure 63 Example OC-IP call flow



Detailed call progression

This section describes the steps in a successful OC-IP call progression.

1 *Call queue and OC host selection*. When a TOPS call in an OC remote switch requires an operator, QMS refinements determine a final call queue. If HRNQT is active, the final call queue is checked against table OCHOSTQ to determine whether the call is destined for an OC host. If HRNQT is not active, table OCPARMS and OCHOST determine the destination of the call.

2 *Data link selection*. Table OCGRP determines that the type of data link used to communicate with the host is IP. So, the remote needs a virtual circuit. Virtual circuits are a software resource, and 2048 are associated with each distant office. After a virtual circuit is obtained, table OCIPDL identifies the data links to the host office. Load sharing is done in a round robin fashion. Each call selects the next in-service data link and continues to use that data link as long as it remains in service. The remote selects the next in-service data link.

3 *Request operator.* The remote requests an operator from the host. The host receives the request and QMS processing determines whether the call gets an operator immediately or is queued (or even deflected).

4 *Voice link negotiation in the host.* When an operator becomes available, the host initiates voice link negotiation. In the host, table OCGRP determines the voice trunk group CLLI associated with the call. The host selects an idle member from this group and marks it call processing busy (CPB). Next, table IPINV in the host determines the Gateway card associated with the selected member, and the IP address of the Gateway. The host signals this IP address along with the specific trunk member to the remote using an OC Request Voice Link message on the data link.

5 *Voice link selection in the remote*. The remote initiates voice link selection using the same process as in the host. In the remote, table OCGRP determines the trunk group associated with the call. The remote selects an idle member from the group and marks it CPB. Table IPINV determines the Gateway card associated with the selected member, and its IP address. At this point in the call, the remote knows the IP address and member of *both* ends of the voice link.

6 *Voice link setup*. The remote establishes the voice link by sending an ISUP IAM message to its IP-XPM and Gateway. The Gateway converts the ISUP message into an IGIP Setup message and sends it to the host Gateway. The host makes DMS switch network connections between the OC voice link and the operator voice circuit. The host notifies the remote using an OC Got Operator message on the data link. The Gateways select the appropriate voice codec based on proprietary information in the ISUP IAM.

7 *Recording unit and conference circuit allocation*. The remote allocates a TOPS recording unit and a conference circuit. Next, the remote makes DMS switch network connections among the subscriber, the conference circuit, and the OC voice link.

8 *Initial screen update message*. The remote determines the appropriate screen update information and sends it to the host using an OC message on the data link.

Note: If the host selects an OPP-compatible position for the call, the remote bundles all of the initial screen update information into a single OC message rather than sending it in several messages, as is done with DCM OC, ETMS OC, and OC-IP for non-OPP positions.

9 *Voice link cut over.* In response to the screen update message, the host sends an ISUP ANM message to its IP-XPM and Gateway. The Gateway converts the ISUP message into an IGIP Connecting message and sends it to the remote Gateway.

10 *Call presentation to the operator.* The host updates the operator position with call presentation information and plays call arrival tones to the operator.

11 *Operator call processing.* At this point in the call, the operator has complete call presentation information, and both operator and subscriber are able to communicate. A series of key functions and screen updates typically occurs.

12 *Operator release in the remote*. When the operator is no longer needed on the call, the remote requests the host to release the operator using an OC Release Operator message on the data link. The remote also sends an ISUP REL message to its IP-XPM and Gateway to idle the remote end of the voice link.

13 *Call conclusion in the host.* The host sends the remote an OC Operator Released message that includes the operator work time for the AMA record, and it closes communication on the OC data link. The host also makes the operator available to serve other calls, and it sends an ISUP REL message to its IP-XPM and Gateway to idle the host end of the voice link.

14 *Call conclusion in the remote*. The remote closes communication for the call on its end of the OC data link. The call proceeds until conclusion, at which time the remote generates an AMA record.

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 11: “TOPS-IP logs.”

Requeuing or rerouting can be used in the following situations:

- Requeuing is used when there is a temporary lack of a resource within the OC remote or OC host switch. This places the call back into the same queue at the same host, with the expectation that the resource will be available the next time an operator is selected. When a call is requeued because of a resource shortage, the operator position that was originally selected for the call is placed in the make busy state, and the operator will need to re-enter the call processing screen by keying Start.
- Rerouting 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. Datafill in table OCHOSTQ determines whether the call is rerouted to an alternate host or to treatment. The alternate host for an OC-IP call can be another OC-IP host, a TDM OC 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.

  If an alternate host is not datafilled for the call’s reroute reason, the call is routed to treatment. The treatment datafilled in table TQCQINFO (TOPS QMS Call Queue Information) is used if deflection is permitted for the call; otherwise CQOV (CAMA queue overflow) treatment is used.

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 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.

Note: IGIP call control messages use TCP.

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 6: "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 104). 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 TOPS105 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.* As is done for TDM OC, unexpected messages will take a call down.

Chapter 4: 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

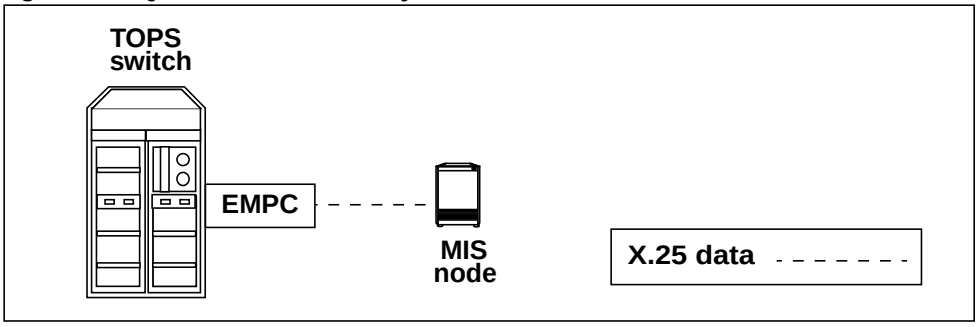
TOPS QMS MIS is a switch application that collects event-driven data about TOPS calls and sends this data to an external reporting facility, such as an MIS vendor server. With QMS MIS, the switch sends the data continuously and within a few seconds of the event. The MIS vendor can choose, depending on 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 64 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 64 QMS MIS connectivity without TOPS-IP



QMS MIS-IP introduction

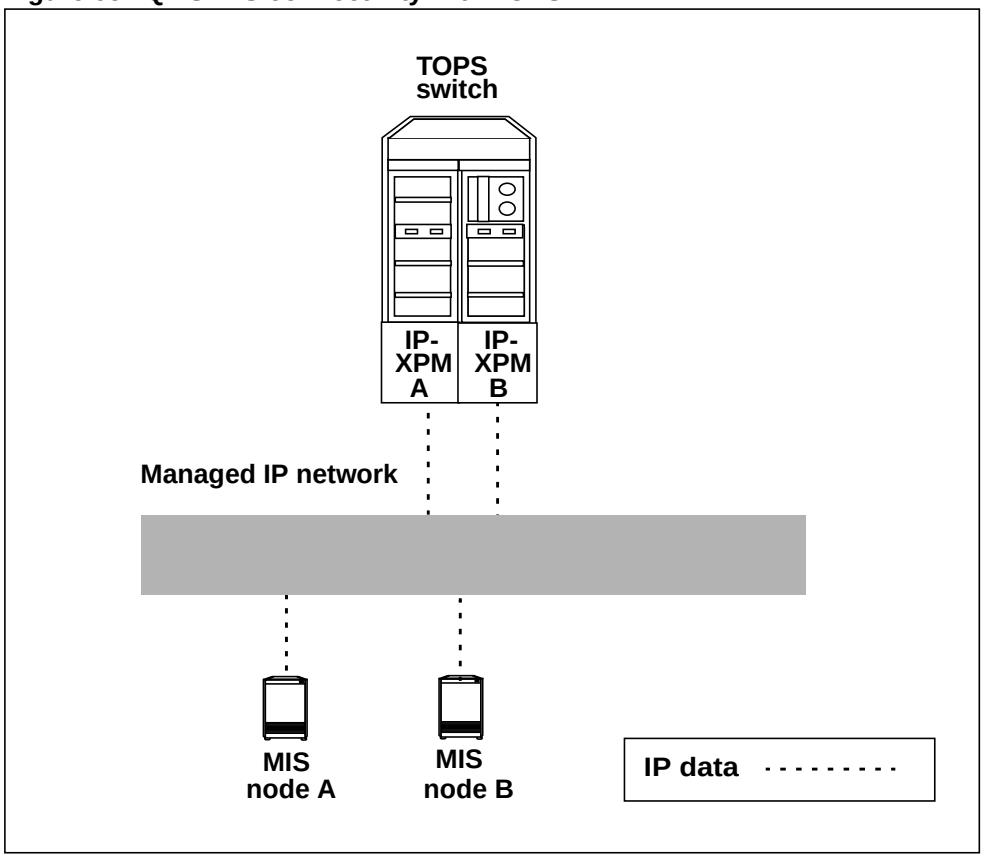
In a TOPS-IP network, a common IP infrastructure replaces the provisioning of X.25 data for the TOPS QMS MIS application. Using a DTC equipped with an SX05DA processor, the QMS MIS application sends data to an MIS node over the managed IP network.

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 6: "TOPS-IP engineering guidelines."

Figure 65 shows a TOPS switch having two QMS MIS-IP connections, one on each IP-XPM.

Figure 65 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 7: “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 9: "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 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 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 66 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 6: "TOPS-IP engineering guidelines."

2 Datafill the IP infrastructure in tables LTCINV, XPMIPGWY, and XPMIPMAP. Refer to Chapter 7: "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 67 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 68 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 69 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 70 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 5: TOPS-IP feature impact

This chapter lists the limitations and restrictions of TOPS-IP capabilities in the network, focusing on the following areas:

- IP data communication
- IP voice communication
- IP-XPM
- managed IP network
- TOPS-IP product
- OC-IP application
- QMS MIS-IP application
- Simple Network Management Protocol (SNMP)

Note: Chapter 6: “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 OC-IP or QMS MIS-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 latest firmware release is recommended.

- During an XPM SWACT (including a warm SWACT), both TCP and UDP applications 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 will transition to a SYSB state; however, after the cold SWACT completes, the Gateways will transition automatically back to an in-service state.
- 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.

  Note: When DHCP is selected as the configuration method, the IP-XPM receives configuration information from the DHCP server instead of from the CM.

IP port assignment datafill

The following limitations and restrictions apply to IP port assignment datafill:

- 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 to the application. More than one tuple may datafill a 0 in the PORT field. When an application uses a port of 0, the XPM randomly assigns a port in the range 32768 to 65535.

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 7: "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

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
- A single trunk group cannot be used for connections with both OC hosts 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 is crucial to OC-IP call processing in the OC host. It should 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 and OC-IP calls from distant switches cannot terminate on the Gateway.
- 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 TRKMEM members. Table TRKMEM does not allow members associated with a Gateway card to be manually added or removed.

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 OC-IP trunk groups. 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 greater than 2016 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 240.
- 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 will transition to a SYSB state; however, after the cold SWACT completes, the Gateways will transition automatically back to an in-service state.
- 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 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.

  DRAIN is available for the BSY option at the PM;IPGW MAP level used for CM maintenance of the Gateway card. For more information, refer to Chapter 9: “TOPS-IP maintenance activities.”
- 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.
- Although up to 10 7X07 Gateway cards can be installed in the IP-XPM frame, the IP-XPM’s C-side links cannot support the messaging that the OC-IP application would generate for 10 fully-occupied 7X07s unless average hold times at the operator position are a minute or longer. See Chapter 6: “TOPS-IP engineering guidelines,” for provisioning information on 7X07 Gateway cards.

Codecs

The following limitations and restrictions apply to voice codecs:

- Two voice codecs are available at call set up: G.711 (uncompressed) and G.729A (compressed).
- Voice quality is affected with the G.729A codec.
- DTMF tones are not supported on the G.729A codec.

  Note: Codec selection does not affect call arrival tones.

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.
- 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 same IP-XPM cannot be used for OC-IP.
- Each pair of C-side links added to an IP-XPM in table LTCINV 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.
- 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 6: "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:

- Applications that use the SX05DA card are not designed for use on the public Internet. Rather, they are intended for use on a private IP intranet that has been carefully engineered for reliability and adequate bandwidth.
- Routers and other nodes connected to the same local IP network as the IP-XPM must support the Gratuitous Address Resolution Protocol (GARP).
- Routers connected to the same local IP network as the IP-XPM must support the Virtual Router Redundancy Protocol (VRRP) or an equivalent protocol.
- Network routers must support BOOTP/DHCP relay capability if DHCP servers are not provided on each LAN segment.

Note: See Chapter 6: "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:

- The TOPS-IP product is not planned to be generally available; however, it may be ordered by special arrangement. TOPS-IP functionality is intended only for the North American market.
- TOPS-IP does not change the voice or data connectivity for any TOPS application or interface other than OC voice and data links, and TOPS QMS MIS-IP data links. It does not change the data connectivity between the DMS switch and D1 data bases, OPP-compatible operator positions, LIDB databases, or PARS nodes. It does not provide voice over IP between the switch and OSSAIN service nodes or the ISN-DA audio server.

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 LET0015 before OC-IP calls can take place. Other OC switches (TDM-based) must be upgraded to LET0012.
- The following existing limitations of ETMS OC also apply to OC-IP:
  - A maximum of 1023 operator positions can be datafilled in a switch.
  - A maximum of 30 tuples can be datafilled in table OCOFC when HRNQT is used, or 31 tuples when it is not used.
  - A maximum of 1364 conference three-port circuits (CF3P) can be provisioned on a switch. (A CF3P is required for each remote OC call with an operator.)
  - 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.
- The maximum distance between an OC host switch and an OC remote switch is constrained by latency and echo issues. There is no limit on the distance for OC-IP data transmission; this is configurable through standard IP practices. For a discussion of latency issues, refer to Chapter 6: “TOPS-IP engineering guidelines.”

- 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).
- TOPS OC-IP voice links do not use the SS7 network.
- The maximum number of OC-IP voice links depends on the call processing capacity of the IP-XPM. For details, refer to Chapter 6: "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

The following limitations and restrictions apply to mixing OC-IP functionality with traditional OC:

- OC-IP does not change any of the configuration limits associated with DCM OC or ETMS OC.
- For any OC office datafilled in table OCOFC, IP connectivity must be used for both OC voice and OC data, or for neither. A call cannot use traditional TDM-based OC voice links and OC-IP data, or traditional TDM-based data links and OC-IP voice.
- OC-IP voice links in one switch cannot communicate with TDM-based OC voice links in another switch. OC-IP voice links must be configured on both switches.
- OC-IP data links in one switch cannot communicate with TDM-based OC data links in another switch. OC-IP data links must be configured on both switches.
- OC voice link or data link failure during an established call does not cause the call to fall back to traditional OC voice or data facilities. However, alternate hosting to a TDM host is possible.

QMS MIS-IP application limitations and restrictions

The following limitations and restrictions apply to the QMS MIS-IP application:

- The peripheral that supports QMS MIS-IP must be a dedicated peripheral that does not contain 7X07 Gateway cards (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 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 7: "TOPS-IP data schema," for details on datafill.

SNMP limitations and restrictions

The following limitations and restrictions apply to the use of SNMP on the 7X07AA Gateway:

- "Public" is the only supported SNMP community name.
- 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 needs to 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.

Part 4: Planning and engineering

Part 4: Planning and engineering includes the following chapter:

Chapter 6: TOPS-IP engineering guidelines

This chapter discusses guidelines for engineering TOPS-IP, focusing on the following areas:

- TOPS-IP network overview
- Data and voice transport in the IP-XPM
- C-side links to the IP-XPM
- Provisioning the IP-XPM for TOPS-IP applications
- Capacity and performance requirements for the managed IP network
- Switch hardware resources
- IP network warranty service options

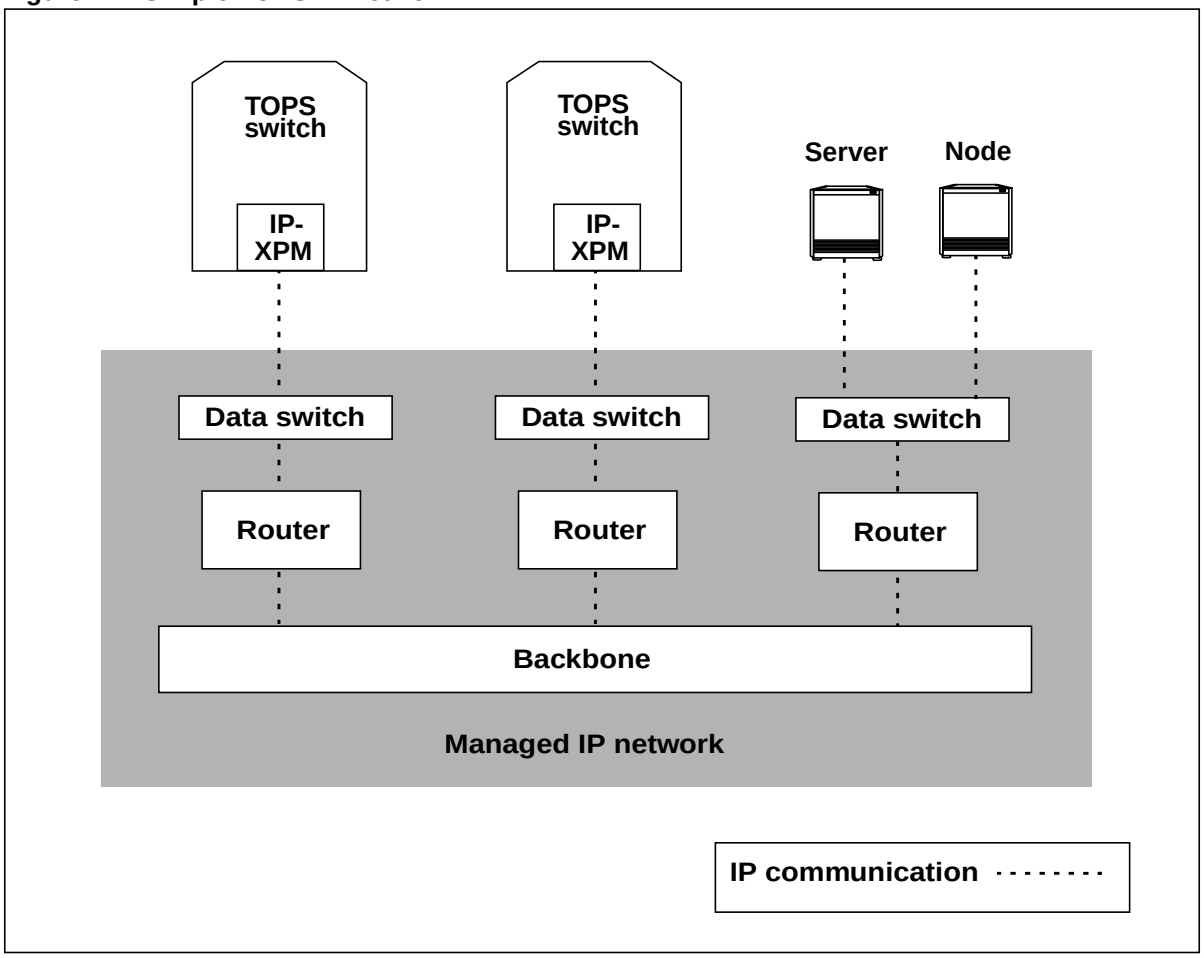
Network overview

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 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.

Figure 71 shows a simple, functional TOPS-IP network configuration.

Figure 71 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 DTC configured with an SX05DA processor, 7X07AA Gateway cards, and an MX76DA messaging card to provide the following IP infrastructure:

- voice gateways between the DMS circuit-switched network and the IP network
- call control, QMS MIS, and other data messages between the DMS CM and nodes on the IP network

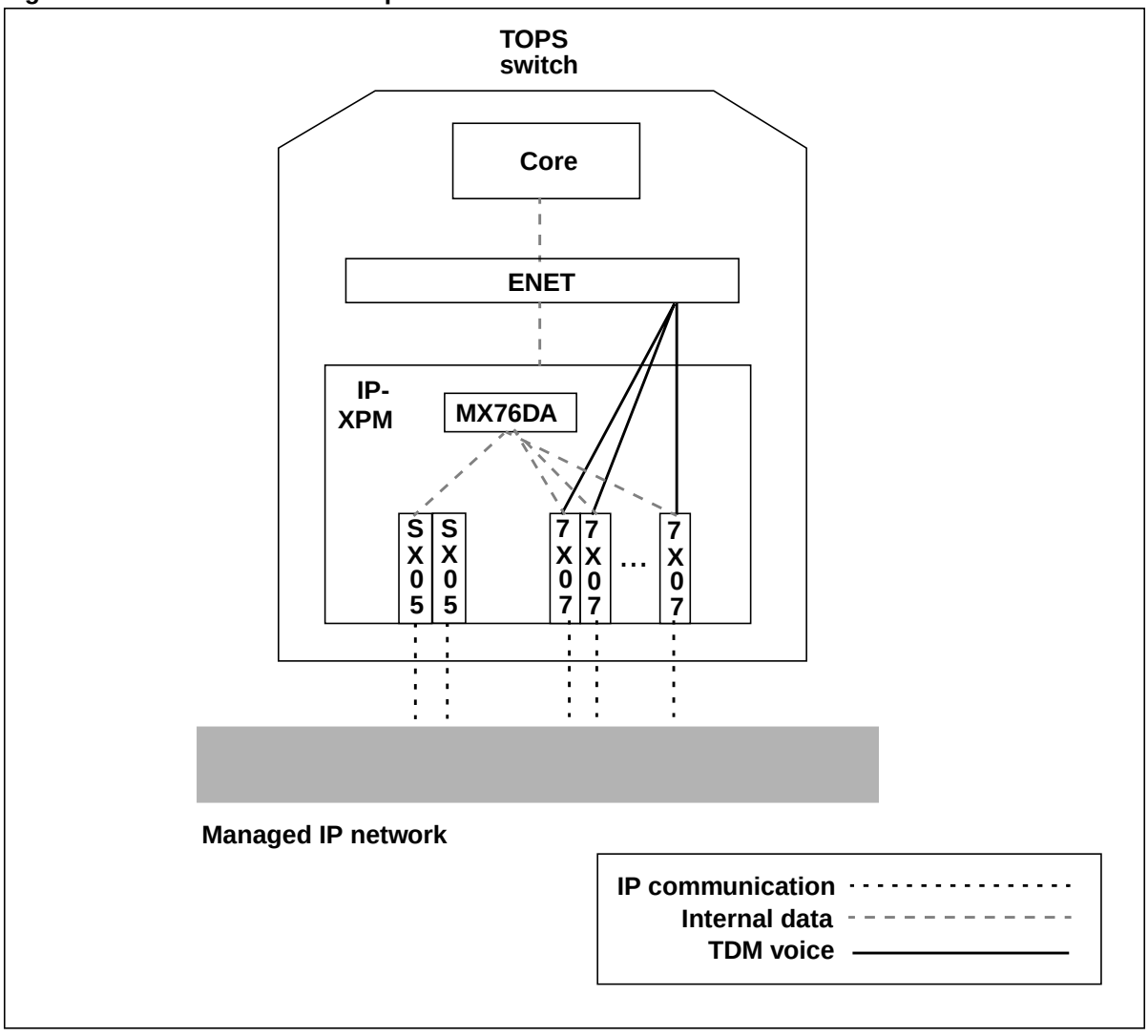
The 7X07 Gateway card is considered to be the first element at the edge of the managed IP network even though it is physically located in the IP-XPM. The 7X07 receives software and IP network datafill from a DHCP network server on the IP network.

Note: The SX05DA and 7X07AA cards require a new backplane, so most existing ETMS peripherals cannot be upgraded in the field. For details refer to “Switch hardware resources” on page 151.

