Critical Release Notice

Publication number: 297-1001-591
Publication release: Standard 04.04

The content of this customer NTP supports the SN06 (DMS) and ISN06 (TDM) software releases.

Bookmarks used in this NTP highlight the changes between the baseline NTP and the current release. The bookmarks provided are color-coded to identify release-specific content changes. NTP volumes that do not contain bookmarks indicate that the baseline NTP remains unchanged and is valid for the current release.

Bookmark Color Legend

Black: Applies to new or modified content for the baseline NTP that is valid through the current release.

Red: Applies to new or modified content for NA017/ISN04 (TDM) that is valid through the current release.

Blue: Applies to new or modified content for NA018 (SN05 DMS)/ISN05 (TDM) that is valid through the current release.

Green: Applies to new or modified content for SN06 (DMS)/ISN06 (TDM) that is valid through the current release.

Attention!
Adobe® Acrobat® Reader™ 5.0 is required to view bookmarks in color.

Publication History

March 2004

Standard release 04.04 for software release SN06 (DMS) and ISN06 (TDM).

Change of phone number from 1-800-684-2273 to 1-877-662-5669, Option 4 + 1.

Card NT9X30AB is Manufacture Discontinued and is replaced by new card NT9X30AC.

297-1001-591

DMS-100 Family

Networks

Maintenance Guide

BASE10 Standard 04.03 March 1999

northern telecom

DMS-100 Family

Networks

Maintenance Guide

Publication number: 297-1001-591
Product release: BASE10
Document release: Standard 04.03
Date: March 1999

Publication history

March 1999

BASE10 Standard 04.03

- Editorial changes

December 1998

BASE10 Standard 04.02

- Removed references to Input/Output devices from Table 2–1.
- Corrected titles of references in Table 2–1.

August 1998

BASE10 Standard 04.01

Added C-side extended messaging information to Chapter 1

February 1998

BASE07 Standard 03.06

Revised ENET MAP display example in Figure 6-10.

December 1997

BASE07 Standard 03.05

Chapter 8 revised to address PRSs

August 1997

BASE07 Standard 3.04

Editing changes

November 1996

BASE07 Standard 3.03

- Editing changes

September 1996

BASE07 Standard 3.02

- Changed command ABTRK to ABTK (chapter 6)
- Added MAPCI;MTC;NET commands CPU and MEMORY (chapter 6)

August 1996

BASE07 Standard 3.01

- Revisions associated with PRS resolutions
- Revisions associated with ACTID AR1926

May 1995

BASE05 Standard 01.02 Revised outreferences for agreement with current NTP numbers and titles.

March 1993

BCS35 Standard 01.01 First release of this document

Contents

About this document

This document is a maintenance guide for maintenance employees that have a basic knowledge of the Digital Multiplex System (DMS). This document is not for operating company personnel in need of exact, step-by-step procedures during the performance of maintenance tasks. This document describes the operation, format, and functions of the double shelf network equipment (DSNE) frame and the Enhanced Network (ENET). This document includes commands and displays for the DSNE and ENET.

When to use this document

This document helps maintenance employees locate and clear faults in the computing module (CM) for the DMS SuperNode and the DMS SuperNode SE switches.

How to check the version and issue of this document

Numbers (for example, 01.01) indicate the version and issue of the document.

The first two digits indicate the version. When an update of the document occurs to support a new software release, the version number increases. For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases when the document is revised and released again in the same software cycle. For example, the second release of a document in the same software release cycle is 01.02.

This document applies to all DMS-100 Family offices. More than one version of this document can be present. Check the release information in *Product Documentation Directory,* 297-8991-001 to determine if you have the latest version of this document. Check the release information to determine the arrangement of documentation for your product.

References in this document

The following documents are referred to in this document:

- *Alarm and Performance Monitoring Procedures*
- *Card Replacement Procedures*
- *Operational Measurements Reference Manual*
- *DMS-100 Family Commands Reference Manual*, 297-1001-822
- *Log Report Reference Manual*

What precautionary messages mean

The types of precautionary messages used in Northern Telecom documents include:

- attention boxes
- danger messages
- warning messages
- caution messages

An attention box identifies necessary information for the correct performance of a procedure or task. An attention box also identifies the correct interpretation of information or data. Danger, warning, and caution messages indicate possible risks.

The following are examples of the precautionary messages:

ATTENTION Information needed to perform a task

ATTENTION

If you do not deprovision the inactive DS-3 ports before you install a DS-1/VT Mapper, you will affect the DS-1