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 for that service can be added.

Figure 72 provides an overview of the way the SX05DA, MX76DA, and 7X07AA are used to route data and voice through the IP-XPM.

Figure 72 Data and voice transport in the IP-XPM



Note: Although an IP-XPM has two SX05DA cards as shown in Figure 72, 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 the proprietary IGIP protocol 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 TOPS-IP product can be implemented only on switches that are provisioned with ENET (enhanced network). TOPS-IP is not supported on switches provisioned with JNET (junctored network). The network connects to an IP-XPM using C-side links, which transfer data between the DMS core and the IP-XPM. Enhanced C-side 14 messaging is required to make available 14 links to each IP-XPM, which significantly increases the data messaging capacity.

The following provisioning rules apply to the IP-XPM:

- The TOPS-IP switch must be provisioned with enhanced C-side messaging capabilities and with fiber peripheral links (SOC code TEL00011).
- For IP-XPMs handling the OC-IP application, 14 C-side links must be provisioned to each IP-XPM.
- For IP-XPMs handling the MIS-IP application, 14 C-side links must be provisioned to each IP-XPM.
- The ENET 9X17 chain cards must have a sufficient number of peripheral links available to provision the necessary number of C-side peripheral links to each IP-XPM. Links are provisioned in the EXTLINKS field in table LTCINV. 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.

Note 1: The EXTLINKS value is datafilled automatically by the CONVERTCSLINKS utility. For more information, refer to Chapter 10: “TOPS-IP CI tools.” For more information on table LTCINV, refer to Chapter 7: “TOPS-IP data schema.”

Note 2: Each pair of C-side links 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.

For details on IP-XPM hardware, refer to “Switch hardware resources” on page 151.

Provisioning the IP-XPM for TOPS-IP applications

In the TOPS15 release, two TOPS-IP applications use the IP infrastructure provided by the IP-XPM: Operator Centralization (OC-IP) and Queue Management System Management Information System (QMS MIS-IP).

Note: OC-IP functionality is discussed in Chapter 3: "TOPS OC-IP application," and QMS MIS-IP functionality is discussed in Chapter 4: "TOPS QMS MIS-IP application."

Engineering the managed IP network for TOPS-IP applications 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 (UDP is used for both of these)

The TOPS-IP switch must be provisioned with one or more IP-XPM peripherals to handle TOPS-IP data and voice. This section describes the five-step process for engineering and provisioning the IP-XPM:

1 Determine the number of OC-IP trunks (voice ports) required for each OC remote and OC host switch.

2 Determine the number of 7X07 Gateway cards to provision in the IP-XPM to handle this OC-IP capacity and to provide redundancy.

3 Determine whether QMS MIS-IP will be used, and if so, how many MIS-IP data links to provision to connect with the MIS vendor server (or servers).

4 Determine the number of IP-XPMs required.

5 Determine how the IP-XPMs should be configured for load balancing if more than one IP-XPM is provisioned for OC-IP.

Note: This section contains *estimated* values for the maximum number of 7X07 Gateway cards.

Step 1: OC-IP capacity requirements

The first step in the engineering and provisioning process is to determine the required OC-IP capacity, as follows:

- *OC-IP remotes*. For each TOPS OC remote, determine the maximum number of simultaneous voice connections required to the OC host or hosts. This number will be used to determine the number of 7X07 Gateway cards required in the remote.
- *OC-IP hosts*. For each TOPS OC host, determine the maximum number of simultaneous OC voice connections required to all remotes. This number will be used to determine the number of 7X07 Gateway cards required in the host.

Step 2: 7X07 Gateway card requirements for OC-IP

The number of 7X07 Gateway cards includes those needed to provide the necessary OC-IP voice port capacity plus additional capacity for Gateway card N+1 redundancy per trunk group.

7X07 requirements for OC-IP

A single 7X07 Gateway card can support 48 OC-IP voice ports. To determine the number of 7X07 Gateway cards to provision for OC-IP on each switch (excluding redundancy), divide the number of OC-IP voice ports required on the switch by 48 and round up. Refer to the following examples:

- *Example 1*— If 120 OC-IP trunks are required on an OC remote, then three 7X07 cards are required to support OC-IP (120/48 = 2.5, which is then rounded up to 3).
- *Example 2*—If an OC host is to support 50 OC trunks to Remote A, 120 OC trunks to Remote B, and 80 OC trunks to Remote C, then six 7X07 cards are required to support OC-IP (a total of 50+120+80 = 250 trunks are needed, and 250/48 = 5.2, rounded up to 6 cards).

The following considerations apply to the 7X07 Gateway cards:

- Voice links are added in multiples of 48.
- All 48 trunks associated with a Gateway card are added to the same trunk group.
- Different Gateway cards on the same IP-XPM can be assigned to different trunk groups.
- A single trunk group can use Gateway cards on different IP-XPMs.
- A single trunk group can use more than one Gateway card on the same IP-XPM.
- It is recommended that all OC-IP voice links be assigned to a single trunk group, or to two trunk groups in a hybrid host/remote.
- The IP-XPM does not support TDM speech cards, such as the 6X50.

7X07 requirements for redundancy

The 7X07 operates in simplex mode, so a single failure affects 48 trunks. Each 7X07 has two Ethernet ports. The managed IP network can be engineered so that no single failure in the IP network will prevent a 7X07 from connecting to the network, although there will be brief interruptions of service in the following cases:

- while the 7X07 switches to its alternate Ethernet interface
- during an IP-XPM swact (including warm swact)
- while routers in the IP network discover new routes
- while a VRRP (virtual router redundancy protocol) router takes on the traffic intended for its associated master router or when control is returned to the original router
- while traffic at the alternate router is returned to the original master router after recovery of a fault protected by VRRP

  Note: For more information on the operation of VRRP routers, refer to "Redundancy in the managed IP network" on page 144.

OC-IP trunks are defined in one or more OC-IP trunk groups. Redundant port capacity is configured on a per-trunk group basis. It is recommended that an additional 7X07 (48 voice ports) be provisioned for each OC-IP trunk group to ensure N+1 redundancy. To minimize the sparing requirements, it is therefore recommended that only one trunk group be defined for OC-IP (or two in a hybrid host/remote). When all OC-IP ports are assigned in a single trunk group, only one additional 7X07 is needed for redundancy. Two additional 7X07s are needed in a hybrid host/remote.

Total 7X07 requirements

The total number of 7X07 Gateway cards required on a TOPS-IP switch is equal to the number of cards required to support OC-IP voice trunks plus the number required to provide redundancy. Using the same examples as on page 140, provision for redundancy to determine the total requirements as follows:

- *Example 1*—Three 7X07 cards are required to support the 120 OC-IP trunks on the OC remote. If all 120 trunks are provisioned in a single trunk group, one additional 7X07 will be required for N+1 redundancy. So a total of four 7X07 Gateway cards should be provisioned.
- *Example 2*—Six 7X07 cards are required in the OC host to support the trunks from the three OC remotes. If all 250 trunks are provisioned in a single trunk group, a total of seven 7X07 cards will support OC-IP with N+1 redundancy.

Step 3: MIS-IP requirements

QMS MIS-IP is an optional TOPS-IP application that can only be implemented on TOPS OC hosts or TOPS standalone switches. MIS-IP is not available on TOPS remotes.

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). No 7X07 Gateway cards are provisioned in the MIS-IP 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.

Step 4: Number of IP-XPMs required

Although up to 10 7X07 cards can be installed in the IP-XPM frame, the IP-XPM's C-side links cannot support the messaging that the OC-IP application would generate for 10 fully-occupied 7X07s unless average hold times at the operator position are a minute or longer. Because traffic patterns and operator practices can differ greatly among OSCs, the actual capacity of an IP-XPM must consider the average time each call is handled at a position and the typical amount of operator keying per call. Table 1 lists *estimated* 7X07 capacities with various average call hold times for DA calls with VROPT parameter DA_AUTO_POS_RLS set to Y.

Table 1 7X07 requirements for IP-XPMs used for OC-IP

Average hold times at operator position	Maximum 7X07 capacity (excluding redundancy)
15 seconds	4
20 seconds	6
30 seconds	7
45 seconds	9
60 seconds	10

More than one IP-XPM is required under the following conditions:

- If more than the maximum supported number of 7X07s are needed (see Table 1) to handle OC-IP traffic.
- If optional provisioning of an additional IP-XPM is desired for additional redundancy.
- If MIS-IP data link(s) are provisioned. As discussed in Step 3, to support the heavy MIS messaging load, an MIS-IP data link requires a dedicated IP-XPM.

Step 5: Load balancing for OC-IP

When multiple IP-XPMs are required or desired for OC-IP, it is important to ensure that the traffic is evenly shared. TOPS-IP is designed to spread traffic evenly over the available trunks and data links. TOPS-IP offices should be provisioned to distribute the 7X07 cards, OC-IP trunks, and OC-IP data links evenly among the IP-XPMs.

Limiting the use of dynamic voice links

When provisioning additional 7X07 cards for use as spares, it may be important to ensure that this extra capacity is reserved so that it is available if a 7X07 card fails. It may also be desirable to limit the number of 7X07 voice trunks in use to restrict the bandwidth demands on the IP/ATM network transporting the OC-IP packets.

The MAXCONNS field in table TOPSTOPT provides a mechanism for "reserving" this spare capacity. By using MAXCONNS to reserve trunks in blocks of 48, it can be assured that one or more card's worth of trunks can be reserved. This applies only to dynamic trunk groups.

Each Gateway card supports 48 trunk members. When a maximum is datafilled in MAXCONNS, the switch loops over all in-service Gateway cards for the affected trunk group and calculates a member limit for each card. This allows the maximum specified to be distributed across all in-service Gateway cards. So, for example, if MAXCONNS is set to 100, and three Gateway cards are associated with the trunk group, the first card is limited to 34 members and the second and third cards are limited to 33 each.

During call processing, the switch checks Gateway trunk members as they are selected. If a trunk member is not usable due to the MAXCONNS limit, the switch places the trunk member in a holding queue and selects another member. Unusable trunks appear as restricted idle (RES) when viewed at the TTP level of the MAP. The call processing deload (CPD) function is not used when a MAXCONNS limit is datafilled.

If a user changes the MAXCONNS value, the limit on each in-service Gateway card is updated with the new limit. This allows the new set of usable trunks to be evenly distributed across the in-service cards. Trunk members are moved into or out of the holding queue as necessary. No calls end as a result of changing the MAXCONNS value.

As Gateway cards are added and brought into service, the limit per card is reduced so that each card supports the same number of available members. Likewise, as Gateway cards are removed from service, the available members are redistributed among the remaining cards.

TOPS-IP dynamic trunks are moved to the holding queue (and to the RES state) during trunk selection. To reduce per-call CPU use, TOPS-IP trunk selection moves only a handful of trunk members to the holding queue during a single call. During subsequent calls, additional members move to the holding queue. As a result, there may be a short time when the number of usable members in a trunk group is more than the datafilled limit. As new calls arrive and further trunk selection occurs, more members are moved to the holding queue until the number of unusable trunks is equal to the limit.

Note 1: For information on the maintenance of dynamic trunks, refer to Chapter 9: "TOPS-IP maintenance activities."

Note 2: For details on datafilling MAXCONNS in table TOPSTOPT, refer to Chapter 7: "TOPS-IP data schema."

Monitoring IP-XPM resource use

For OC-IP, OM groups such as XPMMSGOC (XPM Messaging Occupancy), provide data that may be used to monitor XPM resource usage in order to avoid overload conditions. For details on how to use this OM group to monitor the IP-XPM, refer to Chapter 12: "TOPS-IP OMs."

Capacity and performance requirements for the managed IP network

The capacity and performance requirements for the managed IP network are derived from the traffic offered by all the TOPS-IP applications in use in the network. Capacity requirements are based on the volume of messages created by the applications. Performance requirements such as delay and jitter depend on the types of traffic. For example, voice requires low delay and jitter but can tolerate up to 0.1% packet loss.

For OC-IP call control messages, the maximum tolerable message loss is 0.0001%. However, OC call control messages can tolerate more delay than voice traffic can.

QMS MIS-IP uses TCP/IP and is relatively insensitive to both message loss and delay.

Redundancy in the managed IP network

The managed IP network must be designed to detect faults and quickly change from one route to another to minimize disruption of IP voice and data streams. The network should be engineered with redundant pairs of routers to act as gateways to the network. Likewise, these routers should have redundant alternate paths through the backbone network so that no single point of failure can isolate an OC host from an OC remote.

The managed IP network should have enough bandwidth such that when one component or path fails, the remaining components or paths can handle the full traffic load. Provisioning for reduced capacity under network failure conditions is not recommended. This is because there is no mechanism to preferentially throttle new originations when the load on the network is too high; calls already in progress will be adversely affected if the bandwidth is insufficient for the total offered traffic.

Virtual Router Redundancy Protocol (VRRP)

The redundant pair of routers will have Virtual Router Redundancy Protocol (VRRP) configured on their LAN interfaces. VRRP is a standard router redundancy protocol based on RFC 2338 and provides redundancy that eliminates the single point of failure common in a single default router environment.

With VRRP, the default router is backed up by several physical routers. The responsibility for the virtual router is assigned to a physical router by a priority system. The highest priority operating physical router forwards packets for the virtual router. This is referred to as the *master router.* If the master router becomes unavailable, the next highest priority router becomes the new master and forwards packets for the virtual router.

VRRP also has the advantage that it does not require dynamic routing or router discovery protocols. VRRP typically provides faster fail-over than a dead neighbor detection scheme.

The network administrators can configure the Gateway cards to balance the load between the two routers. Two virtual routers need to be configured with the physical router priority set so each router is master for one of the addresses. Each physical router is then configured as the backup for the mate address. By selecting alternate use of the two virtual routers by the Gateway cards, the load is shared by the two physical routers. Upon failure of one physical router the remaining physical router supports both addresses. When the failed physical router is restored, it again becomes master for its priority virtual address again.

A critical interface may be added to the VRRP function. The status of this other router interface is used in the determination of *master* state for the virtual interface, which can be used to enhance network fail-over response. For more details, refer to RFC2338 *Virtual Router Redundancy Protocol*.

Local failure detection in the 7X07AA

The 7X07 Gateway monitors the Ethernet link on both of its ports. If both ports are available, one is randomly chosen at startup. Upon a failure of the Ethernet port, the 7X07 will switch traffic to the other port. This port redundancy allows recovery from cabling and hub/switch faults in the local network. The use of VRRP on the gateway routers completes the redundancy in the local area network.

Note: For details on the datafill for routers required in the DHCP server, refer to Appendix A: "DHCP server guidelines."

Dead neighbor detection scheme

A dead neighbor detection scheme uses a polling method to periodically verify conductivity to (and sanity of) a necessary host. Polling may range from a simple ping (ICMP echo) to a separate handshake protocol of hello and response messages. The results of the polls are used to determine a host's capability to communicate and perform required tasks.

Local failure detection in the SX05DA

The SX05DA in the IP-XPM does not incorporate Ethernet link monitoring. Rather, it uses a ping message as its only failure detection method. The IP-XPM periodically pings its default gateway router. If it does not receive a reply to several pings, it attempts to ping a second default gateway router (if datafilled).

If the ping to the second gateway router is successful, the IP-XPM will start using this router as its default gateway router. Even when the original gateway router recovers, the IP-XPM will not use it unless the current router fails.

If the ping to the second gateway router is unsuccessful, the active unit of the IP-XPM queries the inactive unit concerning its ping reply status. If the inactive unit is able to ping any of its datafilled gateway routers, the IP-XPM will perform a switch of activity (SWACT). The same detection method is used to discover cabling or hub/switch faults.

Note 1: VRRP virtual IP addresses do not respond to ping messages as defined in RFC2338. These virtual addresses must *not* be datafilled as the default gateway router for the SX05DA card. Instead, physical gateway router interface IP addresses must be used. This datafill is present in either table XPMIPGWY (at the switch) or in the DHCP server.

Note 2: For details on the datafill for routers required in the DHCP server, refer to Appendix A: "DHCP server guidelines."

IP network message volume for voice links

Table 2 shows the message rate and data bandwidth used by a single voice link from the 7X07. The packet size and data rate columns include the protocol headers for RTP, UDP, and IP. They do not include lower layer headers such as Ethernet, Frame Relay, or ATM, since these depend on the transport chosen for a particular network.

TOPS-IP currently supports only G.711 at a packet length of 20 ms or G.729A at a packet length of 20 ms. Optional silence suppression is available but is not recommended for carrier-grade quality voice. The codec is selected by datafill in tables PKTVPROF and TQCQINFO. The codec is assigned based on call queue, which allows considerable flexibility.

Note: Datafilling the G.729 codec is not recommended if carrier-grade voice is required.

The routers in the IP network must be able to handle 50 packets per second in each direction for every voice link passing through the router, and network transport must have sufficient bandwidth to support 80K bits per second for each voice link if G.711 is used, or 24K bits per second if G.729A is used.

Table 2 Voice over IP packet rates and sizes

Codec	Packet length	Packet size	Packet rate	Data rate	Bandwidth per 1K calls
G.711	20 ms	200 bytes/packet	50 packets/sec	80.0K bits/sec	80M bits/sec
G.729A	20 ms	60 bytes/packet	50 packets/sec	24.0K bits/sec	24M bits/sec

IP network message volume for data links

The approximate message volume for data links is shown in Table 3 for 20-second DA calls. These figures will vary for different call hold times and call types. The size is inclusive of IP and UDP or TCP headers. These messages are sent through the SX05DA. Some additional call control messages are handled by the 7X07s along with the voice packets.

Table 3 Summary of IP network data message rates for sample DA call type

Application	IP messages/sec generated by host at 1000 calls/hour	Average IP message size from host	IP messages/sec generated by remote at 1000 calls/hour	Average IP message size from remote
OC DA calls	1.6	120 bytes	2.2	140 bytes
OC TA calls	2.1	120 bytes	2.6	140 bytes
QMS MIS data links	0.04	1500 bytes	n/a (QMS links only exist in host)	n/a (QMS links only exist in host)

Since the volume of control messages generated is less than 1% of the voice bandwidth, the control messages have a minor impact on total bandwidth requirements. Successful delivery of control messages is, however, critical. The small volume of control (data) messages must be given highest priority.

IP network performance requirements for voice over IP

The main factors that affect quality of speech that are introduced by using packet transport are the latency or delay introduced by collecting and processing packets, the loss of fidelity introduced by compressing codecs, and the impairment caused by loss of packets. Another factor called jitter is really a property of packet networks which forces network designers to make a trade-off between the amount of delay and the amount of packet loss that users encounter. The impact of the various impairment factors can be assessed separately, but the overall effect on voice quality is cumulative.

To the extent that the network can differentiate quality of service (QoS) for different types of traffic, the requirements for latency, packet loss, and jitter are described here. If QoS cannot be differentiated, the network must meet the most stringent requirements in each area (latency, packet loss, jitter).

Impact of network latency

In the absence of other impairments, latency does not cause problems for most users until it reaches about 200 ms. It then causes people to have trouble knowing when to start and stop speaking. For carrier-grade voice, maximum end-to-end latency of 150 ms or less is required. To achieve this, the IP/ATM network used to transport OC-IP voice must have latency of 40 ms or less for RTP/RTCP voice packets.

Latency accumulates at many points in the speech path:

- The collection of speech samples into packets. TOPS-IP currently uses packets of 20 ms duration as a trade-off between network processing overhead and latency.
- The processing time in the originating Gateway for codecs and message processing to convert the TDM stream to IP packets.
- The processing of packets in the IP transport network. The performance of cost-effective IP routers is improving from a few tens of milliseconds delay per router to a few microseconds delay per router.
- The transmission delay depending on the distance between the source and destination.
- The use of jitter buffers in the receiving Gateway to ensure that there are no gaps in received speech.
- The processing time in the terminating Gateway for codecs to convert the received packets to a TDM stream.

For OC-IP, the sending and receiving IP-XPM and 7X07 Gateway contribute approximately 70ms to 75ms latency. This includes accumulating the 20ms TDM voice sample, codec processing and packetizing the sample, queuing and transmitting the voice (RTP/RTCP) packet, receiving and processing the incoming voice packet, jitter buffer delay, and codec processing the sample to convert back to TDM.

Impact of codec selection and packet loss

TOPS-IP supports two codecs. G.711 does no compression and requires higher bandwidth. G.729A compresses the 64K bit per second TDM stream to an 8K bit per second rate. Each speech packet also requires a 40-byte header, so the total bit rate through the IP network for a single voice link can be higher than the bit rate for a corresponding TDM trunk when no compression is used (see Table 2, page 147). However, the IP voice link uses no bandwidth at all unless a connection is in use, whereas the TDM trunk's capacity is permanently reserved in the network. As compared to the speech quality of G.711, the impact of G.729A compression is similar to the effect of about 50 ms extra latency and 1% extra packet loss.

If a call encounters more than one instance of compression (for example, a cellular call would be compressed on the radio link, restored to Mu law pulse code modulation, then compressed again on OC links if G.729A is used), the impairment caused by all the compression operations is cumulative. This is known as "transcoding." It is necessary to consider the nature of all traffic sources routed on OC-IP voice links. G.711 is recommended when other sources of compression may be used in the network.

In practice, it is advisable to keep overall latency of IP voice packets below 150 ms in each direction and packet loss below 0.1%. If the G.729A codec is to be used, it is especially important to hold other impairment factors to a minimum.

While it is supported, we do not recommend the use of silence suppression in carrier-grade voice applications such as operator services and directory assistance.

Impact of jitter

Jitter refers to variation in the transmission time from one packet to the next. It is necessary to accumulate incoming packets in buffers (called jitter buffers) to ensure that there will always be a new packet available when the old one has been processed. Any packet that is delayed long enough for the jitter buffers to empty will be lost. The purpose of jitter buffers is to trade off a small delay for a reduction in the rate of packet loss. The 7X07 adapts this delay to match the jitter that is actually encountered in the network. The IP network should be engineered to provide the lowest possible jitter for speech packets, in order to minimize the latency added by the jitter buffers.

Target specifications

The targets for the TOPS-IP network are:

- Voice packet latency less than 40 ms in each direction is required, and latency less than 35 ms is desired.
- Voice packet loss less than 0.1% within the network is required.
- Data packet loss less than 0.0001% for OC call control messages is required.
- Jitter less than 15 ms for speech packets in the IP network is required, and jitter less than 10 ms is desired.

Message priority

It is expected that the IP network will be designed using knowledge of UDP port numbers to give different priorities for TOPS-IP voice and data traffic. As previously noted, the maximum tolerable message loss for call control messages is 0.0001%, while voice can tolerate up to 0.1% packet loss. Also, while voice requires low delay and jitter, call control messages can tolerate more delay.

The RTP and RTCP protocol for the voice traffic between 7X07s is carried on UDP ports in the range 2326 to 2444.

The UDP ports for data links on the SX05s are assigned in table IPSVCS (see Chapter 7: “TOPS-IP data schema”). It is recommended that OC-IP data links use port numbers in the range 8600 to 8899.

Other sources of IP traffic

The other identified sources of traffic in the managed IP network are:

- DHCP and 7X07 Gateway loadfiles
- Simple Network Management Protocol (SNMP)

IP traffic for these functions should not affect the bandwidth provisioning of the managed IP network. However, it is necessary to ensure that the network gives priority to voice and call processing services, as described earlier in this section, so that this traffic does not interfere with call processing. If the network has been provisioned to handle the voice traffic for a 7X07 while it is in service, there will be capacity available when the 7X07 is out of service to load the card using FTP (file transfer protocol).

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.

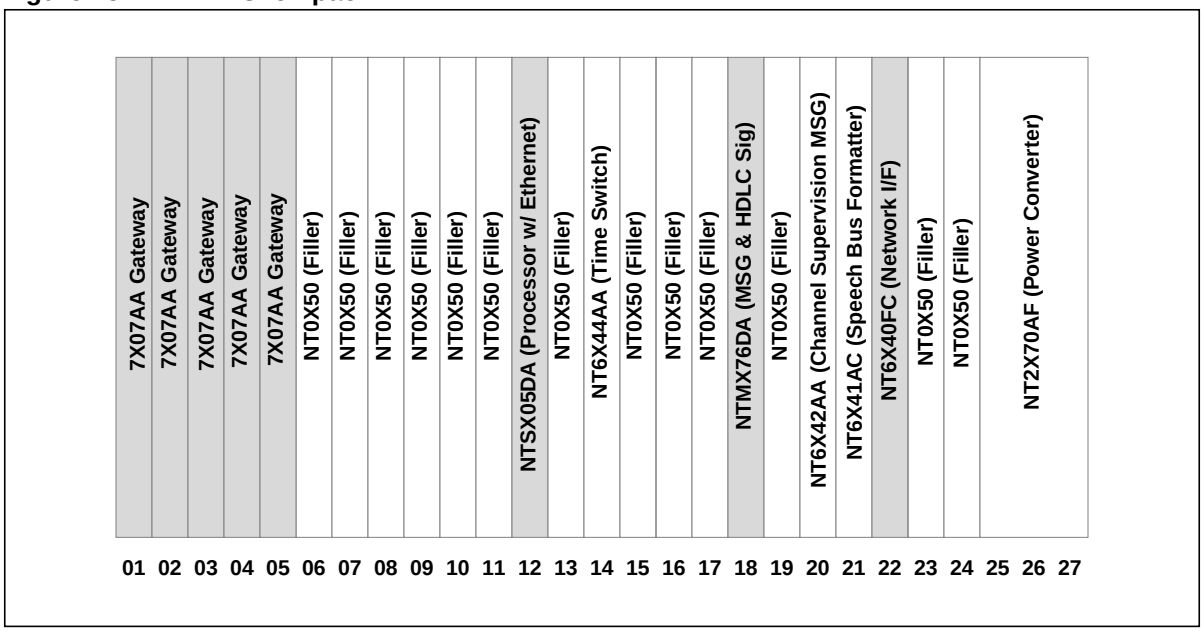
Core hardware requirements

TOPS-IP can generate a significant volume of data that must be exchanged between the TOPS CM and the IP-XPM. To support TOPS-IP applications, the TOPS switch must be equipped with either SuperNode 70 or XA-Core SuperNode processors.

IP-XPM shelf packfill requirements

Figure 73 lists the IP-XPM packfill (NT6X02MG).

Figure 73 IP-XPM shelf packfill



The following rules apply to the IP-XPM for TOPS-IP applications:

- 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.
- Provision up to five NT7X07AA Gateway cards in slots 01 to 05 of each shelf (10 cards per IP-XPM).

  Note: Refer to the section “Provisioning the IP-XPM for TOPS-IP applications” on page 139 for important capacity information on the maximum number of 7X07 cards to provision.
- Provision one SX05DA Unified Processor card in slot 12 of each shelf (two cards per IP-XPM).

- Provision one NTMX76DA messaging card in slot 18 of each shelf (two cards per IP-XPM).
- Provision one NT6X40FC interface card in slot 22 of each shelf (two cards per IP-XPM).

Frame and shelf requirements

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.

Ethernet patch panel requirements

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.

IP-XPM cable requirements

The IP-XPM requires two system cables (NT0X96NW or NT0X96NV). If an Ethernet patch panel is not used, the NT0X96NW cable interconnects the backplane directly to a compatible Ethernet switch on the LAN. If the Ethernet patch panel is used, the NT0X96NV cable interconnects the backplane to the patch panel.

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. The latest firmware release is recommended.

To verify that the IP-XPM has the correct version of firmware, users can follow this procedure at the MAP:

1 Enter the MAPCI NODISP;MTC;PM level at the MAP.

2 Post the IP-XPM (for example, DTC 10).

3 Issue the QUERYPM CNTRS command. The MAP displays the information similar to that shown in Figure 74.

Figure 74 MAP display of SX05DA firmware information

```
>MAPCI NODISP;MTC;PM;POST DTC 10;QUERYPM CNTRS
    Unsolicited MSG limit = 250, Unit 0 = 0, Unit 1 = 0
    Unit 0:
    Ram Load: QD715AY
    EPRom Version: AA01
    EEPRom Load: Executable: AG04, Loadable: AG04
    UP:SX05DA
    Unit 1:
    Ram Load: QD715AY
    EPRom Version: AA01
    EEPRom Load: Executable: AG04, Loadable: AG04
    UP:SX05DA
```

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.

IP network warranty service options

The TOPS-IP managed IP network consists of components from several Nortel Networks product groups. The network 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 5: Provisioning

Part 5: Provisioning includes the following chapters:

Chapter 7: 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 159)

  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 196)

  This datafill provisions the OC-IP application at the switch so that OC hosts and OC remotes can communicate with each other over the managed IP network.

- QMS MIS-IP datafill (page 205)

  This datafill provisions the QMS MIS-IP application at the switch so that MIS data can be sent to an MIS vendor node on the managed IP network.

- XIPVER datafill (page 209)

  This datafill provisions the XIPVER test tool at the switch so that users can test IP data communication through the IP-XPM.

Alphabetical reference for tables

The following table lists each table in alphabetical order and the page where its description begins.

Table 4 Alphabetical reference for TOPS-IP table descriptions

Table name	Page number
CLLI	page 176
CARRMTC	page 164
IPCOMID	page 174
IPINV	page 184
IPSVCS	page 172
LTCINV	page 162
LTCPSINV	page 165
OCGRP	page 198
OCIPDL	page 201
OCOFC	page 198
OFCENG	page 193
OFCVAR	page 203
PKTVPROF	page 194
QMSMIS	page 206
SITE	page 183
TOPSPARM	page 204
TOPSTOPT	page 191
TQCQINFO	page 195
TRKGRP	page 177
TRKMEM	page 189
TRKOPTS	page 180
TRKSGRP	page 178
XPMIPGWY	page 167
XPMIPMAP	page 169

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 ports on the IP-XPM used for data communication, defines the 7X07 Gateway cards, and establishes the trunk groups 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 6: "TOPS-IP engineering guidelines."

Note 2: TOPS-IP CM applications (OC-IP, QMS MIS-IP) are dependent on IP infrastructure datafill. For details on 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 5 IP infrastructure datafill sequence

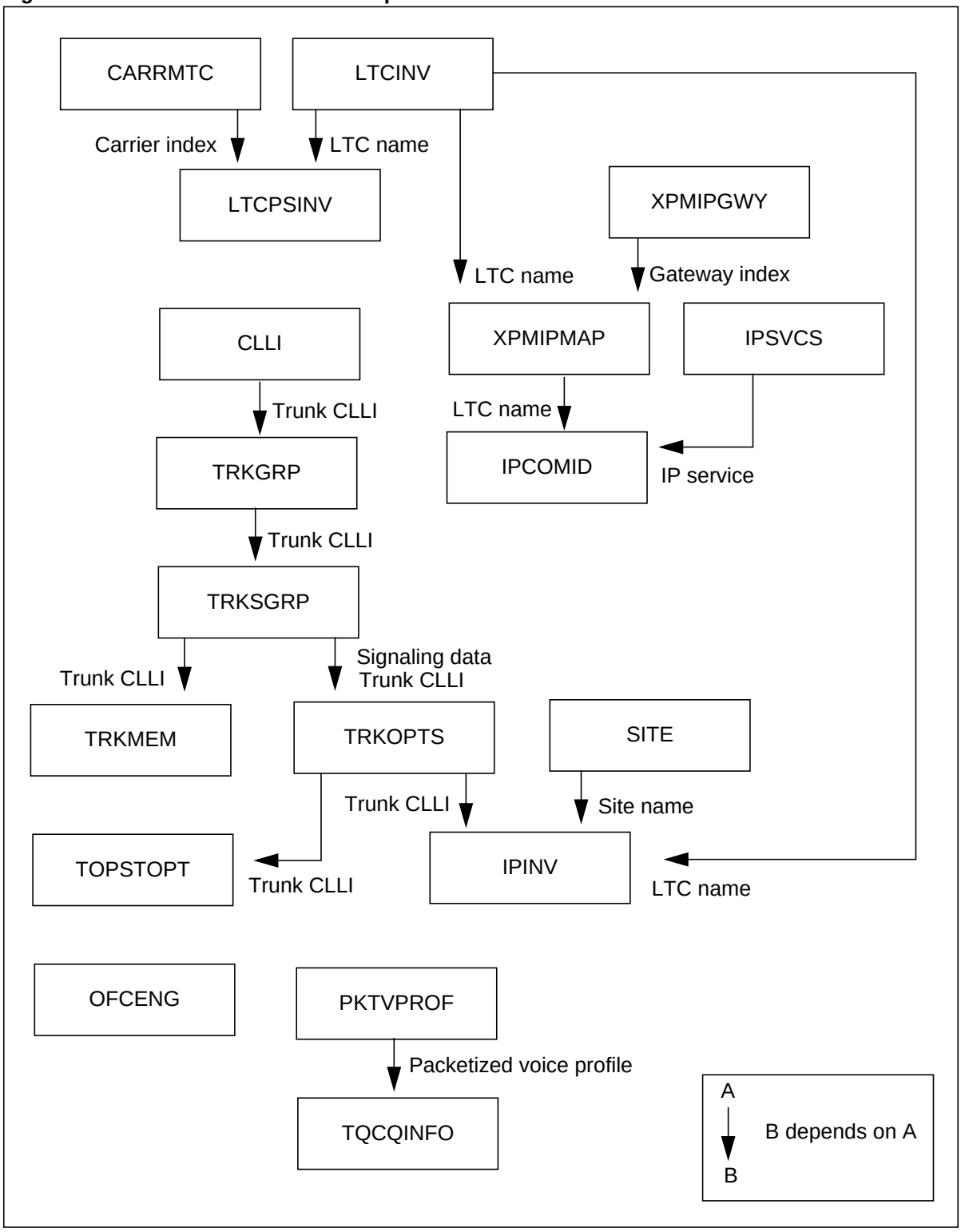
Table name	Definition
Hardware provisioning tables	
LTCINV	Line Trunk Controller Inventory. This table defines hardware for the IP-XPM (see Note 1).
CARRMTC	Carrier Maintenance. This table defines maintenance control information for peripheral modules, such as the IP-XPM (DTC).
LTCPSINV	LTC P-side Inventory. This table defines peripheral-side links for the IP-XPM.
Data provisioning tables	
XPMIPGWY	XPM IP Gateway. This table contains information on 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 associates a port and protocol for each CM IP service name.
IPCOMID	IP Communication Identifier. This table assigns a COMID number to each service and associates the COMID with local connectivity information.

Table 5 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) 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 the group of 7X07 Gateway cards datafilled in table IPINV.
IPINV	Internet Protocol Inventory. This table defines the individual 7X07 Gateway cards in the IP-XPM 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 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 a packetized voice profile used in selecting a voice codec for a call queue.
TQCQINFO	TOPS QMS Call Queue Information. This table defines TOPS QMS call queues, including the packetized voice profile to use.
Note 1: Table PMLOADS must be datafilled before table LTCINV. See the explanation for the LOAD field (page 162) and the E2PROM field (page 163) for more information. ***Note 2:*** When the DYNAMIC trunk option is set in table TRKOPTS, table IPINV automatically datafills table TRKMEM with individual trunk members.	

Figure 75 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 75 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 6 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		QD715xx	Load. Enter the load name. For TOPS15, the valid value is QD715<version>. ***Note:*** The load name QD715<version> represents the load name for IP access. This value must first be datafilled in table PMLOADS.
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. ***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.
EXTLINKS		6	Extended links. This number identifies the number of pairs of C-side 14 extended messaging links. ***Note:*** The EXTLINKS value is datafilled automatically by the CONVERTCSLINKS utility. For more information, refer to Chapter 10: “TOPS-IP CI tools.”

Table 6 Datafilling table LTCINV

Field	Subfield or refinement	Entry	Explanation and action
E2LOAD		SXFWAGxx	EEPROM firmware load. Enter the firmware load name. For TOPS15, the valid version must be at least 02. ***Note:*** The value SXFWAG<version> represents the firmware load name. This value 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. See page 152 for details.
OPTATTR		CCS7	Option attributes. Enter CCS7. ***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 76 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  QD715XX (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         SXFWAG04      (CCS7) $
       6X40FC    N
DTC 11  1002   LTE    0    51    0     C   0    6X02AF   QD715XX (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          SXFWAG04     (CCS7) $
       6X40FC    N
DTC 20  1002   LTE    0    51    0     C   0    6X02AF   QD715XX (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          SXFWAG04     (CCS7) $
       6X40FC    N
```

LTCINV error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 7 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.

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 8 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. ***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 DTC (IP-XPM) used by the Gateways for voice over IP communication.

Figure 77 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 186.

Note 3: After datafilling a new Gateway or changing the datafill for an existing Gateway, users should update the static data for the SX05DA. This is done by performing 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. For more information, refer to “Updating static data” on page 222.

The following table shows the datafill specific to TOPS-IP for table LTCPSINV.

Table 9 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. ***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 184).
	PSDATA	See refinements	P-side data. This field consists of the AREASELECT, CARRIDX, and ACTION refinements.
	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 the three DTCs. In DTC 10 and DTC 11, DS-1 signaling and TGWY (template name from table CARRMTC) are datafilled for P-side links. 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 an MIS-IP data link). No Gateway cards are installed, so the P-side links remain NILTYPE.

Figure 78 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) $

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 6: “TOPS-IP engineering guidelines.”

Note 3: An IP address in switch datafill consists of four octets delimited by a single space (no periods).

The following table shows the datafill specific to TOPS-IP for table XPMIPGWY.

Table 10 Datafilling table XPMIPGWY

Field	Subfield or refinement	Entry	Explanation and action
GWINDEX		0 to 255	Gateway index. Enter the index number for the router.
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. ***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. ***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 default router indexes.

Figure 79 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 11 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 do not take effect until the next RTS. After changing this field, users should 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. For more information, refer to “Updating static data” on page 222.

The following table shows the datafill specific to TOPS-IP for table XPMIPMAP.

Table 12 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.

Table 12 Datafilling table XPMIPMAP

Field	Subfield or refinement	Entry	Explanation and action
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: - Enter CM if the CM configures the XPM. Also datafill the following refinements: ACTADDR, INADDR, UNIT0, UNIT1, GWINDEX, DNSINFO. - Enter DHCP if the DHCP server configures the XPM. No further datafill is required.
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.

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 80 MAP display example for table XPMIPMAP

```
XPMNAME  AUTONEG  SUBNMASK       IPCONFIG  ACTADDR       INADDR
      UNIT0         UNIT1          GWINDEX           DNSINFO
-------------------------------------------------------------------------------
DTC 10   AUTO     255 255 255 0  CM        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        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 13 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. ***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 13 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 14 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. ***Note 1:*** It is recommended that OC-IP data links assign port numbers in the range 8600 to 8899. ***Note 2:*** QMS MIS-IP data links 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 four IP transport services. REMOTE_IPSVC and DAHOST_IPSVC 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 81 MAP display example for table IPSVCS

```
SERVICE           PORT       PROTOCOL
-------------------------------------------------------------------------
REMOTE_IPSVC      8660       UDP
DAHOST_IPSVC      8670       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 15 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. ***Note:*** Each TOPS-IP application has its own recommendation for port values. For details, refer to information on the specific application.

Table 15 Error messages for table IPSVCS

Error message	Explanation
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. ***Note:*** Each TOPS-IP application has its own rules for changing or deleting a service name. 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 16 Datafilling table IPCOMID

Field	Subfield or refinement	Entry	Explanation and action
COMID		0 to 1023	Communication identifier. Enter the COMID. ***Note:*** A given service may be used by more than one COMID number, but the same COMID number *cannot* use more than one service.
SERVICE		Service name from table IPSVCS	Service. Enter the name of the IP transport service.
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 seven IP COMIDs. REMOTE_IPSVC, DAHOST_IPSVC, and XIPVER distribute data communication over both DTC 10 and DTC 11. QMSMIS uses DTC 20.

Figure 82 MAP display example for table IPCOMID

```
COMID     SERVICE          XPMNAME
-------------------------------------------------------
1         REMOTE_IPSVC     DTC 10
2         REMOTE_IPSVC     DTC 11
8         DAHOST_IPSVC     DTC 10
9         DAHOST_IPSVC     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 17 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 (duplicate tuple).
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 for the specified application. ***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 any given 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 18 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. ***Note:*** Entering a value higher than 2016 wastes resources.
ADMININF		Alphanumeric up to 32 characters	Administrative information. Enter the administrative information.

CLLI example

The following example shows datafill for a switch that uses two trunk groups for the OC-IP application, OCIPTOREMOTE and OCIPTOHOST.

Figure 83 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 a given 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 19 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: - Enter 2W for two-way (used for incoming). - 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 84 MAP display example for table TRKGRP

```
GRPKEY          GRPINFO
-------------------------------------------------------------------
OCIPTOREMOTE    IT 0 TLD NCTC 2W IA MIDL 000 NPRT NSCR 619 619 000 N N $
OCIPTOHOST      IT 0 TLD NCTC OG IA 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 20 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 OC 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 in table TRKOPTS. No options are allowed.
`Table TRKOPTS DYNAMIC OC 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 in table TRKOPTS. Only MIDL or LIDL are valid.

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 21 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.

Table 21 Datafilling table TRKSGRP

Field	Subfield or refinement	Entry	Explanation and action
	DIR	2W, OG	Direction. Enter the same direction for the subgroup as in table TRKGRP. Also datafill the PROTOCOL and COTREQ refinements. ***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 85 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
```

TRKSGRP error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 22 Error messages for table TRKSGRP

Error message	Explanation
`Table TRKOPTS DYNAMIC OC 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 in table TRKOPTS. Only C7UP is allowed.
`Table TRKOPTS DYNAMIC OC 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 in table TRKOPTS. Only Q764 is allowed.
`Table TRKOPTS DYNAMIC OC 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 in table TRKOPTS.
`Table TRKOPTS DYNAMIC OC 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 in table TRKOPTS. Only 0 is allowed.

Table 22 Error messages for table TRKSGRP

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 subgroup that is defined as DYNAMIC OC in table TRKOPTS. Only 2W or OG are allowed.
`Table TRKOPTS DYNAMIC OC 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 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 23 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	Application. Enter OC for the OC-IP application.

TRKOPTS example

The following example shows the trunk options for the dynamic trunk groups.

Figure 86 MAP display example for table TRKOPTS

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

TRKOPTS error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 24 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 dynamic trunking application: Tuples for this CLLI must be deleted from Table IPINV.`	The user tries to delete 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 a tuple for a DYNAMIC OC trunking application that has datafill in table OCGRP.
`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 (NA100 software).
`For the TOPS-IP OC 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 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 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 tuple whose direction is not OG or 2W.
`For the TOPS-IP OC 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.

Table 24 Error messages for table TRKOPTS

Error message	Explanation
`For the TOPS-IP OC 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 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 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 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 dynamic trunking application: Tuples for this CLLI must be deleted from Table IPINV.`	The user tries to add a DYNAMIC tuple whose CLLI is present 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 add a DYNAMIC tuple whose CLLI is present in table OCGRP.
`For the TOPS-IP OC 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 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 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 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 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 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.

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 25 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 line modules 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 87 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: After datafilling the trunk members for a TOPS-IP application, table IPINV automatically datafills the trunk members in table TRKMEM (page 152). Removing TOPS entries in 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. 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 the PORT field for TOPS-IP applications. Refer to Table 27 on page 186 for information on how to map the port number with P-side links that are datafilled in table LTCPSINV.

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. 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 26 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 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, which refers to the unit of the Gateway and not 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.
IPPEC		7X07AA	IP PEC. Enter 7X07AA for the Gateway card.

Table 26 Datafilling table IPINV

Field	Subfield or refinement	Entry	Explanation and action
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 165). Refer to Table 27 on page 186.
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. ***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 not allow the Gateway to come 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 27 for the correct port mapping.

Note: Until the correct port datafill is present, the switch will generate PM777 log reports.

Table 27 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 the TGWY office datafilled with a total of six Gateway cards. Two trunk groups are datafilled for OC-IP: OCIPTOREMOTE and OCIPTOHOST, each of which supports 144 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 88 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
```

IPINV error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 28 Error 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 offline state.
`ERROR: Associated trunk members not INB.`	The user tries to delete a Gateway card that has been offlined 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 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. ***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 28 Error 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 fields LOAD and IPZONE 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. 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 256.
Could not allocate store. 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. 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 28 Error 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.` `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. ***Note:*** Currently all TOPS-IP switches are considered “non-bypass.”
`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, manual datafill in TRKMEM is not allowed because tuples are *automatically* datafilled by table IPINV (page 184) when a Gateway card is defined. Table IPINV datafills the members in blocks of 48.

The following table shows the datafill specific to TOPS-IP for table TRKMEM.

Table 29 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.

Table 29 Datafilling table TRKMEM

Field	Subfield or refinement	Entry	Explanation and action
	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 24 of the 144 trunk members in group OCIPTOREMOTE that are automatically datafilled by table IPINV.

Figure 89 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 3       0    DTC 10 6 4
OCIPTOREMOTE 4       0    DTC 10 6 5
OCIPTOREMOTE 5       0    DTC 10 6 6
OCIPTOREMOTE 6       0    DTC 10 6 7
OCIPTOREMOTE 7       0    DTC 10 6 8
OCIPTOREMOTE 8       0    DTC 10 6 9
OCIPTOREMOTE 9       0    DTC 10 6 10
OCIPTOREMOTE 10      0    DTC 10 6 11
OCIPTOREMOTE 11      0    DTC 10 6 12
OCIPTOREMOTE 12      0    DTC 10 6 13
OCIPTOREMOTE 13      0    DTC 10 6 14
OCIPTOREMOTE 14      0    DTC 10 6 15
OCIPTOREMOTE 15      0    DTC 10 6 16
OCIPTOREMOTE 16      0    DTC 10 6 17
OCIPTOREMOTE 17      0    DTC 10 6 18
OCIPTOREMOTE 18      0    DTC 10 6 19
OCIPTOREMOTE 19      0    DTC 10 6 20
OCIPTOREMOTE 20      0    DTC 10 6 21
OCIPTOREMOTE 21      0    DTC 10 6 22
OCIPTOREMOTE 22      0    DTC 10 6 23
OCIPTOREMOTE 23      0    DTC 10 6 24
```

TRKMEM error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 30 Error messages for table TRKMEM

Error message	Explanation
`Table TRKOPTS DYNAMIC OC option is assigned. Manual operations are not allowed in Table TRKMEM.TRKMEM data conflicts with data in table TRKOPTS.`	The user tries to change a member of a trunk group that is defined as DYNAMIC OC 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.

The DMS switch invokes the MAXCONNS function during trunk selection for each TOPS-IP call when the trunk group's MAXCONNS field is set to a value less than 2016. The switch does not invoke the MAXCONNS function when the value is 2016 or greater, or when the 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.

Note: For more information on reducing dynamic trunk members, refer to "Limiting the number of available dynamic trunks" on page 69.

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 31 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. The CLLI must be defined as DYNAMIC in table TRKOPTS.
MAXCONNS		0 to 32767	Maximum connections. Enter the maximum number of voice connections supported by this dynamic trunk group. ***Note 1:*** A value of 0 specifies no connections allowed for that trunk group. ***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 two trunk groups.

Figure 90 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
```

TOPSTOPT error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 32 Error messages for table TOPSTOPT

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.
`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 is not supported in the switch software. The value is set to 2016, but 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 33 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 card's C-side links. In all standard office configurations, the value of this parameter should be set to AUTO (default). ***Note*:** Any change in the value of this parameter requires the Gateway card to be reloaded.
NUMPERMEXT	0 to 32767	1	This parameter allocates data structures for calls. For TOPS-IP, this value should be incremented by one for each member of a remote trunk group (defined with a direction of OG in table TRKGRP).

Table 33 Datafilling table OFCENG

Parameter name	Range of values	Default value	Explanation
TOPS_NUM_OC_EXT	0 to 32767	100	This parameter 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. (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 value of this parameter.			

OFCENG example

The following figure shows example datafill for the OFCENG parameters.

Figure 91 MAP display example for table OFCENG

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

PKTVPROF

Table PKTVPROF defines profiles used for packetized voice. The profile index specifies a voice codec and is referenced in table TQCQINFO by call queue. The codecs supported are G.711 and G.729. If G.729 is datafilled, silence suppression may also be specified. The use of silence suppression discontinues the codec output if it detects parts of a signal where there is no speech. NOSILSUP (default) specifies no silence suppression; SILSUP specifies silence suppression.

Note 1: Datafilling the G.729 codec is not recommended if carrier-grade voice is required.

Note 2: Table PKTVPROF contains two default tuples, 0 and 1.

The following table shows the datafill specific to TOPS-IP for table PKTVPROF.

Table 34 Datafilling table PKTVPROF

Field	Subfield or refinement	Entry	Explanation and action
PROFNUM		0 to 63	Profile number. Enter the profile index.
PKTVFLDS		See subfields	Packetized voice fields. This field contains the subfields CODEC and refinements specific to the codec entered.
	CODEC	G711, G729	Codec. Enter the voice codec for the profile. If G729 is datafilled, also enter a value for the SILEN refinement.
	SILEN	NOSILSUP, SILSUP	Silence suppression. Enter SILSUP to allow silence suppression to be performed; otherwise enter NOSILSUP.

PKTVPROF example

The following example shows datafill for three packetized voice profiles.

Figure 92 MAP display example for table PKTVPROF

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

TQCQINFO

Table TQCQINFO defines TOPS call queues, including the packetized voice profile index (at the OC remote switch) that applies to the call queue. 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 35 Datafilling table TQCQINFO

Field	Subfield or refinement	Entry	Explanation and action
PKTVPROF		Profile from table PKTVPROF	Packetized voice profile. Enter the profile that applies to the call queue.

TQCQINFO example

The following example shows datafill for three packetized voice profile indexes against call queues.

Figure 93 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 159.

Table datafill dependencies

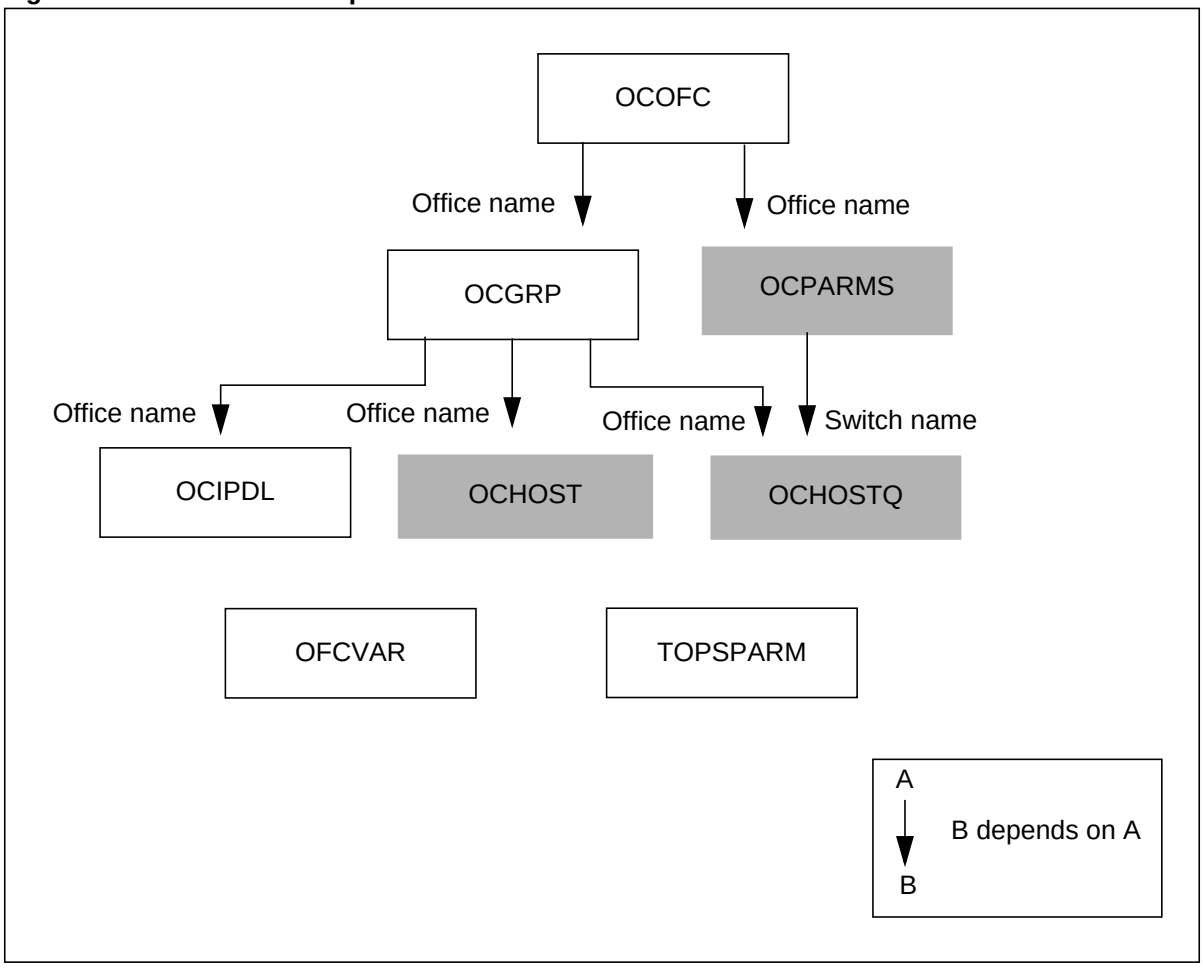
The following OC-IP tables are listed in the order in which they should be datafilled.

Table 36 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 a voice link group and data link group with each office. This table also contains an IP data link selector.
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.

Figure 94 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 94 OC-IP datafill dependencies



Note 1: Tables OCPARMS, OCHOST, OCHOSTQ are shown in Figure 94 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 37 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.

Figure 95 MAP display example for table OCOFC

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

OCGRP

Table OCGRP identifies each distant office referenced in table OCOFC as a host or remote. The datafill also associates an OC-IP voice trunk group with a particular 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. This functionality differs from DCM OC or ETMS OC, for which it is recommended (but not required) to datafill the data link member tables before using the data link group in OCGRP.

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 38 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: - OG direction for a host office voice trunk CLLI. - 2W direction for a remote office voice trunk CLLI.
DLOVRLAY		IP	Data link overlay. Enter IP. ***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 a value of 50 (or greater). ***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 three offices that have IP data and voice connectivity with the switch.

Figure 96 MAP display example for table OCGRP

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

OCGRP error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 39 Error 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. ***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.
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 side 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. This ensures that each OC switch is aware of the data links used for IP transport services, so that data messages can be routed to the correct XPM and to the correct application software. 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 40 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. ***Note:*** It is recommended that OC-IP data links assign port numbers in the range 8600 to 8899.

OCIPDL example

The following example shows four data links datafilled for each of three distant offices.

Figure 97 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
```

OCIPDL error messages

The following table lists possible error messages related to adding, changing, or deleting tuples.

Table 41 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 offline 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.

Table 41 Error messages for table OCIPDL

Error message	Explanation
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.
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. INTERNAL ERROR #2	Contact Nortel Networks technical support.
ERROR: INVALID APPLICATION ID. INTERAL ERROR #4.	Contact Nortel Networks technical support.
ERROR: UNABLE TO VALIDATE COMID. INTERNAL ERROR #5	Contact Nortel Networks technical support.
ERROR: UNREGISTERED APPLICATION. INTERNAL ERROR #6	Contact Nortel Networks technical support.
ERROR: MISC IP COMID BIND ERROR. 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 42 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.

OFCVAR example

The following example shows datafill for the OFCVAR parameters.

Figure 98 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 TOPS-IP for table TOPSPARM.

Table 43 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 state of an OC-IP data link is changed from INSV to SYSB.

TOPSPARM example

The following example shows datafill specific to TOPS-IP for table TOPSPARM.

Figure 99 MAP display example for table TOPSPARM

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

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 159 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 44 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 45 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. ***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. ***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 45 Datafilling table QMSMIS

Field	Subfield or refinement	Entry	Explanation and action
	DESSTAT	INACTIVE, ACTIVE	Destination status. Enter the desired destination status. ***Note 1:*** When the destination status of the node is set to INACTIVE, the switch does not send MIS message buffers to this node. ***Note 2:*** When the DESSTAT field is changed from ACTIVE to INACTIVE, messages may be lost. ***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 100 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 46 Error messages for table QMSMIS

Error message	Explanation
`You must set DATALINK to IP or MPC for TOPS MIS facility.` `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 46 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 159 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 10: "TOPS-IP CI tools."

Chapter 8: TOPS-IP software ordering

The TOPS-IP product is not planned to be generally available; however, it may be ordered by special arrangement. TOPS-IP functionality is intended only for the North American market. For more details, contact your Nortel Networks representative.

This chapter provides information on ordering both PCL (product computing module load) and NCL (non-CM) software loads.

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.

Note: SOC provides an interface at the MAP terminal. Users can enable or disable options, 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.

TOPS-IP infrastructure—OSB00101

The SOC code for the TOPS-IP infrastructure is OSB00101, Basic Operator Services.

OC-IP application—ENSV0107

The SOC code for OC-IP is ENSV0107, TOPS-IP OC. This order code must be in the ON state before OC-IP data links may 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. Furthermore, the ENSV0107 order code requires the TEL00011 order code (see description on page 212).

QMS MIS-IP application—OSB00101

The SOC code for QMS MIS-IP is OSB00101, Basic Operator Services. Although OSB00101 has no prerequisites, the QMS MIS-IP functionality requires the TEL00011 order code (see description on page 212).

C-side 14 Extended Messaging—TEL00011

The SOC code for C-side 14 extended messaging is TEL00011. C-side 14 is a prerequisite for TOPS-IP applications.

Position-IP application

This option is not orderable.

NCL software loads

The following NCL software corresponds to the TOPS15 PCL software:

- TGWY0003 provides the 7X07AA Gateway Release 3 functionality.
- QD715 provides the IP-XPM functionality.

  Note: Users should load the latest version of QD715 software.

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 9: TOPS-IP maintenance activities

This chapter discusses maintenance activities for the following TOPS-IP areas:

- IP Gateway (IPGW) maintenance (page 217)
- TOPSIP MAP (maintenance and administration position) level (page 246)
- OC-IP data link maintenance (page 247)
- TOPS QMS MIS-IP maintenance (page 262)

Note: For information on using switch CI tools, refer to Chapter 10: "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 Gateway cards (page 218)
- Datafilling the Gateway cards (page 219)
- Updating static data (page 222)
- Using the MAP commands at the IPGW level (page 222)
- Bringing a Gateway card into service (page 225)
- Troubleshooting the Gateway (page 231)
- Maintaining dynamic voice trunks (page 240)

Note: Before performing any maintenance on the Gateway cards, users should review the limitations and restrictions listed in Chapter 5: "TOPS-IP feature impact."

Installing the 7X07AA Gateway cards

Figure 101 shows the slot positions and related port numbering for up to 10 Gateway cards in the IP-XPM shelf (front view).

Figure 101 7X07AA Gateway card slot position and port numbering in the IP-XPM

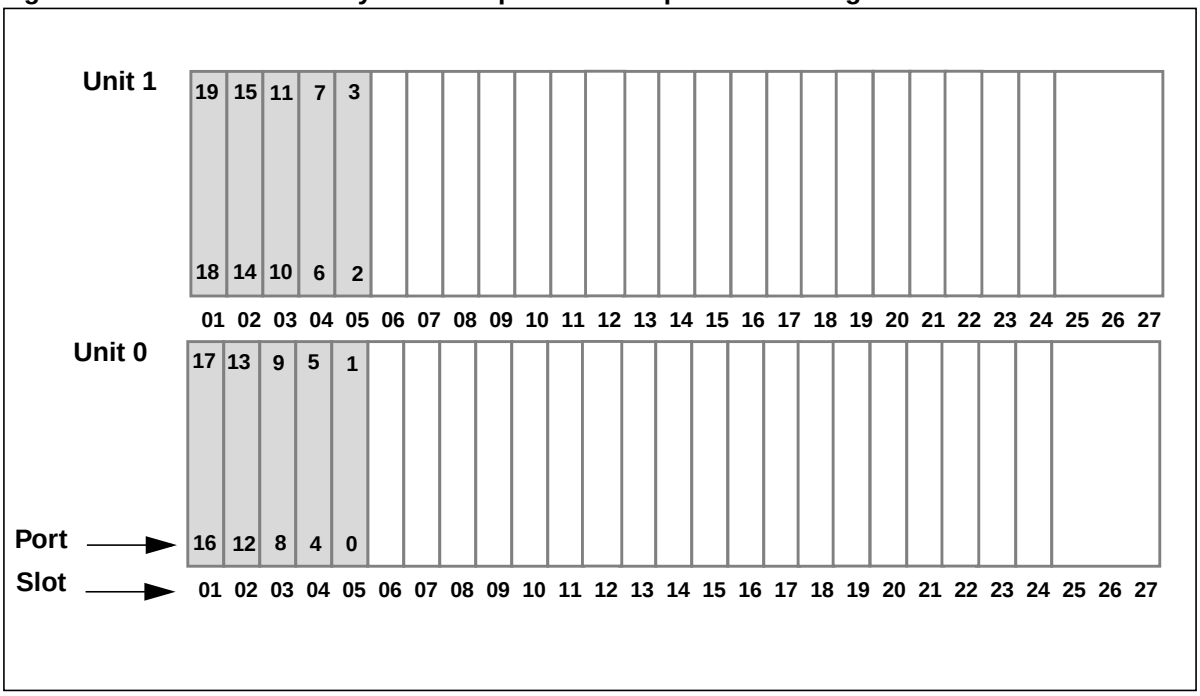


Table 47 lists the correct port mapping that is defined through datafill in tables LTCPSINV and IPINV.

Note: Until the correct port datafill is present, the switch will generate PM777 log reports.

Table 47 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 7: "TOPS-IP data schema" for datafill sequence and details on fields and valid values.

Note 2: For Gateway engineering information, refer to Chapter 6: "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 102 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 47 on page 218.

Note 3: After completing the datafill for a new Gateway or changing the datafill for an existing Gateway in table LTCPSINV, static data for the SX05DA should be updated. Refer to "Updating static data" on page 222.

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 11. 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 three Gateways defined in table IPINV.

Figure 103 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) $
```

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 104 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 six Gateway cards identified by the site name TGWY. Three Gateway cards are located in DTC 10 and three are located in DTC 11. Associated with the Gateway cards are the TOPS application and the OCIPTOREMOTE and OCIPTOHOST trunk groups, each of which supports 144 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 47 on page 218.

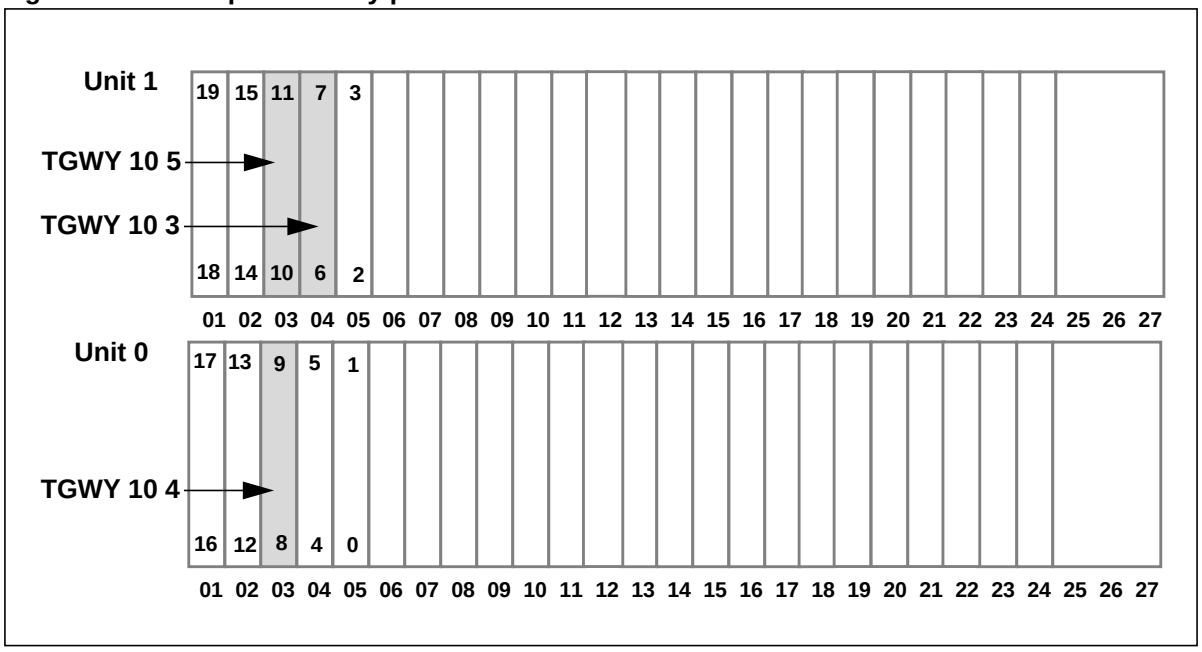
Note 2: TOPS Gateways require the correct IP address in the IPZONE field. In the OC host switch, the primary IP address must match the one assigned to the Gateway by the DHCP server. Any mismatch between DHCP datafill and CM datafill for a Gateway will not allow the Gateway to come into service.

Figure 105 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 106 shows an example of the Gateway packfill for DTC 10.

Figure 106 Example Gateway packfill to match datafill for DTC 10



Updating static data

Static data for the SX05DA card should be updated after users perform the following datafill:

- After datafilling a new Gateway or changing the datafill for an existing Gateway in table LTCPSINV
- After changing 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.

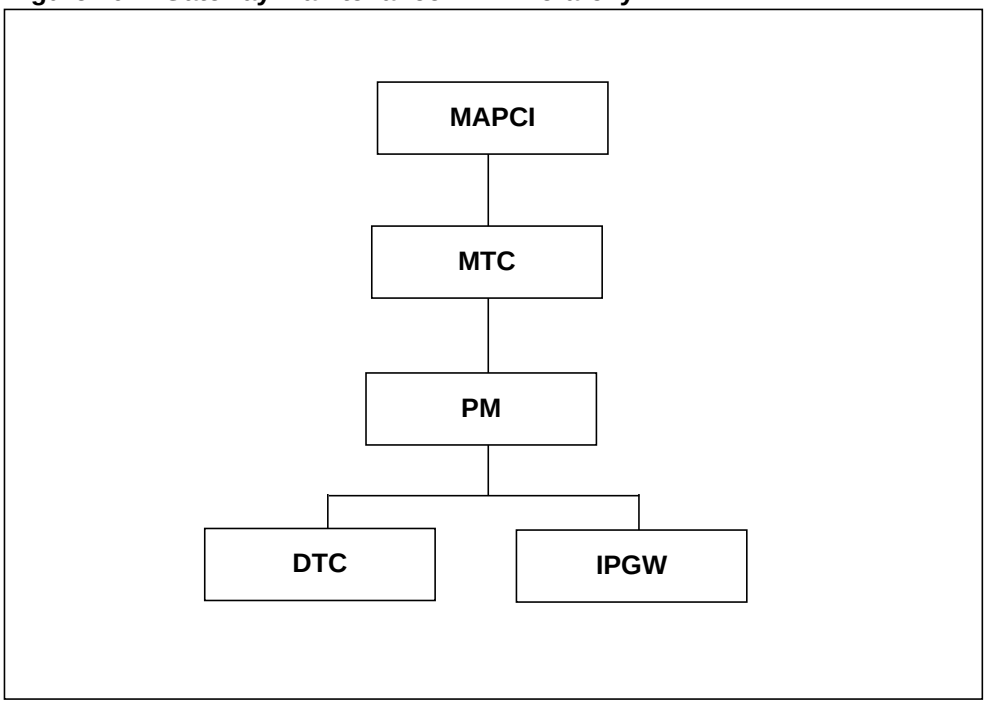
The automatic recovery takes three to four minutes. To recover the Gateways faster, they can be posted at the MAPCI;MTC;PM;IPGW level and manually busied and returned to service (with the FORCE option). This should be done after the Gateway's state is updated to SYSB by the system.

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 107 shows the MAP menu hierarchy.

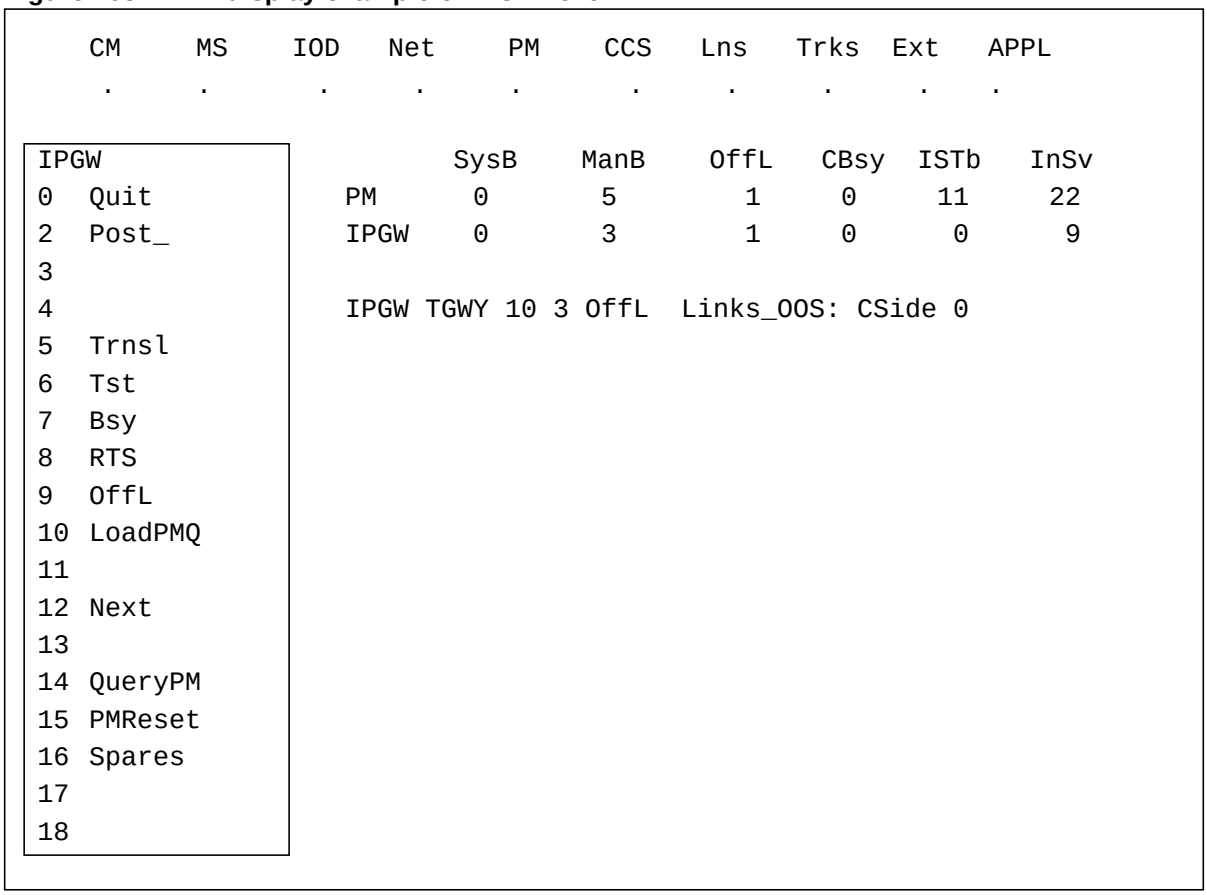
Figure 107 Gateway maintenance MAP hierarchy



IPGW MAP level

Figure 108 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 108 MAP display example of IPGW level



The following list briefly describes the IPGW commands in the order in which they appear at the MAP:

- QUIT returns the user to the previous MAP level or, or if used with the ALL parameter, returns the user to the CI level.
- 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 offlines 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 219). The DHCP server, which provides configuration information for the Gateway cards, also must be properly installed and configured with Nortel Networks 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 109 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 card. Type

```
>TRNSL P
```

and press the Enter key. The P-side links transition from offline to manual busy (MBSY) automatically during the datafill processing for table IPINV

Figure 110 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 111 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 112 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.

Figure 113 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 05 0 PMReset/LoadPMQ Passed
10 LoadPMQ            THE IPGW CONTAINS A VALID LOAD.
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

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 231 for information on error messages and user actions.

8 Bring the Gateway card into service. Type

```
>RTS
```

and press the Enter key.

Figure 114 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
```

Note: If RTS is not successful, refer to “Troubleshooting the Gateway” on page 231.

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 235). PMRESET reloads the Gateway card. If PMRESET is not successful, refer to “PMRESET error” on page 234.

Figure 115 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 05 0 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                 >LOADPMQ
8  RTS                 LOAD QUERY HAS BEEN SUBMITTED...
9  OffL                IPGW TGWY 05 0 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 234.

Figure 116 MAP display example of IPGW level—RTS error message

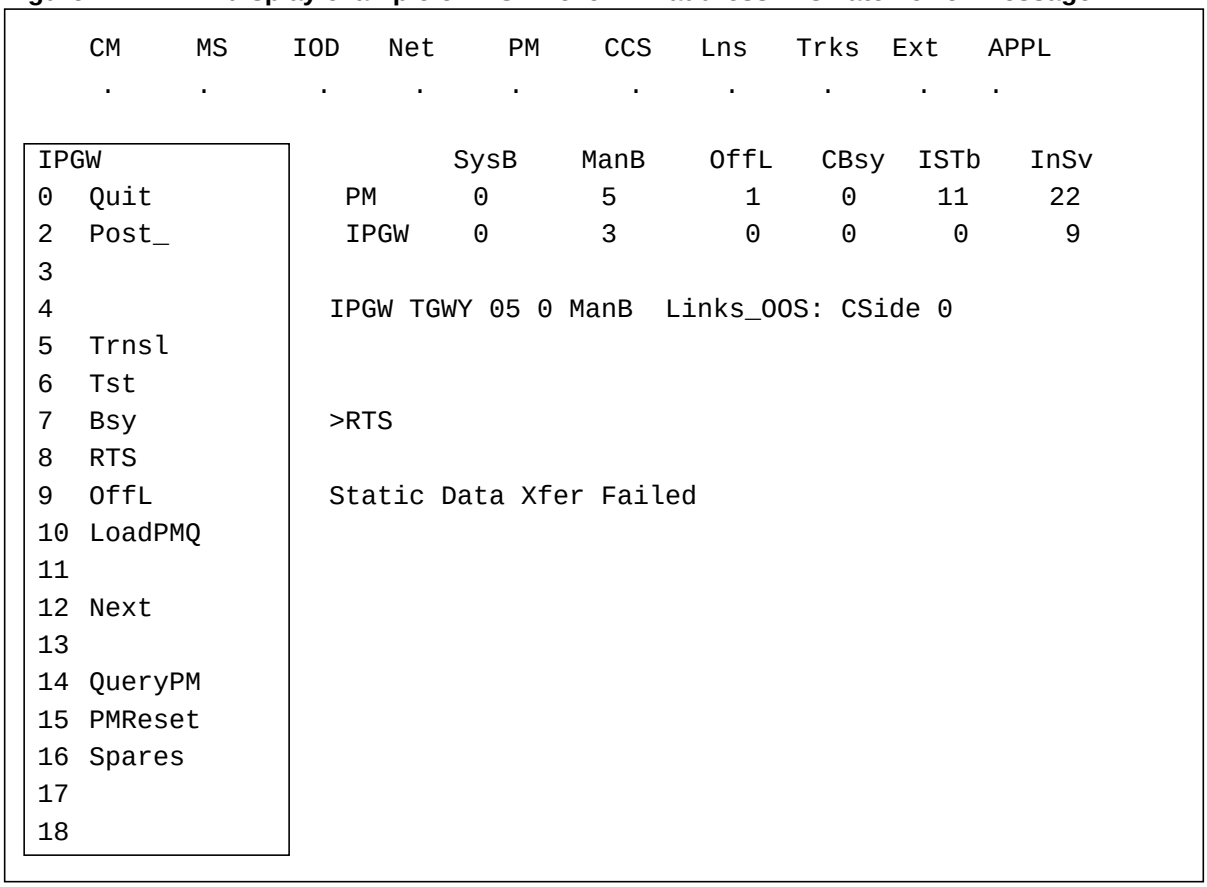
```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

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 05 0 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 117 MAP display example of IPGW level—IP address mismatch error message

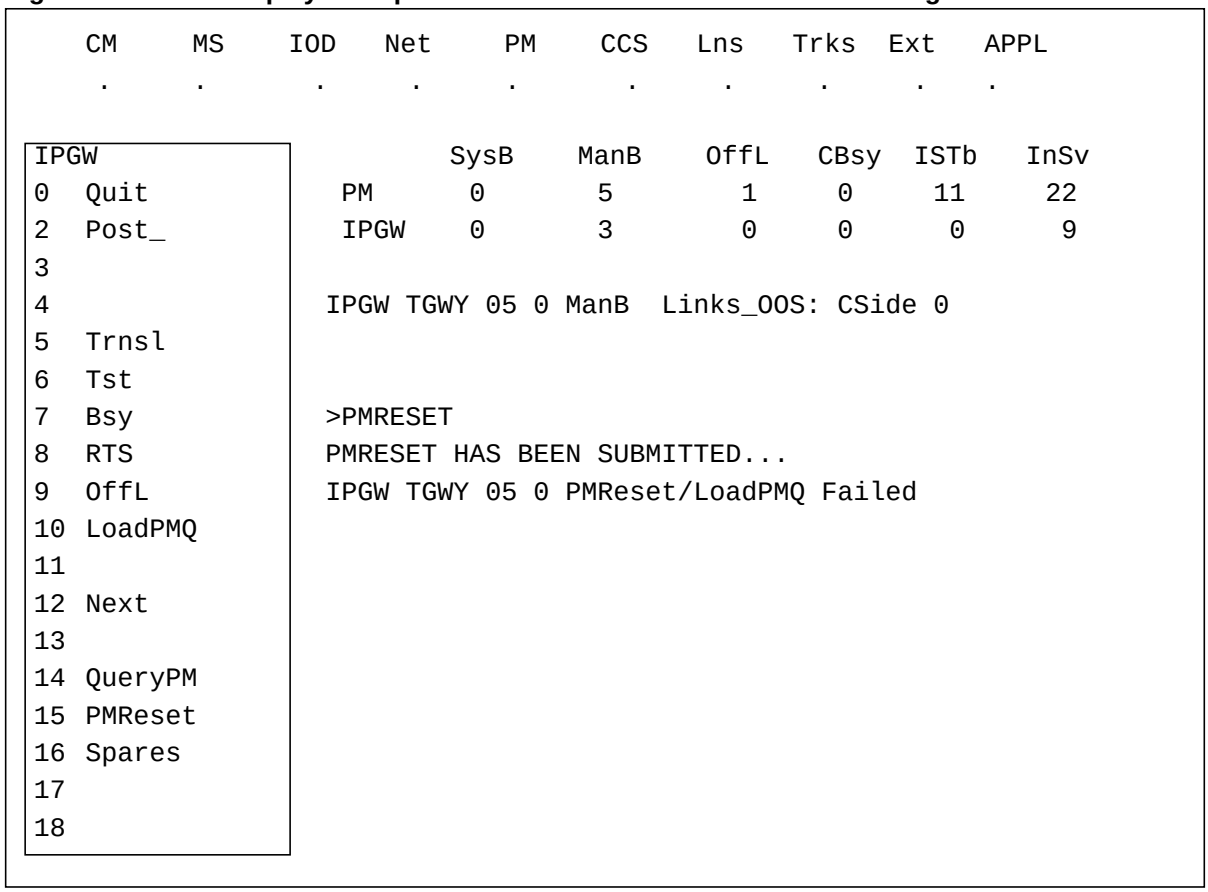


PMRESET error

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 118 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 230) of "Procedure: Bringing a Gateway card into service."

Figure 119 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 05 0 ManB  Links_OOS: CSide 0
5  Trnsl
6  Tst
7  Bsy                >PMRESET
8  RTS                PMRESET HAS BEEN SUBMITTED...
9  OffL               IPGW TGWY 05 0 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 48 when a Gateway fails to load.
- Use Table 49 when a Gateway fails to RTS.
- Use Table 50 when a Gateway goes SYSB.
- Use Table 51 when the active LED is off.
- Use Table 52 when the active LED is blinking.
- Use Table 53 for miscellaneous error conditions.

Table 48 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 49 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. 2. Perform an out-of-service test if RTS fails again. 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 50 Gateway goes SYSB

Error condition	User action
The 7X07 self-test failed.	1. Post the Gateway at the MAP and issue the PMRESET command. 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. ***Note:*** For more information on Gateway diagnostics, refer to “Gateway card diagnostics” on page 236.

Table 51 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 52 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. If SYSB, busy the posted Gateway card, issue the LOADPMQ command, and return to service the Gateway. If OFFL, then busy the posted Gateway card, issue the LOADPMQ command, and return to service the Gateway.

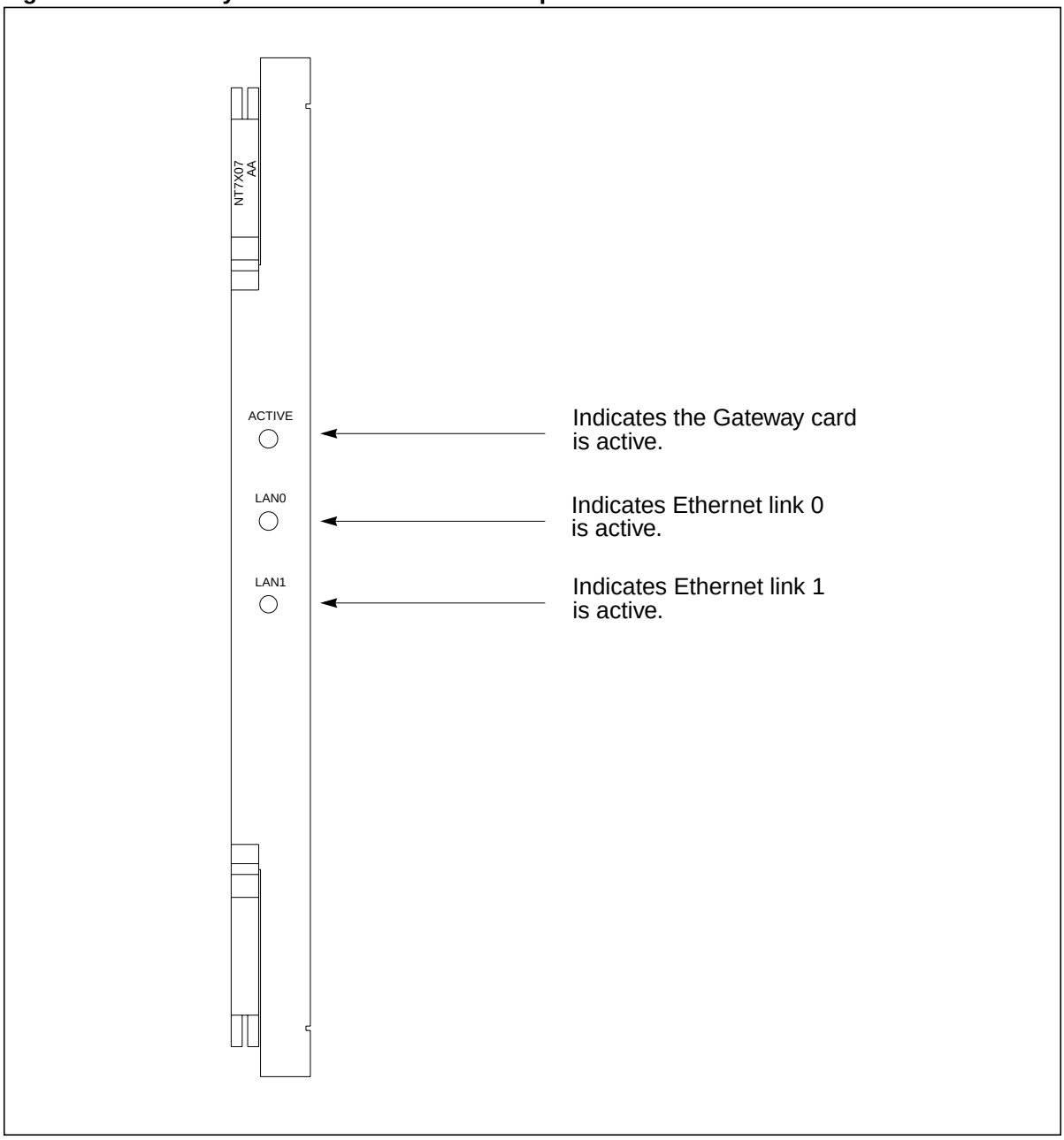
Table 53 Miscellaneous error conditions

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 120 shows the LED indicators on the faceplate.

Figure 120 Gateway LED indicators on the faceplate



The following table describes the possible Gateway or link states that correspond to the LED states.

Table 54 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 offline.
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

The OC-IP application uses dynamic voice trunks. The maintenance strategy for dynamic trunking is based on the operation of the 7X07 Gateway cards in the IP-XPM. Since a Gateway does not maintain any trunk information, dynamic trunks must mimic the state of the Gateway.

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 55 compares the Gateway states to the trunk states.

Table 55 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 offline. The Gateway card is offline 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 details, refer to “Limiting the use of dynamic voice links” on page 244.)
- 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 to limit member usage within a trunk group. (For details, refer to "Limiting the use of dynamic voice links" on page 244.)
- 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 offline state must be done at the CARRIER level, not at the PM level. Other commands (for example, busying from a non-offline state) are done at the PM level.

Limiting the use of dynamic voice links

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.

Each Gateway card supports 48 trunk members. When a maximum is datafilled in MAXCONNS, the switch loops over all in-service Gateway cards for the affected trunk group and calculates a member limit for each card. This allows the maximum specified to be distributed across all in-service Gateway cards. So, for example, if MAXCONNS is set to 100, and three Gateway cards are associated with the trunk group, the first card is limited to 34 members and the second and third cards are limited to 33 each.

During call processing, the switch checks Gateway trunk members as they are selected. If a trunk member is not usable due to the MAXCONNS limit, the switch places the trunk member in a holding queue and selects another member. Unusable trunks appear as restricted idle (RES) when viewed at the TTP level of the MAP. The call processing deload (CPD) function is not used when a MAXCONNS limit is datafilled.

If a user changes the MAXCONNS value, the limit on each in-service Gateway card is updated with the new limit. This allows the new set of usable trunks to be evenly distributed across the in-service cards. Trunk members are moved into or out of the holding queue as necessary. No calls end as a result of changing the MAXCONNS value.

As Gateway cards are added and brought into service, the limit per card is reduced so that each card supports the same number of available members. Likewise, as Gateway cards are removed from service, the available members are redistributed among the remaining cards.

TOPS-IP dynamic trunks are moved to the holding queue (and to the RES state) during trunk selection. To reduce per-call CPU use, TOPS-IP trunk selection moves only a handful of trunk members to the holding queue during a single call. During subsequent calls, additional members move to the holding queue. As a result, there may be a short time when the number of usable members in a trunk group is more than the datafilled limit. As new calls arrive and further trunk selection occurs, more members are moved to the holding queue until the number of unusable trunks is equal to the limit.

Note: For details on datafilling MAXCONNS in table TOPSTOPT, refer to Chapter 7: “TOPS-IP data schema.”

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 was created as part of the preparatory work to support IP positions. Although IP positions are not orderable, the TOPSPOS level is still visible at the MAP.
- The OCDL command accesses the OCDL MAP level used to maintain OC-IP data links (see "OC-IP data link maintenance" on page 247.)

Figure 121 shows an example of the TOPSIP MAP display.

Figure 121 MAP display example of TOPSIP level

```
    CM     MS    IOD   Net     PM    CCS   Lns   Trks  Ext   APPL
     .      .      .     .      .      .     .     .     .     .

                   OAMAP      SDM      SWMTC    SDMBIL    TOPSIP
                     .          .        .         .          .

TOPSIP
0  Quit
2                  OCDL: .   TOPSDEV: .   IPOS: .    IPDB: .
3  TOPSDEV
4  TOPSPOS
5  OCDL
6
7
8                  MTC:
9                  APPL:
10                 TOPSIP:
11
12
13
14
15
16
17
18
```

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 247)
- Maintenance states and transitions (page 249)
- Data link recovery (page 251)
- End-to-end connectivity (page 251)
- OCDL level MAP commands (page 252)
- Related alarms (page 260)
- Related logs (page 262)

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 217.

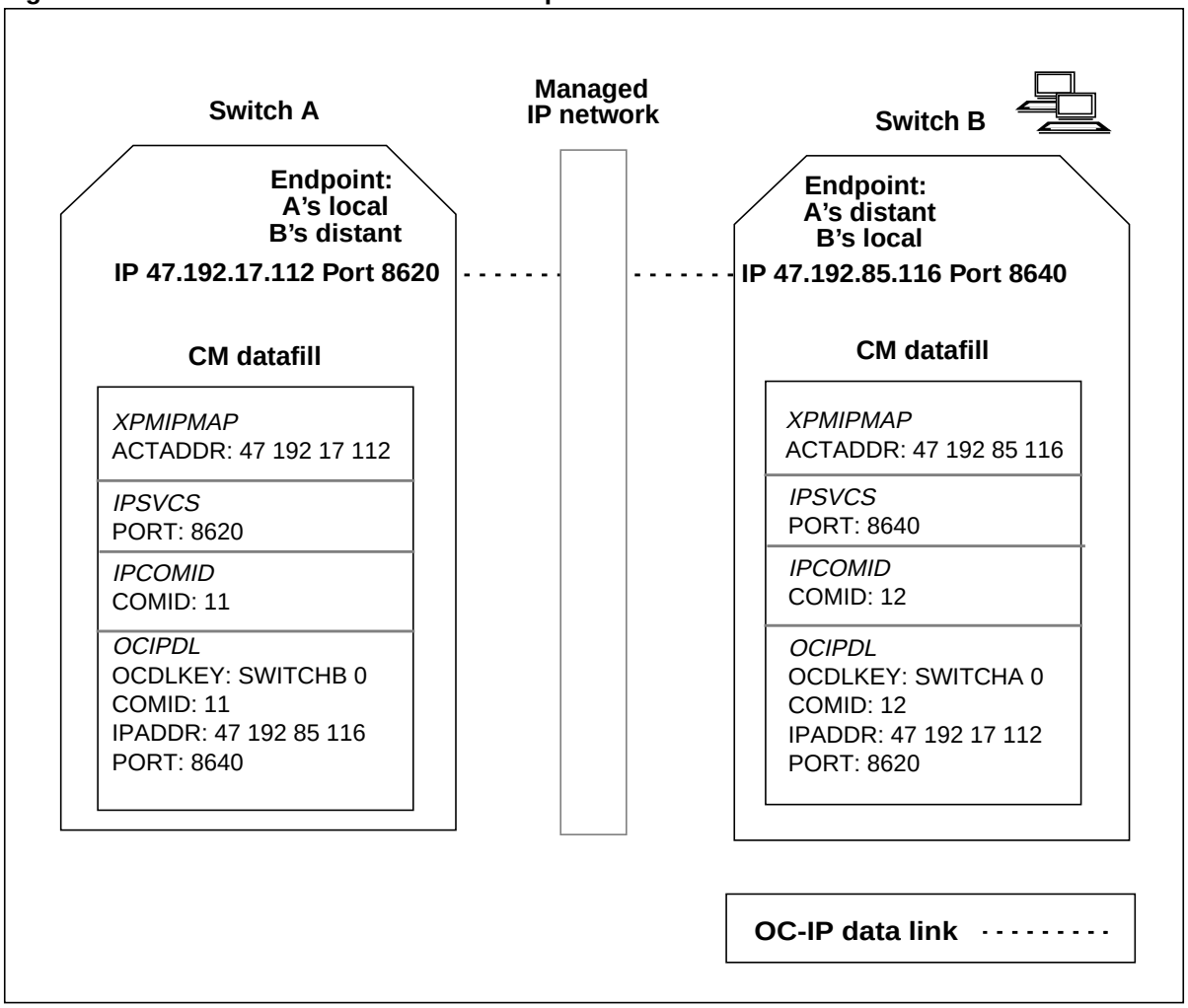
Data link connectivity

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 122 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 122 OC-IP data link connection endpoints and related datafill



Note: Datafill shown in Figure 122 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

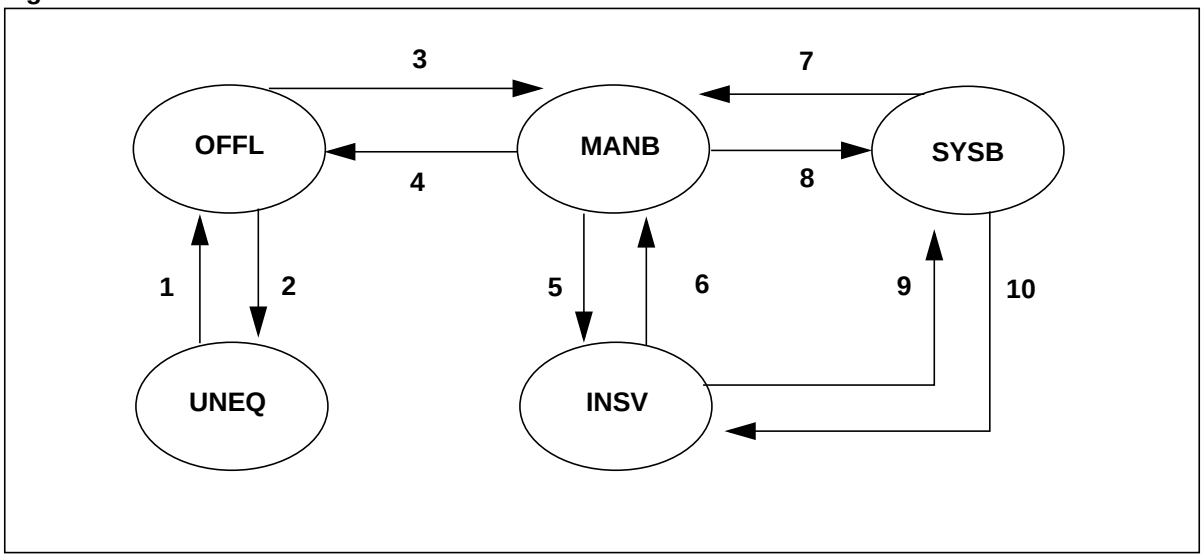
Table 56 describes the maintenance states for OC-IP data links.

Table 56 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	Offline 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: - The SX05 (on the IP-XPM) associated with the COMID is in service. - 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. - The local endpoint of the data link must have connectivity with the distant endpoint. 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 123. Each transition number is described following the figure. (MAP commands are described beginning on page 252.)

Figure 123 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 offlined 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 57.

Table 57 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.

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.

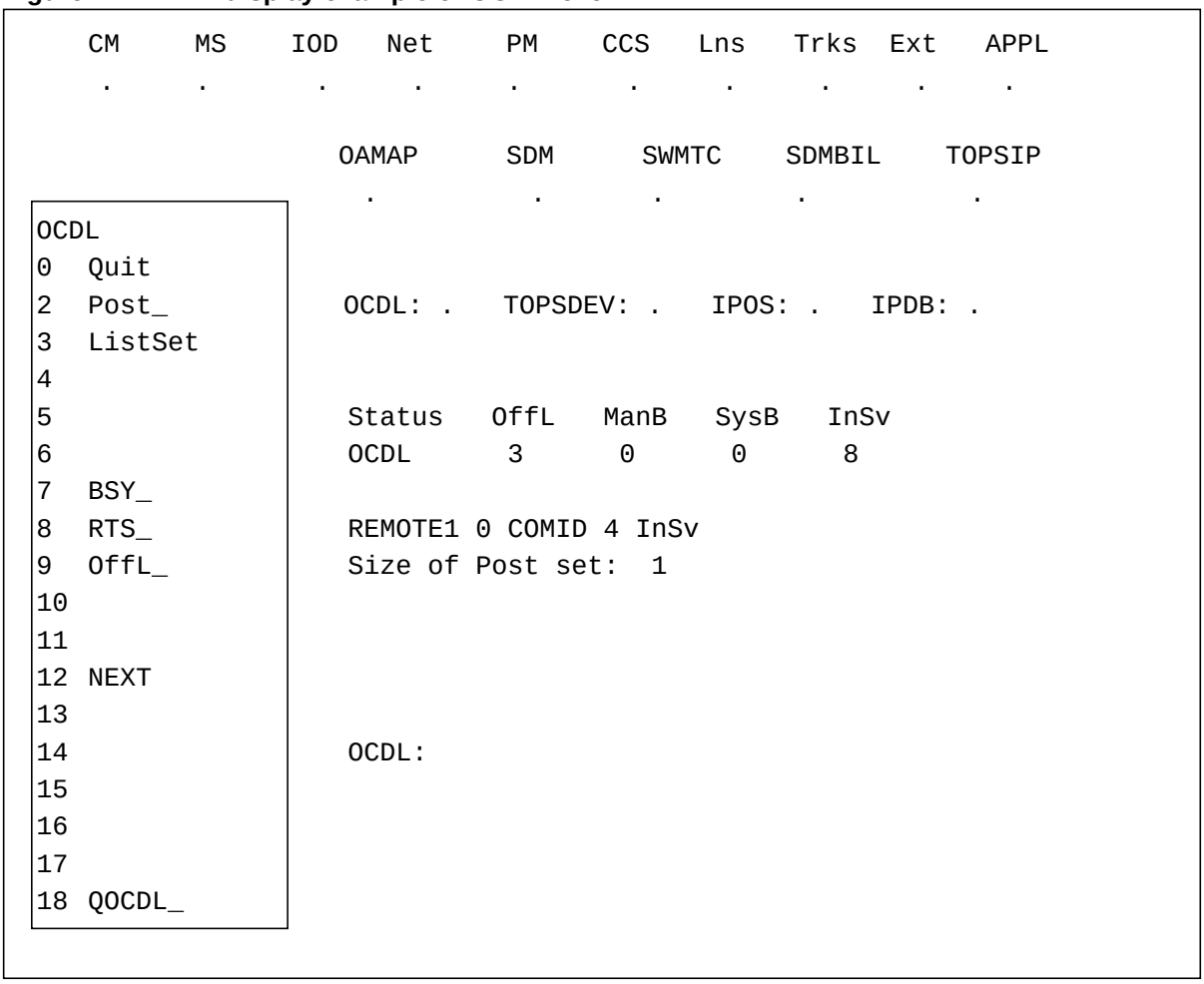
Note: There are reasons other than audits that may cause an OC-IP data link to go SYSB. For more information refer to log report “TOPS304” on page 351.

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 124 shows an example of the OCDL MAP display. In the figure, the status (INSV) of the currently posted data link (REMOTE1 0) is displayed along with its COMID (4). The post set contains one data link.

Figure 124 MAP display example of OCDL level



The next subsections provide details on parameters and responses for the OCDL MAP commands:

- QUIT (page 253)
- POST (page 254)
- LISTSET (page 255)
- BSY (page 255)
- RTS (page 256)
- OFFL (page 257)
- NEXT (page 258)
- QOCDL (page 259)
- RECREATE (unlisted) (page 260)

QUIT

Exits user from the OCDL MAP level. When QUIT is executed successfully, control is returned to the level specified by the user.

Table 58 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 59 QUIT responses and actions

Response	Explanation	User action
`QUIT–Unable to quit requested number of levels` `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 60 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 61 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` `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` `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` `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` `Could Not Create Post Set`	User specified a COMID that is not provisioned in table table OCIPDL.	Check table OCIPDL.

Table 61 POST responses and actions

Response	Explanation	User action
`There are no data links in the (OffL, ManB, SysB, InSv) state` `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 62 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 63 BSY parameters

Parameter	Definition
ALL	Busies all posted data links.

The following table lists common error responses, explanations, and actions.

Table 64 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 125 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 65 RTS parameters

Parameter	Definition
ALL	Returns to service all posted data links.

The following table lists common error responses, explanations, and actions.

Table 66 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 351 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

Offlines 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 67 OFFL parameters

Parameter	Definition
ALL	Offlines all posted data links.

The following table lists common error responses, explanations, and actions.

Table 68 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 69 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 70)
- distant IP address and port (see Note 2 in Table 70)

Table 70 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. ***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. ***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 71 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.
`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 126 shows an example of a successful QOCDL command response at the MAP.

Figure 126 Example of successful QOCDL command response

```
Data Link:                DAHOST 0
Data Link State:          InSv
SysB Reason:              No Failure
COMID:                    8
XPM:                      DTC 10
Local IP Address:         47.192.3.24
Local Port Number:        8602
Distant End IP Address:   47.192.63.100
Distant End Port Number: 8602
```

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 72 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

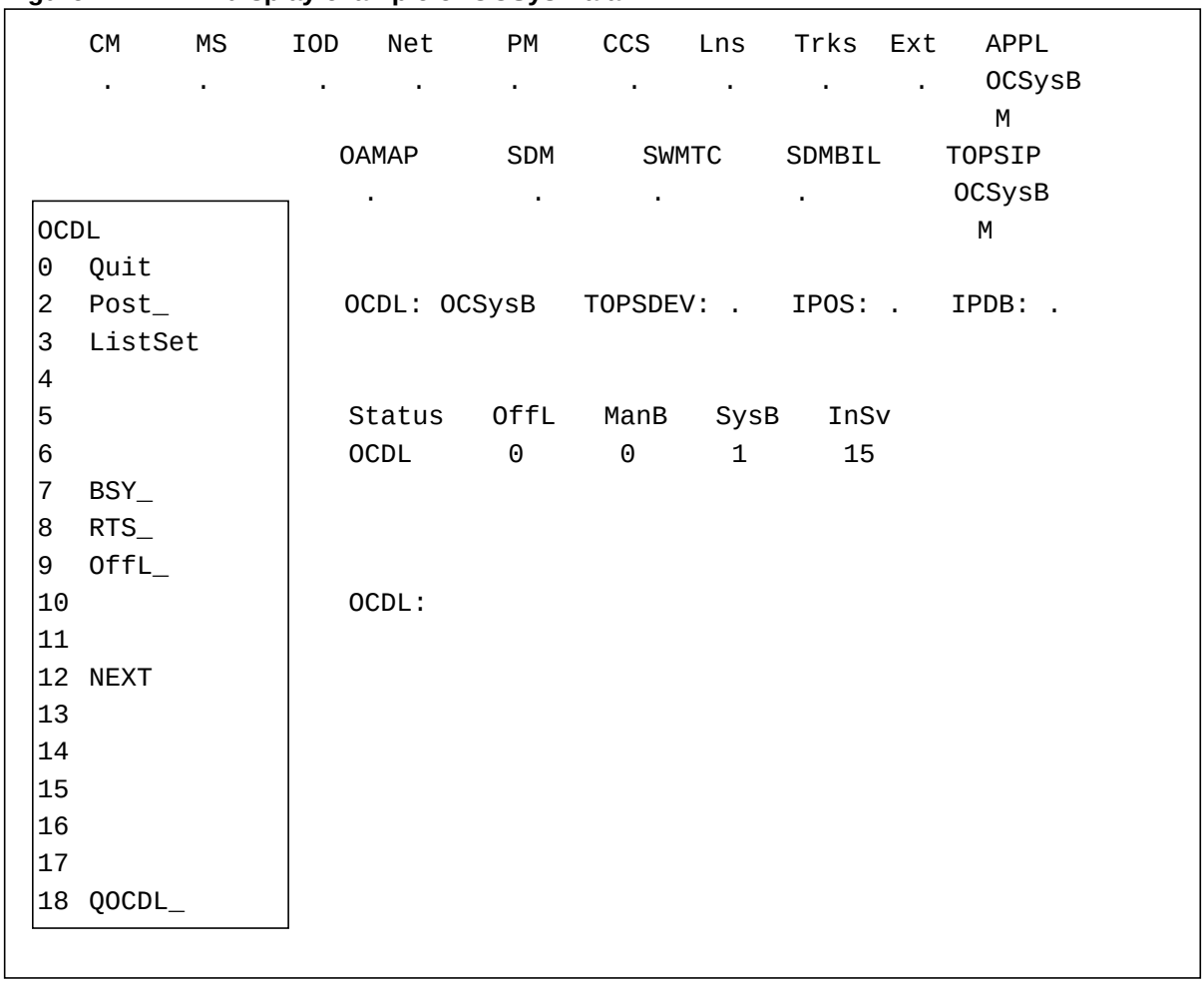
The switch raises an OCSysB alarm when an OC-IP data link transitions to the SYSB state. The OCSysB alarm is lowered if there are no longer any SYSB data links. The severity of the alarm is associated with the following conditions:

- 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.

Display of OCSysB alarm

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. Figure 127 shows an example of the OCSysB alarm at the MAP.

Figure 127 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 and 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 11: "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 peripheral that supports QMS MIS-IP must be a dedicated peripheral that does not contain 7X07 Gateway cards (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 6: "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 73 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 73 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 (swerrs), and traps to find the cause. 2. Use the MISCHILD command in the TQMIST tool to recreate the child process. 3. Perform a maintenance SWACT. ***Note:*** For details on using the TQMIST tool, refer to *Translations Guide*.
MIS IP interface cannot send a buffer ***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. 2. Use the PING command in the XIPVER tool to determine if the MIS server is responding. ***Note:*** Refer to Chapter 10: 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 74 on page 264 for details)	1. Use the PING command in the XIPVER tool to determine if the MIS server is responding. 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 ***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 74 on page 264 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 74 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 74 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
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 11: “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 12: “TOPS-IP OMs.”

Chapter 10: 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 7: "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 128 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 129 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 75 lists each parameter command and the page where its description begins.

Table 75 XIPVER parameter commands

Command	Purpose	Page
DIP	Sets the destination IP address parameter.	272
DP	Sets the destination application port number parameter.	272
MESSAGE	Sets the outgoing data message.	273
PACKETSIZE	Sets the size of packet for the PING command.	274
PINGTIMEOUT	Sets the timeout parameter for the PING command.	275
RR	Sets the record route option.	275
TIMEOUT	Sets the timeout parameter for the XIPVER commands (except CONNECT and PING, which is set using PINGTIMEOUT).	276
TTLIVE	Sets the time-to-live parameter.	277

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 76 lists each connection command and the page where its description begins.

Table 76 XIPVER connection commands

Command	Purpose	Page
CLOSE	Closes all the sockets, or the specified sockets, associated with the XIPVER tool session.	278
COMIDBIND	Binds the XIPVER tool session to a COMID datafilled in table IPCOMID.	280
COMIDUNBIND	Unbinds the COMID from the XIPVER tool session.	281
CONNECT	Establishes a TCP connection with a remote machine.	281
FORCECLOSE	Closes all the sockets, or the specified sockets, associated with a COMID.	282
PING	Sends an ICMP echo request message.	283
SEND	Sends a TCP or UDP message to a remote machine.	285
TCPSERVER	Sets up the tool as a TCP server.	286
UDPSOCKET	Sets up the tool as a UDP socket.	286

Tracing commands

The tracing commands allow the user to create tracesets and enable or disable message tracing. Table 77 lists each tracing command and the page where its description begins.

Table 77 XIPVER tracing commands

Command	Purpose	Page
TRACESET	Sets the traceset options.	287
TRACE	Enables or disables message tracing.	289

Query commands

The query commands allow the user to query the IP-XPM and the COMID. Table 78 lists each query command and the page where its description begins.

Table 78 XIPVER query commands

Command	Purpose	Page
GETPMINFO	Queries an Ethernet-based SX05DA XPM.	291
QUERYCOMID	Displays information about a COMID datafilled in table IPCOMID.	292

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 79 lists each miscellaneous command and the page where its description begins.

Table 79 XIPVER miscellaneous commands

Command	Purpose	Page
HELP	Displays available commands.	294
Q <command>	Displays detailed information on a specific command.	296
QUIT	Exits the XIPVER tool.	296
RESET	Resets the XIPVER tool parameters.	297
SHOW	Shows the current value of the XIPVER parameters.	298
SHOWUSERS	Shows the current users of the XIPVER tool	298

Using the parameter commands

The parameter commands (listed on page 269) 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 80 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 130 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 81 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 131 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 82 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 132 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 83 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 133 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 84 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 134 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 143 on page 284.)

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 85 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 135 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 86 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 136 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 87 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 137 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 270) 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 282) 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 88 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. ***Note 1:*** A value of -1 is recommended for users who want to close all resources associated with a COMID. ***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 138 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 281) 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 89 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 139 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 140 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 141 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 90 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 142 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 91 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 143 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 281)
- as a TCP server with the TCPSERVER command (page 286)

  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 286)

The SEND command has the following syntax:

`SEND` (used for TCP client or UDP socket)
`SEND <socket number>` (used for TCP server)

Table 92 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 144 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 145 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 146 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 270) 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 290 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 93 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 93 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. ***Note:*** This is the IP address of the remote node.
XPM <type> <number>	DTC, PDTC 0 to 255	Specifies message tracing for a particular XPM.
Direction	IN, OUT, BOTH	Specifies the direction of tracing: incoming, outgoing, or both. ***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 147 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 287), 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 94 TRACE parameters

Parameter	Range of values	Explanation
<activation>	ENABLE, DISABLE	Enables or disables tracesets. ***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 148 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 11: "TOPS-IP logs."

Figure 149 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 271) 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 95 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 150 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 96 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 151 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 271) 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 152 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 97 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 153 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 98 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 98 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 154 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 155 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 156 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 157 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 300)
- Setting up the tool parameters, including:
  - showing tool users (page 300)
  - changing tool parameters (page 300)
  - showing current tool parameters (page 301)
  - resetting tool parameters (page 301)
- Sending TCP and UDP messages, including:
  - binding and unbinding a COMID (page 301)
  - querying a COMID (page 302)
  - querying an XPM (page 302)
  - setting up a UDP socket (page 303)
  - setting up a TCP server (page 303)
  - setting up a TCP client (page 304)
  - sending messages as a UDP socket (page 304)
  - sending messages as a TCP server (page 305)
  - sending messages as a TCP client (page 306)
  - sending and receiving ping (ICMP echo) messages (page 307)
  - closing a UDP socket (page 308)
  - closing a TCP server (page 309)
  - closing a socket on a TCP server (page 310)
  - closing a listening socket on a TCP server (page 311)
  - closing a TCP client (page 312)
- Tracing messages, including:
  - setting up tracesets (page 313)
  - enabling and disabling tracesets (page 313)
  - displaying tracesets (page 313)
- Exiting an XIPVER session (page 314)

Entering an XIPVER session

Figure 158 Entering an XIPVER session

```
>XIPVER
USER# :0
For a list of available commands type: HELP<cr>.
```

Showing tool users

Figure 159 Showing tool users

```
>SHOWUSERS
<><><><><><><><><><><><><><><><><><><><>
USER#             : 0
USER NAME         : USER1
COMID             : NIL
STATE             : XIPVER_NIL
PROTOCOL          : TCP
<><><><><><><><><><><><><><><><><><><><>
```

Changing tool parameters

Figure 160 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 161 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 162 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 163 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 164 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 165 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 166 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 167 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 168 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 169 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 170 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 171 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 172 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 173 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 174 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 175 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 176 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 177 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 178 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 179 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 180 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 181 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 99 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 99 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 99 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 99 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: 1. The XPM is not yet in service. 2. Table XPMIPMAP and table XPMIPGWY (if used) may contain incorrect datafill. Also, if a DHCP server is used, its configuration may be incorrect. 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.) 2. Check datafill in tables XPMIPMAP and XPMIPGWY (if used), and possibly the configuration of the DHCP server. 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 99 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 99 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: 1. The XPM is not yet in service. 2. Table XPMIPMAP and table XPMIPGWY (if used) may contain incorrect datafill. Also, if a DHCP server is used, its configuration may be incorrect. 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.) 2. Check datafill in tables XPMIPMAP and XPMIPGWY (if used), and possibly the configuration of the DHCP server. 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. 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.) 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 99 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. 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.) 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. ***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 100 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 182 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 327).

Figure 182 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  QD715xx (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          SXFWAG04     (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 183, Figure 184, Figure 185, Figure 186, and Figure 187.

Figure 183 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 184 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 185 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 186 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 187 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 188 shows an example of datafill for DTC 4 after the conversion.

Figure 188 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  QD715xx (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          SXFWAG04    (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 9: “TOPS-IP maintenance activities.”

Refer to Figure 189 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 189 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 190 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 190 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 190 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 191).

Refer to the IPGWSTAT example shown again in Figure 191. 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 191 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 "Limiting the number of available dynamic trunks" on page 69 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 101 gives an explanation for the output.

Table 101 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 11: 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 102 lists each log and the page in this chapter where its description begins.

Table 102 TOPS-IP logs

Log name	Page number
XPM IP data communication (XIP) logs	
XIP600	334
XIP890	337
XIP891	339
XIP892	340
XIP893	340
External alarm (EXT) logs	
EXT106	341
EXT107	341
EXT108	342
QMS MIS (QMIS) logs	
QMIS102	343
QMIS103	343
TOPS logs	
TOPS106	344
TOPS112	344
TOPS133 ***Note:*** TOPS133 replaces TOPS105 on OC-IP calls.	345

Table 102 TOPS-IP logs

Log name	Page number
TOPS304	351
TOPS504	353
TOPS505	353
TOPS614	354

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.” With severe errors, the switch may not be able to display any message data. If it cannot be displayed, the log contains the text: “Unable to format message.”

The following figure shows an example log report.

Figure 192 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 103.

Table 103 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.
Unable to Send Message to Peripheral	The CMDC application was unable to send a message to the XPM. The most common reason is when an application (such as TOPS OC-IP) is in the process of attempting to send a message to an XPM and that XPM goes out of service.
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 103 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. ***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 12: "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 10: "TOPS-IP CI tools."

The following figure shows an example log report.

Figure 193 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 10: "TOPS-IP CI tools."

The following figure shows an example log report.

Figure 194 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 195 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 196 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 197 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 198 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 199 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 200 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 201 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 202 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 10: “TOPS-IP CI tools” for details on the commands.

Associated OM registers

None.

TOPS106

This log is generated for various problems with data links. The log report displays the voice link CLLI, OC office name, OC-IP data link number and a trouble code. The following figure shows an example log report.

Figure 203 Example log report for TOPS106

```
TOPS106 AUG31 08:16:32 8658 SYSB TOPS DATALINK TROUBLE
TOPSVCCT 0503CD
PROBLEMNO = 1241
OCOFC = DAHOST  OCIPDLNUM = NA
TRBLCODE = NO_DATALINK_MEMBERS_AVAILABLE
```

Note 1: Field support can use the value in PROBLEMNO for troubleshooting.

Note 2: TOPS106 can be generated in both a standalone and an OC configuration. If standalone, the value in the OCOFC field is "NA." If OC, the value in OCOFC is an office name datafilled in table OCOFC.

Action

For OC-IP data links, check the states at the OCDL level of the MAP. Refer to Chapter 9: "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 204 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 205 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: 219361
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 104.

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 104 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.

Table 104 TOPS133 field descriptions

Field	Value	Description
Trouble	MESSAGING_PROBLEM, OPR_ACK_WAIT_TIMEOUT, TABLE_OCGRP_DATA, VOICE_LINK_NOT_ AVAILABLE, VOICE_LINK_CONN_FAIL, EXT_BLOCK_UNAVAILABLE, PORTPERM_BLOCK_ UNAVAILABLE	Indicates the reason the log was generated. See "Action" on page 349 for more explanation.
Remote callid	0 to 4294967295, or "Not avail"	The call identifier of the call in the OC remote switch that generated the log. This call identifier is passed to the host switch during OC-IP call setup, so TOPS133 logs generated in the remote as well as the host should contain the remote callid. 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 that generated the log. 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. "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. ***Note:*** The voice link is a trunk member datafilled on the call's NT7X07 Gateway card.

Table 104 TOPS133 field descriptions

Field	Value	Description
Remote IPGW	Contains three components: 1. The IP Gateway (NT7X07 card) in use by the remote call. 2. The IP address of that IPGW. 3. The terminal identifier (TID) of the specific voice link in use by the remote call. 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. 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). 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 hosts’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).
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). The office number corresponds to the tuple in table OCOFC. For example, TOPSVCCT 160568 means office number 16 (hex) and circuit number 0568 (hex). ***Note:*** To determine the IP addresses and IP-XPMs involved, it is necessary to examine the DLNUM field.

Table 104 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. To determine the distant IP address, use the “To office” field combined with the “DLNUM” field as an index into table OCIPDL. The destination IP address and port are in the IPADDR and PORT fields. To determine the local IP-XPM in use on the call, examine the COMID field in table OCIPDL. Use this as an index into table IPCOMID. The local IP-XPM for this call is in the XPMNAME field. To determine the local IP-XPM’s IP address, use the XPMNAME as an index into table XPMIPMAP. The IP address is in the ACTADDR field.
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 105 lists user actions for each trouble code.

Table 105 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. 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. Field support can use the other information in the log to further analyze the problem.
OPR_ACK_WAIT_TIMEOUT	The host or remote was expecting a call control message from the other, and timed out waiting for it. Occasional appearance of this log can indicate race conditions, which may be ignored. More frequent appearance suggests probable network problems, which should be corrected.	Using IP network management tools, investigate the network to ensure that it is operating properly. 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.

Table 105 TOPS133 trouble code text descriptions and actions

Trouble code text	Description	Action
VOICE_LINK_CONN_FAIL	Indicates a voice setup failure, which could be due to loss of an OC data link message, loss of an ISUP/IGIP message, or an invalid message received on the voice link.	Field support can use information in TOPS133 to diagnose these failures. Also check the associated IPGW log reports. If the value in the "Problem number" field is 1241, the call received an unexpected REL message from the IP-XPM. Other problem numbers indicate lost messages (either voice call control or data call control). Field support can use this information to further analyze the problem.
EXT_BLOCK_UNAVAILABLE	An 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 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 store when needed. (Refer to the NUMPERMEXT tuple in table OFCAUT.) Consider increasing system memory.

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.

Associated OM registers

TOPS133 is associated with the following registers in OM group TOPSVC:

- VCFL
- MSGLOST
- OPRLOST

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 206 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 207 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 106 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 106 TOPS304 reason text descriptions and actions

Reason text	Description	Action
No failure	The data link is not in trouble.	No action is required.
CM child dead	The maintenance child process for the data link is dead and not scheduled for recovery.	1. Use the RECREATE command. 2. Delete and re-add datafill for the data link (table OCIPDL), and BSY and RTS it. 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. 2. Wait 30 seconds for automatic recovery. 3. BSY and RTS the data link.
Peripheral failure	1.The XPM is out of service. 2. A socket/COMID error occurred in the XPM. 3. The XPM is not responding. 4. Other XPM failure	1. Check the maintenance state of the XPM at the MAP, and recover the XPM if necessary. 2. Check all logs. 3. Wait 30 seconds for automatic recovery. 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. ***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. 2. Check the network. 3. Use the PING command in the XIPVER tool to determine if the far end is reachable. ***Note:*** Refer to Chapter 10: 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. 2. Use the QOCDL CNTRS command at the MAP. 3. Check the network.

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 208 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

This log is generated when an IP position transitions to another state. The log report displays the following information:

- position number
- reason text (manual command, system detected trouble, system corrected trouble, datafill change)
- from state and to state
- error code from position

Note: IP positions are not orderable and this log is never generated if an IP position is not datafilled.

The following figure shows an example log report.

Figure 209 Example log report for TOPS505

```
TOPS505 JUN23 18:12:05 5050 INFO TOPS IP DataLink Fault
Data Link:  TOPSPOS 501
Reason:     Manual Command
From:       OFFL
To:         MANB
Error code: 0
```

Action

None; this log is for information only.

Associated OM registers

None.

TOPS614

This log is generated when the switch receives a message from an IP address and port that does not match the far-end IP address and port datafilled for the data link. 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 210 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.

Chapter 12: 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 107 lists each OM group associated with TOPS-IP and the page in this chapter where its description begins.

Table 107 TOPS-IP OMs

OM group	Page number
QMSMIS	356
TOPSOC	358
TOPSVC	359
XIPCOMID	360
XIPDCOM	362
XIPMISC	364
XIPSVCS	366
XPMMSGOC	368

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 108 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 211 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 109 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.
OCMCCS	OC mechanized calling card service. This register is never pegged, as its related functionality (inwards MCCS) is no longer supported.
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 212 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     OCMCCS     OCQABN

    3     REMOTE1
                0          0          0
    4     REMOTE2
                0          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 110 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 213 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 111 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. ***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. ***Note:*** If the message is severely corrupted, this register may not be pegged.

The following figure shows an example for OM group XIPCOMID.

Figure 214 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 112 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 112 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. ***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. ***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 215 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 113 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 113 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 216 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 114 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. ***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 114 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. ***Note:*** If the message is severely corrupted, this register may not be pegged.

The following figure shows an example for OM group XIPSVCS.

Figure 217 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 used to predict messaging overload on XPMs, especially those supported by a BRISC front end. When messaging overload occurs, messages can be lost and calls can be adversely affected.

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 115 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 115 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 218 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 tuple that is most important to monitor on the IP-XPM is the NET tuple. This corresponds to the C-side DMSX links. These links are usually the first bottleneck in a heavily-loaded IP-XPM (with BRISC).

Although capacity testing was not complete at the time of publication, the following figure shows representative pegs for an IP-XPM that is approaching but has not reached the capacity of its DMSX links.

Note 1: Any number of pegs in the HQABV40 register indicates a messaging capacity problem. Preliminary test results suggest that any pegs in HQ30 are a warning of a possible problem, and that it is desirable for HQ10 to have more pegs than HQ20.

Note 2: These numbers are for a BRISC switch. Message characterization on XA-Core may be different.

Figure 219 MAP display example for OM group XPMMSGOC—NET tuple

```
              HQ00       HQ05       HQ10       HQ20
              HQ30       HQ40     HQABV40    AVGRATE
           MAXRATE   NUMREPTS

50          DTC      5 NET
              0         14         89         77
              0          0          0         19
             22          1
```

Associated OM groups

None.

Associated logs

None.

Appendixes

The following appendixes are included in *TOPS-IP User's Guide*:

Appendix A: "DHCP server guidelines" beginning on page 373.

Appendix B: "TOPS-IP support for SNMP" beginning on page 403.

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 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 information on upgrading the Gateway load (page 399) and changing the configuration of the Gateway (page 401).

DHCP server requirements

Two DHCP servers (NTNX55PA) 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 (at a minimum):

- Intel Pentium II 350 MHz processor
- 128 MB RAM
- Internal CD-ROM drive
- 10/100Base-T Network Interface Card
- 4GB hard drive
- 15” or higher monitor (NTNX55QA)
- Standard 101 keyboard with integrated touch pad (NTNX55RA)

DHCP server software

The following software is required:

- Microsoft Windows NT 4.0 Server operating system (A0806702)
- Nortel Networks NetID 1500 product (version 4.1.6) (DH0008027)

  Note: The NetID 1500 CD-ROM contains the NetID product suite, the Oracle runtime database, the NetID user documents, and the Adobe Acrobat Reader software used to read the documents.
- Java 1.1-compliant Web browser (for example, Netscape 4.5)

Gateway software

The 7X07AA Gateway cards require the TGWY0003 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.”

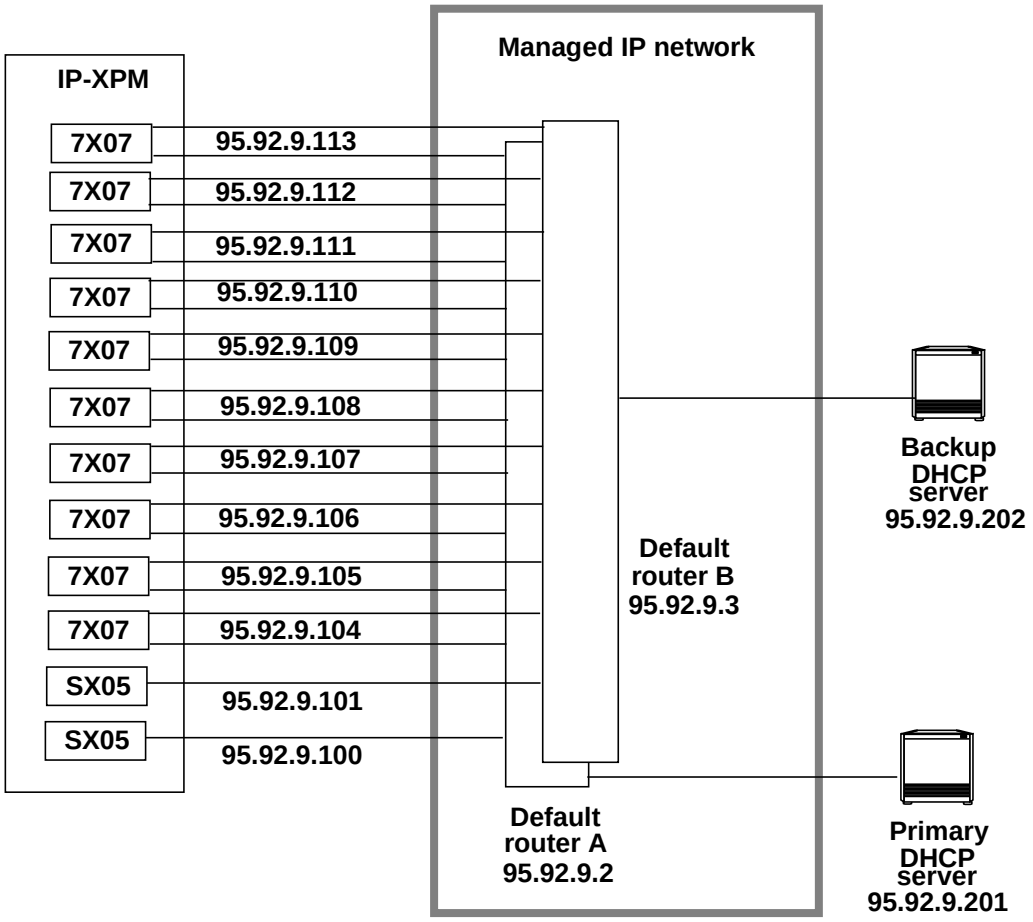
Preparation

Before installing the DHCP servers for TOPS-IP, it is recommended that you collect and diagram your site-specific IP addressing information. Figure 220 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 6: “TOPS-IP engineering guidelines” contains important information on how many 7X07 Gateway cards to provision in an IP-XPM.

Figure 220 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 116 Network provisioning information worksheet

System variable	Example value	Your value
Windows NT user ID	Administrator	
Windows NT password	topsip1	
Windows NT 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	
Physical router 1 IP address (see Note 1)	95.92.9.2	
Physical router 2 IP address (see Note 1)	95.92.9.3	
Virtual router 1 IP address (see Note 1)	95.92.9.1	
Virtual router 2 IP address (see Note 1)	95.92.9.1	
Gateway loadfile directory	C:\Gateway	
Gateway loadfile (boot file) name	topsipgw30ar	
Gateway load user access password	tazmanian	tazmanian (see Note 2)
Note 1: This IP address will be unique for each subnetwork. ***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 220 on page 375. 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 117 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 393.

Table 118 DHCP options for Gateway cards

Parameter	Example value	Your value
Application and Service Parameters:		
Boot File	topsipgw30ar	
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	
RFC1497:		
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. ***Note 2:*** The Gateway cards must use the virtual router IP address (or addresses).		

Table 119 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	
RFC1497:		
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 120 lists the procedures needed to install and configure NetID as a DHCP server for TOPS-IP.

Table 120 DHCP server procedures

Procedure	Name	Page
1	Install Windows NT 4.0 Server	379
2	Install the NetID database	384
3	Install the NetID product	385
4	Install the Web browser and connect to NetID	387
5	Install Adobe Acrobat Reader	389
6	Set up Gateway load user access	390
7	Configure NetID	393
8	Upgrade the Gateway load	399

Note 1: 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.

Note 2: Users will need a blank diskette to use for an Emergency Repair Disk in the Windows NT installation procedure.

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 NT 4.0 Server

Installing Windows NT 4.0 Server consists of the following broad steps:

- Change the First Boot Device to CD-ROM drive.
- Delete the existing partitions on the hard disk, and create a new partition on which to install Windows NT.
- Change back the First Boot Device setting to Hard Drive.
- Install the Windows NT 4.0 Server software.
- Install the Windows NT 4.0 Service Pack software.
- Install the Intel-based video adapter.

At the PC

1 Insert the CD with Windows NT 4.0 Server in the CD drive.

2 Change the First Boot Device to boot from CD-ROM using the following steps:

a Restart the PC, but do not wait for a complete restart. At the Motherboard splash screen (displayed briefly at startup), press F2 to enter the BIOS Setup Utility menu.

b Use the right arrow key to move to the Boot tab.

c Use the down arrow key to select the CD-ROM Drive.

d Use the + key to move the CD-ROM Drive up to First Boot Device.

e Press F10 to save the changes.

f Press Enter to exit the BIOS Setup Utility menu.

The PC restarts using the CD-ROM drive. The system starts the text portion of the Windows NT Server Setup. This may take a few minutes.

3 Delete the existing partition (or partitions) on the PC and install a fresh copy of Windows NT 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 NT licensing agreement and press F8 to continue.

c If no previous version of Windows NT exists on the PC, press Enter to continue. If a previous version does exist, press N (for New Version).

The system displays a list of hardware and software components.

d Press Enter to continue.

The system displays a list of all hard disks and partitions.

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 C to create a new partition.

i Enter the desired size of the partition (less than the maximum) in megabytes (MB) and press Enter.

j Press Enter to install Windows NT on the selected new (unformatted) partition.

k Select the NTFS file system type and press Enter.

The system formats the new partition. This may take a few minutes.

l Press Enter to accept the default directory of `\WINNT`.

m Press Enter to allow the system to examine the hard disk.

The system checks the hard disk and proceeds to copy the files needed for Windows NT Setup. This may take a few minutes.

n When prompted, remove the Windows NT 4.0 Server CD.

o Press Enter to restart the PC.

The PC restarts and converts to the NTFS file system. Wait for the PC to restart for a second time.

p When it restarts the second time, do not wait for a complete restart. At the Motherboard splash screen, press F2 to enter the BIOS Setup Utility menu.

4 Return the CD-ROM Drive to Third Boot Device using the following steps:

a Use the right arrow key to move to the Boot tab.

b Use the down arrow key to select the CD-ROM Drive.

c Use the - key to move the CD-ROM Drive down to Third Boot Device.

d Press F10 to save the changes.

e Press Enter to exit the BIOS Setup Utility menu.

The PC restarts using the hard drive. Wait for a complete restart.

5 Install Windows NT using the following steps:

a When prompted at the Windows NT installation window, reinsert the Windows NT 4.0 Server CD.

b Click the OK button to load files from the CD.

The system starts the graphical portion of Windows NT Sever Setup.

c Click the Next button to continue.

d Follow the directions in each of the installation windows by entering the requested data and clicking the Next button to proceed to the next window:

i Enter the name and organization.

ii Enter the number of concurrent sessions per server for the Licensing Mode.

iii Enter the unique computer name.

iv Select the correct domain controller server type.

Note: Select Primary Domain Controller when installing the primary DHCP server; select Backup Domain Controller when installing the backup DHCP server. Ensure that the servers are connected to the Ethernet LAN.

v Enter the administrator password.

Note: When installing the backup DHCP server, this password is not entered at this step.

vi Select Yes to create an Emergency Repair Disk. You will be prompted later to insert a disk on which to store the files.

Note: You may skip this step when installing the backup DHCP server.

vii Accept the default components.

The Windows NT Server Setup window opens to continue with the installation.

viii Click the Next button to begin setting up the network.

ix Select Wired to the Network.

x Click the Next button to install Microsoft Internet Information Server.

xi Insert the disk with the Intel-based network adapter.

xii Click the Select from list button.

xiii Click the Have Disk button.

xiv Select the adapter and click the OK button.

The system installs the network drivers.

xv Ensure that the TCP/IP Protocol is highlighted.

xvi Accept the Network Services default settings.

xvii Click the Next button to install the network components.

The system installs the network components.

xviii Remove the network adapter disk.

xix Click the No button regarding the use of DHCP. (Dynamic DHCP is not used for TOPS-IP.)

The system loads configuration information and opens the TCP/IP Properties window.

xx Enter the DHCP server IP address.

Note: Use the primary IP address when installing the primary DHCP server; use the backup IP address when installing the backup DHCP server.

xxi Enter the subnet mask address.

xxii Enter the default gateway (router) address.

xxiii While still in the TCP/IP Properties window, click the DNS tab and enter the DNS domain name for your company.

xxiv Click the OK button.

xxv Accept the default bindings for all services.

xxvi Click the Next button to start the network.

The system starts the network.

xxvii Enter the domain for the network managed by the primary domain controller.

Note: When installing the backup DHCP server, the administrator name and password are also required in this step.

xxviii Click the Finish button to finish configuring Windows NT.

The system configures the PC to run Windows NT.

xxix Click the OK button to accept the default options.

xxx Click the Yes button to create the `C:\WINNT\System32\inetsrv` directory.

xxxi Click the OK button for Publishing Directories.

xxxii Click the Yes button to create the directories.

The system loads the files.

xxxiii Click the OK button to accept the default ODBC drivers.

xxxiv Select the time zone and close the window.

xxxv Click the OK button to accept the default video adapter.

xxxvi Click the OK button to close the Display Properties window.

The system copies the files. This may take a few minutes.

Note: At this step, the system prompts you to label and insert an Emergency Repair Disk. The system copies the files to the disk. This may take a few minutes.

xxxvii Remove the Windows NT 4.0 Server CD when prompted.

xxxviii Click the Restart Computer button to restart the PC.

The PC restarts. Wait for a complete restart. The system displays the Windows NT login window.

e Log on by pressing Ctrl+Alt+Delete and entering the password.

The Windows NT desktop opens.

6 Install the Windows NT 4.0 Service Pack software using the following steps:

a Insert the CD with Windows NT 4.0 Service Pack software in the CD drive.

The Service Pack Installation window opens.

b Scroll through the instructions and select the link for Service Pack installation for Intel-based systems.

c Click the Open button to accept the Service Pack files.

d Click the Yes button to install.

The system installs the files and prompts you to restart. This may take a few minutes.

e Leave the Service Pack CD in the drive and click the OK button.

The system closes the window and restarts the PC.

f Remove the Service Pack CD.

g Log on by pressing Ctrl+Alt+Delete and entering the password.

The Windows NT desktop opens.

7 Install the Intel-based video adapter using the following steps:

a Insert the CD with the video adapter.

b Select **Start->Settings->Control Panel**.

c Double-click the Display icon.

The Display Properties window opens.

d Click the Settings tab.

e Click the Display Type button.

f Click the Change button.

g Click the Have Disk button and change to the D:\ drive.

h Browse the disk for the video adapter file by following this path: Video\Nt40\Atirage.

i Click the Open button.

j Click the OK button to copy the file from the disk.

k Select the ATI RAGE PRO TURBO AGP video adapter and click OK.

l Click the Yes button to install third party software.

m Click the OK button.

n Close the Display windows, leaving open the Control Panel window.

o Remove the video adapter CD.

p Click the Yes button to restart the PC.

The PC restarts.

q Log on by pressing Ctrl+Alt+Delete and entering the password.

r Click the OK button on the message confirming a new graphics driver.

The Display Properties window is already open to the Settings tab.

s Adjust the pixel settings to the desired resolution.

t Click the Test button and the OK button to start the test.

The system checks the bitmap settings.

u Click the Yes button.

v Click the Apply button.

w Click the OK button on the Display Properties window.

The system redraws the screen at the new resolution.

8 You have completed this procedure. Windows NT 4.0 Server is now installed.

Procedure 2 Install the NetID database

From the Windows NT desktop

1 Insert the CD with NetID 1500 software in the CD drive.

The NetID 1500 main menu opens.

2 Click the Launch NetID Setup button.

The NetID 1500 Setup window opens.

3 Click the Next button.

The Welcome to NetID Setup window opens.

4 Read the instructions on the window. When you finish, click the Next button.

The Setup Type window opens.

5 Install the NetID database using the following steps:

a Click the Setup NetID Database button.

The Oracle License Agreement window opens.

b Click the Yes button on the license agreement.

The NetID Oracle Runtime Database Setup Type window opens.

c Select Typical and click the Next button.

The NetID Oracle Runtime DB Setup Summary window opens.

d Review the settings. If the settings are incorrect, follow the instructions in the window. If the settings are correct, click the Next button.

Note: These settings are site-specific. If the Typical settings are not appropriate for your site, return to the previous step and select Custom. Then enter the values required by your site.

The Oracle Installation Settings window opens.

e The company name defaults to the one entered in the Windows NT installation. Leave the other fields set to the defaults. Click the OK button. NetID will create the database. The process takes about 10 minutes.

Your terminal displays a number of windows related to the Oracle database. When NetID finishes the process, the NetID Database verification box opens.

f Click OK.

The System Restart window opens.

g Ensure that Yes is selected and click the Finish button.

The NetID installation process finishes and the PC restarts.

6 Remove the NetID 1500 CD.

7 You have completed this procedure. The NetID database is installed.

Procedure 3 Install the NetID product

From the Windows NT desktop

1 Reinsert the CD with NetID 1500 software in the CD drive.

The NetID 1500 main menu opens.

2 Click the Launch NetID Setup button.

The NetID 1500 Setup window opens.

3 Click the Next button.

The Welcome to NetID Setup window opens.

4 Click the Next button.

The Setup Type window opens.

5 Install the NetID product using the following steps:

a Click the Setup NetID Products button.

The NetID License Agreement window opens.

b Read the license agreement. When you finish, click the Yes button.

The Organization Name window opens.

c The organization name defaults to the company name entered in the Windows NT installation. Click the Next button.

The NetID Product Setup Type window opens.

d Select Custom and click the Next button.

The NetID Product Directory window opens.

e Ensure that the destination directory is correct. Follow the instructions on the window if you want to change the destination directory. When the destination directory is correct, click the Next button.

The NetID Component & Subcomponent Selection window opens.

f Ensure that all NetID components are checked and click the Next button.

g Select Configure an existing client kit (Oracle) and click the Next button.

The Existing Database and Client Kit Type window opens.

h Select Oracle Server 8.0.5 and higher/Net 8 Client and click the Next button.

The Oracle Connection Parameters window opens.

i Use the default value for Connect ID. Click the Next button.

The Database UserID and password window opens.

j Use the defaults for User ID and Password. Click the Next button.

The NetID Application Server Setup window opens.

k For the application server, enter port number 8080 and use the defaults for Max Connections and Session Timeout. Click the Next button.

The NetID Server Manager Setup window opens.

l For the server manager, use the defaults for Port Number and Max Connections. Click the Next button.

The NetID Server Manager - DHCP Hosting Setup Window opens.

m Use the defaults for Port Number and Keep Alive Timer. Click the Next button.

The NetID Server Manager Connection Setup window opens.

n For the server manager, ensure that the IP Address is for the primary DHCP server. Use the default for Port Number. Click the Next button.

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 NetID Alternate Server Manager Connection Setup window opens.

o For the alternate server manager, use defaults for IP Address and Port Number. Click the Next button.

The NetID Polling Parameters Setup window opens.

p Use the defaults for Delta Log Poll Time and Expire Address Time. Click the Next button.

The NetID DHCP Server Setup window opens.

q Enter the DHCP IP address of the PC in the Server ID field, and use the default for ICMP Timeout Time. Click the Next button.

Note: Use the primary IP address when installing the primary DHCP server; use the backup IP address when installing the backup DHCP server.

The NetID Dynamic DNS Setup window opens.

r Select Disable Dynamic DNS Updates. Click the Next button.

The NetID DNS Server Setup window opens.

s The Fully Qualified Domain Name (FQDN) of the DNS server defaults to the name entered in the Windows NT installation. Click the Next button.

The NetID SNMP Trap Destination window opens.

t Enter the IP address of the SNMP network management node in the Trap Destination IP field. Enter “public” for the Trap Community. Click the Next button.

The NetID Services Startup Selection window opens.

u Leave all the selections checked. Click the Next button.

Note: If DNS is not used, uncheck NetID DNS Server.

The NetID Product Summary window opens.

v Ensure that the information is correct. If the information is not correct, follow the instructions on the window to change the information. When the information is correct, click the Next button.

NetID begins the installation process. Note any errors during the installation. The NetID Database Client Kit Configuration Verification window opens.

w When the installation process finishes, click the OK button.

The NetID SQL Utility window opens.

x Click the OK button.

The Performance Database Maintenance window opens.

y Click the Yes button to complete the NetID setup.

The Windows NT desktop opens.

z Ensure that Yes is selected and click the Finish button to restart the PC.

The PC restarts.

6 Remove the NetID 1500 CD.

7 You have completed this procedure. The NetID product is installed.

Procedure 4 Install the Web browser and connect to NetID

Note: This procedure lists the steps to install and configure the Netscape 4.5 Web browser, although any Java 1.1-compliant Web browser may be used with the NetID Management Console. If not installing Netscape, follow the steps provided with your selected browser software. Be sure that your browser can connect to NetID (see Step 19).

From the Windows NT desktop

1 Insert the CD with Netscape software in the CD drive.

2 Double-click the My Computer icon.

3 Double-click the CD drive.

4 Double-click the Netscape executable icon.

A series of dialog boxes opens.

5 Click the Yes or Next button in each dialog box that opens until the Setup Type window opens.

6 Ensure that the setup information is correct:

- Typical is the type of setup.
- The destination directory is correct. If necessary, change the destination drive from D to C.

7 Click the Next button.

A dialog box opens to ask if you want to create a directory.

8 Click the Yes button.

The Netscape Desktop Preference Options window opens.

9 Click the Next button.

The Select Program Folder window opens.

10 Click the Next button.

The Start Copying Files window opens.

11 Click the Install button.

The system loads the Netscape files.

12 Click the Yes button to read the README file and close the window when finished.

Setup is complete.

13 Click the OK button.

14 Ensure that Yes is selected and click the OK button to restart the PC.

The PC restarts.

15 Remove the Netscape CD.

16 Log on by pressing Ctrl+Alt+Delete and entering the password.

The Windows NT desktop opens.

17 Click the cancel button on the message regarding the drive.

18 Configure Netscape using the following steps:

a Open a browser window by double-clicking on the Netscape icon on the desktop.

The Creating a New Profile window opens.

b Click the Next button.

c Enter a name in the Full Name field and click the Next button.

d Enter a profile name and accept the default directory.

The Outgoing Mail server window opens.

e Click the Finish button.

f Click the OK button regarding the home page.

19 Verify that the browser can connect to NetID.

a In the URL field of the browser window, enter the physical IP address and port of the DHCP server.

The browser displays the NetID window and login window. Do not login yet.

Note: You can set the DHCP server IP address as the home page. In Netscape, use **Edit->Preferences->Navigator** to set the home page.

20 Click the Cancel button in the NetID login window.

21 Close the browser window.

22 You have completed this procedure. NetID is now operating as a DHCP server for TOPS-IP.

Procedure 5 Install Adobe Acrobat Reader

From the Windows NT desktop

1 Insert the CD with NetID1500 software in the CD drive.

The NetID 1500 main menu opens.

2 Click the Launch NetID Setup button.

The NetID 1500 Setup window opens.

3 Click the Next button.

The Welcome to NetID Setup window opens.

4 Click the Next button.

The Setup Type window opens.

5 Install Adobe Acrobat Reader using the following steps:

a Click the Setup Adobe Acrobat Reader button and click the Next button.

b Click the Yes button to install in the default directory and click the Next button.

c Click the Yes button on the license agreement.

d Click the Next button to install the files.

e Click the Finish button.

f Close the README file.

g Click the OK button.

The Adobe Acrobat Reader software is installed. The Setup Type window opens.

6 To return to the Windows NT desktop, click the Cancel button in the Setup Type window and Click Yes to exit.

The NetID 1500 main menu opens.

7 Click the Exit button.

8 Remove the NetID 1500 CD.

9 You have completed this procedure.

Note: You can access the NetID documents for printing or reading online. Select **Start->Programs->NetID->NetID Documentation**.

Procedure 6 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.
- Enable the FTP (file transfer protocol) service used to load the Gateway.

From the Windows NT 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 the Next button to install the loadfile.

c Click the Next button to accept the default destination location.

d Click the Next button to accept the default program folder.

e Confirm the settings and click the Next button.

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, `topsipgw30ar`) and copy the file (**Edit->Copy**).

m Paste the file (**Edit->Paste**) in the `C:\Gateway` folder.

The loadfile is listed.

n Close all open windows on the desktop.

2 Add user access for the `C:\Gateway` directory using the following steps:

a Select **Start->Programs->Administrative Tools (Common)->User Manager for Domains**.

The User Manager window opens.

b From the pull-down menu, select **User->New User**.

The New User window opens.

c 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.
- 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.

d Click the Groups button.

i Add the following groups that will have access to the domain by double-clicking on the group name:

- Administrators
- Domain Guests
- Users

ii Click the OK button

e Click the Profile button. Enter `C:\Gateway` in the Home Directory Local Path and click the OK button.

f Click the Hours button. Allow all hours and click the OK button.

g Click the Logon To button. Enter the desired settings and click the OK button.

h Click the Account button. Enter the desired settings and click the OK button.

i Click the Dialin button. Enter the desired settings and click the OK button.

j Click the Add button and close the window.

The new Gateway user access is listed in the User Manager window.

k Close the User Manager window.

3 Enable the FTP service using the following steps:

a Select **Start->Programs->Microsoft Internet Server (Common)-> Internet Service Manager**.

The Microsoft Internet Service Manager window opens.

b Ensure that the state for FTP is Running. Double-click the computer name next to the FTP service.

The FTP Service Properties window opens with the Service tab selected.

c Ensure that Allow anonymous connections is *not* checked. (Click the Yes button if you receive an authentication message.)

d Click the Messages tab and leave all fields blank.

e Click the Directories tab. Add the new directory as the Home (default) directory using the following steps:

i Click the Add button.

ii Click the Browse button and select `C:\Gateway.`

iii Click the OK button.

iv Select Home Directory for the `C:\Gateway.`

v Ensure that Read and Write are both checked.

vi Click the OK button.

f Click the OK button to create the new home directory.

g Click the Logging tab. Enter the desired settings for the `C:\Gateway` directory, making sure of the following options:

- Enable Logging is checked.
- A new log file is opened daily.
- Logs are filed to the directory `C:\Gateway`.

h Click the Advanced tab. Enter the desired settings.

i Click the OK button and close the window.

4 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 375) and from the various provisioning worksheets beginning on page 375. These values are examples only.

Note: For complete information on using NetID, refer to the NetID documentation suite.

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 balanced across the DHCP servers. So, half of the Gateways should be set up to boot from the primary DHCP server, and the other half from the backup DHCP server. Refer to 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 7 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 NT 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 NETID. (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 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.

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 “Up.” 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:

a Expand the root object `Setup`.

b Select `DHCP Option Templates`.

c From the pull-down menu, select **Options->New DHCP Option Template**.

The New DHCP Template window opens at the Name tab.

d Enter a name for the Gateways template.

e Click the DHCP Options tab.

f Expand the `Standard` tree in the right pane.

g Add the following DHCP options to the Gateway template by selecting and double-clicking the option name:

- From the `Application and Service Parameters` tree:
  - `Boot File`
  - `MobileIP Home Agents`
- From the `NetID Managed` tree:
  - `DNS Domain Name`
  - `HostIP Address (BOOTP only)`
  - `Host name`
  - `Lease Time`
- From the `RFC1497 Options` tree:
  - `Routers`

h After the selected DHCP options appear in the left pane of the window, 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 118 on page 378 for examples of valid values used in the sample configuration.

i 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:

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.

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 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).

f Enter the MAC address of the Gateway card. (This is the numerically lower of the two MAC addresses printed on the card.)

g Click the DHCP Options tab.

h Click the Apply Template button.

i Select the Gateway template name defined in the previous step and click the OK button.

j Click the Protocol tab.

k Select the primary DHCP server from the pull-down list.

l Click the DHCP Client box.

m Click the BootP Client box and enter the IP address of the DHCP server that will boot the Gateway in the BootP Server field. Ensure that half the Gateway cards defined boot from the primary DHCP server and half from the backup DHCP server.

n 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.

o Double-click the Gateway 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 Gateway being defined.

p Repeat these substeps for each Gateway, ensuring that they are balanced across the DHCP servers for the BOOTP function.

9 Datafill the DHCP options template for the SX05 cards using the following steps:

a Expand the `Setup` tree.

b Select DHCP Option Templates.

c From the pull-down menu, select **Options->New DHCP Options Template**.

d Enter a name for the SX05 template.

e Click the DHCP Options tab.

f Expand the `Standard` tree.

g 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 `RFC1497 Options` tree:
  - `Routers`

h After the selected DHCP options appear in the left pane of the window, enter your site-specific values next to each option. These same values will be applied to each SX05 in Step 10. Refer to Figure 119 on page 378 for examples of valid values used in the sample configuration.

i 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:

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 Click the DHCP Options tab.

h Click the Apply Template button.

i Select the SX05 template name defined in the previous step and click the OK button.

j Click the Protocol tab.

k Select the primary DHCP server from the pull-down list.

l Click the DHCP Client box.

m 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.)

n 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.

o 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.

p Repeat these substeps for the other SX05 card.

11 You have completed this procedure.

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 8 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 NT 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 the Next button to begin the install process.

c Click the Next button to accept the default destination location.

d Click the Next button to accept the default program folder.

e Confirm the settings and click the Next button.

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, `topsipgw30as`.

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, `topsipgw30as`) 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 RTS step.

d Issue the RTS command. If RTS is not successful, refer to “Troubleshooting the Gateway” on page 231.

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 NT 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 Select `DHCP Option Templates`.

The currently defined DHCP option templates are shown in the right pane.

c Double-click the name of the template used for Gateways.

The Update DHCP Template window opens at the Name tab.

d Click the DHCP Options tab.

e In the left pane in the Boot File field, enter the new loadfile name.

f 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, especially SNMP reboot

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 429 in Appendix B: "TOPS-IP support for SNMP."

Note: By default, the Gateway Telnet password is the same as the Gateway user access password set in Procedure 6 on page 390. However, the Gateway stores and handles them as two separate passwords. The Gateway 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 user access password.

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

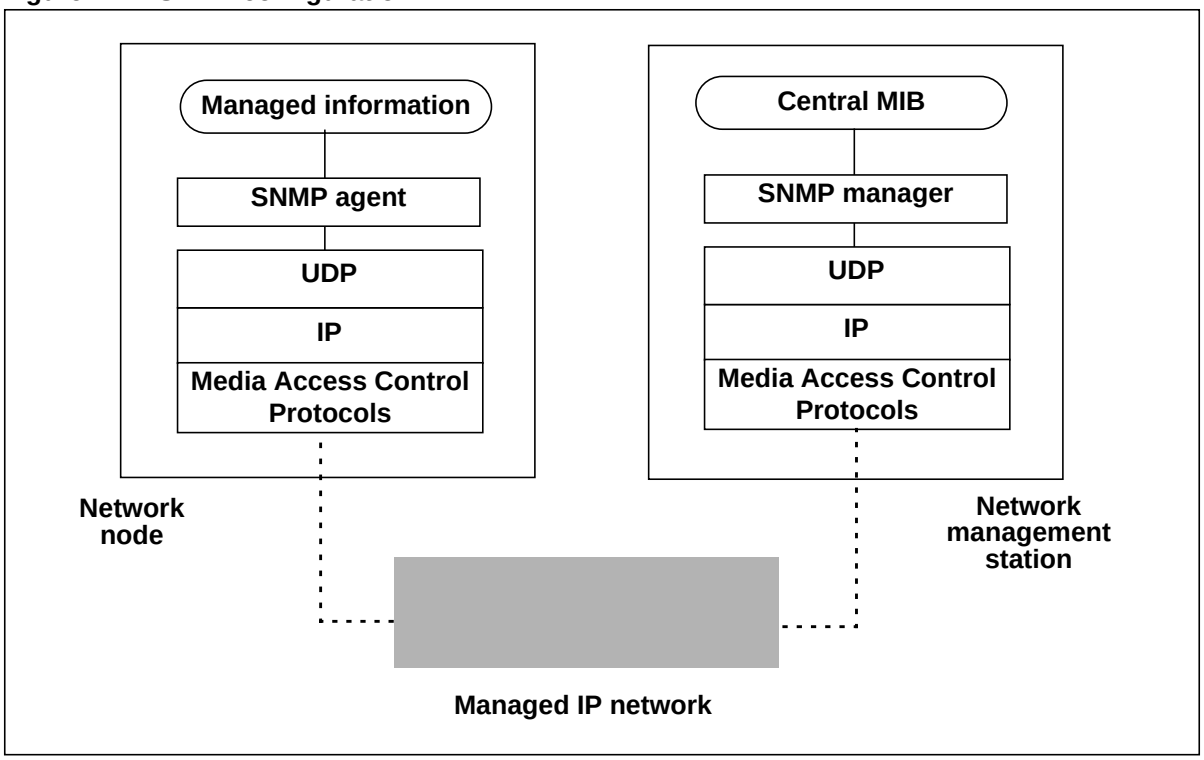
Using SNMP, a network administrator can do the following tasks from a centralized management station on the network:

- 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 221 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 221 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 121 lists the TOPS-IP Gateway private MIBs provided in the TGWY0003 release.

Table 121 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.	407
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.	410
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.	413
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.	426
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 xxiii.

NT7X07AAHW.MIB

Table 122 lists the OIDs in the NT7X07AAHW.MIB. This MIB provides the Gateway card name, firmware version, memory information, and processor state.

Table 122 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: 0–firmware image 0 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 122 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: 1–Interface Device is in reset 2–Interface Device is UP and active 3–Interface Device is UP and in backup mode for active device 4–Interface Device is DOWN 5–Interface Device is under Test

Table 122 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: 1–EEPROM content is valid 2–EEPROM content is invalid 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. ***Note 2:*** The norHwGwMemory group displays useful information on 7X07 memory usage and allocation.				

AUDIOCODE.MIB

Table 123 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 123.

Table 123 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: G711Alaw_64 = 0 G711Mulaw_64 = 1 G729 = 17 Invalid #s: 19, 20, 21, 23, 24 ***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. ***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: 0–Disabled 1–Enabled
.28.0.2.1.5.1.6 gwIPCxVChighPassFilter	Leaf	Read Write	Integer	High Pass Filter–enabled by default: 0–Disabled 1–Enabled
.28.0.2.1.5.1.7 gwIPCxVCpostFilter	Leaf	Read Write	Integer	Post Filter–enabled by default: 0–Disabled 1–Enabled
.28.0.2.1.5.1.8 gwIPCxVCsilenceCompression	Leaf	Read Write	Integer	Silence Compression–enabled by default: 0–Disabled 1–Enabled ***Note:*** This parameter is not used by the Gateway. It is overridden by CM datafill.

Table 123 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: 0–MuteDTMF 1–RelayDTMF 2–TransparentDTMF ***Note:*** This parameter is not used by the OC-IP Gateway application.
.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. ***Note:*** This parameter is not used by the OC-IP Gateway application.
.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. 0–default 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. 0–noAction 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. 0–noAction 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 124 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 124 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 124 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 124 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 124 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 124 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. 0–noAction 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. 0–noAction 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. 0–noAction 1–clear

Table 124 TOPSIPGW.MIB description

OID and name	Type	Access	Syntax	Description
.28.0.2.4.3.4 nnTgwSwLogThresh	Leaf	Read 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. ***Note:*** A threshold of 0 disables log notifications.
.28.0.2.4.3.5 nnTgwSwTrapThresh	Leaf	Read 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. ***Note:*** A threshold of 0 disables trap notifications.
.28.0.2.4.3.6 nnTgwDtmfInterDigitTime	Leaf	Read Write	Integer	The interdigit time for DTMF generated by the Gateway. Range is 10 to 250 ms. The default setting is 10. ***Note:*** This parameter is not used by the OC-IP Gateway application.
.28.0.2.4.3.7 nnTgwDtmfVolume	Leaf	Read 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. ***Note:*** This parameter is not used by the OC-IP Gateway application.
.28.0.2.4.3.8 nnTgwClearCAStats	Leaf	Read Write	Integer	Clear all call agent messaging stats on the Gateway. 0–noAction 1–set ***Note:*** This variable triggers an action, has no default, and will always read 0.
.28.0.2.4.3.9 nnTgwLogTable	Node	None	None	This table contains the current Gateway logs
.28.0.2.4.3.9.1 nnTgwLogTabEntry	Node	None	None	A table entry containing a single Gateway log
.28.0.2.4.3.9.1.1 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 nnTgwSysName	Leaf	Read	Display String	The system name of the Gateway issuing a log ***Note:*** This name is taken from the RFC1213 MIB's System group sysName variable.

Table 124 TOPSIPGW.MIB description

OID and name	Type	Access	Syntax	Description
.28.0.2.4.3.9.1.3 nnTgwLogType	Leaf	Read	Integer	The type of log: 0–swerr 1–info 2–note
.28.0.2.4.3.9.1.4 nnTgwLogTimeStamp	Leaf	Read	Display String	The timestamp of the log
.28.0.2.4.3.9.1.5 nnTgwTask	Leaf	Read	Display String	The name of the task producing the log
.28.0.2.4.3.9.1.6 nnTgwLogText	Leaf	Read	Display String	A text description of this log
.28.0.2.4.3.9.1.7 nnTgwLogTraceback	Leaf	Read	Display String	The function traceback for this log
.28.0.2.4.3.10 nnTgwExcTable	Node	None	None	This table contains the current Gateway exceptions (traps)
.28.0.2.4.3.10.1 nnTgwExcTabEntry	Node	None	None	A table entry containing a single Gateway trap
.28.0.2.4.3.10.1.1 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 nnTgwExcSysName	Leaf	Read	Display String	The system name of the Gateway issuing a trap ***Note:*** This name is taken from the RFC1213 MIB's System group sysName variable.
.28.0.2.4.3.10.1.3 nnTgwExcTimeStamp	Leaf	Read	Display String	The timestamp of the trap
.28.0.2.4.3.10.1.4 nnTgwExcTask	Leaf	Read	Display String	The name of the task producing the trap
.28.0.2.4.3.10.1.5 nnTgwExcVecNum	Leaf	Read	Integer 32	The exception vector number of the trap
.28.0.2.4.3.10.1.6 nnTgwExcPC	Leaf	Read	Display String	The Program Counter of the task producing the trap
.28.0.2.4.3.10.1.7 nnTgwExcMSR	Leaf	Read	Display String	The Machine State Register of the task producing the trap
.28.0.2.4.3.10.1.8 nnTgwExcCR	Leaf	Read	Display String	The Condition Register of the task producing the trap
.28.0.2.4.3.10.1.9 nnTgwExcTraceback	Leaf	Read	Display String	The function traceback for this trap
.28.0.2.4.3.11 nnTgwMtcInfo	Node	None	None	The Maintenance Info group

Table 124 TOPSIPGW.MIB description

OID and name	Type	Access	Syntax	Description
.28.0.2.4.3.11.1 nnTgwStatus	Leaf	Read	Display String	The sparing status of the Gateway (Primary, Spare, Nil) ***Note:*** Gateway sparing is not supported, so Primary is the only sparing status reported by the Gateway.
.28.0.2.4.3.11.2 nnTgwState	Leaf	Read	Display String	The current maintenance state of the Gateway. The possible states are: Reset Booting ROM Critical Fail 1 ROM Critical Fail 2 ROM Critical Fail 3 Offline Busy In-Service Reserved Unknown
.28.0.2.4.3.11.3 nnTgwLogNodeNum	Leaf	Read	Integer 32	The logical node number of the Gateway
.28.0.2.4.3.11.4 nnTgwPhysNodeNum	Leaf	Read	Integer 32	The physical node number of the Gateway
.28.0.2.4.3.11.5 nnTgwVariant	Leaf	Read	Integer 32	The type of Gateway (Toll Bypass, Centrex IP, TOPS)
.28.0.2.4.3.11.6 nnTgwAppVersion	Leaf	Read	Display String	The software version of the Gateway
.28.0.2.4.3.11.7 nnTgwBSPVersion	Leaf	Read	Display String	The BSP software version of the Gateway
.28.0.2.4.3.11.8 nnTgwCurrentTime	Leaf	Read	Display String	The current time on the Gateway
.28.0.2.4.3.11.9 nnTgwCmBcsRelease	Leaf	Read	Integer 32	The CM BCS Release number
.28.0.2.4.3.11.10 nnTgwXpmBcsRelease	Leaf	Read	Integer 32	The XPM BCS Release number
.28.0.2.4.3.11.11 nnTgwHdlcLinkState	Leaf	Read	Display String	The state of the XPM-GW HDLC link
.28.0.2.4.3.11.12 nnTgwFpgaVersion	Leaf	Read	Display String	The version of the Gateway FPGA
.28.0.2.4.3.11.13 nnTgwBootRomVer0	Leaf	Read	Display String	The version of the Gateway BootRom 0
.28.0.2.4.3.11.14 nnTgwBootRomVer1	Leaf	Read	Display String	The version of the Gateway BootRom 1
.28.0.2.4.3.12 nnTgwDhcpInfo	Node	None	None	The DHCP Info group

Table 124 TOPSIPGW.MIB description

OID and name	Type	Access	Syntax	Description
.28.0.2.4.3.12.1 nnTgwBootFile	Leaf	Read	Display String	The name of this Gateway's boot file
.28.0.2.4.3.12.2 nnTgwDhcpClient	Leaf	Read	Display String	The DHCP client name of this Gateway
.28.0.2.4.3.12.3 nnTgwDnsDomain	Leaf	Read	Display String	The DNS domain name in which this Gateway resides
.28.0.2.4.3.12.4 nnTgwDhcpServerIpAddr	Leaf	Read	IP Address	The IP address of this Gateway's DHCP Server
.28.0.2.4.3.13 nnTgwHostInfo	Node	None	None	The Host Info group
.28.0.2.4.3.13.1 nnTgwVxTargetIpAddr	Leaf	Read	IP Address	The IP address of this TOPS-IP Gateway
.28.0.2.4.3.13.2 nnTgwLocalHostIpAddr	Leaf	Read	IP Address	The loopback IP address of the local host
.28.0.2.4.3.13.3 nnTgwBootHostIpAddr	Leaf	Read	IP Address	The IP address of the boot host for this TOPS-IP Gateway
.28.0.2.4.3.14 nnTgwNotifications	Node	None	None	SNMP trap definitions
.28.0.2.4.3.14.1 nnTgwNSysName	Leaf	Notification Element	Display String	The system name of the Gateway issuing a log ***Note:*** This name is taken from the RFC1213 MIB's System group sysName variable.
.28.0.2.4.3.14.2 nnTgwNLogType	Leaf	Notification Element	Integer	The type of log: 0–swerr 1–info 2–note
.28.0.2.4.3.14.3 nnTgwNTimeStamp	Leaf	Notification Element	Display String	The timestamp of the log
.28.0.2.4.3.14.4 nnTgwNTask	Leaf	Notification Element	Display String	The name of the task producing the log
.28.0.2.4.3.14.5 nnTgwNLogText	Leaf	Notification Element	Display String	A text description of this log
.28.0.2.4.3.14.6 nnTgwNTraceback	Leaf	Notification Element	Display String	The function traceback for this log
.28.0.2.4.3.14.7 nnTgwLogNotification	Node	Notification		A Gateway log notification
.28.0.2.4.3.14.8 nnTgwNExcVecNum	Leaf	Notification Element	Integer 32	The exception vector number of the trap
.28.0.2.4.3.14.9 nnTgwNExcPC	Leaf	Notification Element	Display String	The Program Counter of the task producing the trap
.28.0.2.4.3.14.10 nnTgwNExcMSR	Leaf	Notification Element	Display String	The Machine State Register of the task producing the trap

Table 124 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 124 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 125 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 125 Example QoS table

Cell index	**Average latency** Base=0 ms Width=25 ms	**High average latency** Base=0 ms Width=25 ms	**Average jitter** Base=0 ms Width=5 ms	**High average jitter** Base=0 ms Width=5 ms	**Percent packet loss** Base=0% 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 126 lists the OIDs in the TOPSQOS.MIB.

Table 126 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 126 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 126 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: 1–enabled 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 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

Gateway access through Telnet

The Gateway supports access through Telnet. The only reasons to access the Gateway through Telnet are:

- to change the default Gateway Telnet password (page 430)
- to configure the Gateway to recognize additional SNMP network managers (page 433)
- to change the SNMP security settings (page 434)

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 9: "TOPS-IP maintenance activities."

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 222 shows an example of the PMDEBUG level at the Gateway.

Figure 222 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 430.

Note 2: For details on the persistence of Gateway data, refer to "Summary of persistence of user-configured Gateway data" on page 437.

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 223 shows an example of the top-level PMDEBUG commands.

Figure 223 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 224 shows a portion of such a table.

Figure 224 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 224.

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 225.

Figure 225 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 226 shows an example of the PMDEBUG commands.

Figure 226 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 227 shows an example of the SNMP commands. The commands in bold are described after the figure.

Figure 227 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 228 shows an example of this command level.

Figure 228 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 disabled. The ability to disable an SNMP-requested reboot is provided, as well as the ability to collectively disable Set operations against all other write-accessible objects.

Both Set Enable options default to an enabled state (1), which allows all Set operations to be executed by the Gateway. 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 229 shows an example of the SNMP commands.

Figure 229 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 230 shows an example of this command level.

Figure 230 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: Enabled.
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 231 shows an example log report.

Figure 231 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.

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 127 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 127 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.

List of terms

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

BOOTP

Bootstrap Protocol

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

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.

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.

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.

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

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.

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.

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 measurements

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

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

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.

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 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.

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

Simple Network Management Protocol (SNMP)

An industry standard protocol used to manage and monitor network activity and performance.

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

TLI

Transport Layer Interface

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).

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.

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

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: TOPS15 and up
Document release: Preliminary 02.03
Date: September 2001
Printed in the United States of America

NORTEL NETWORKS™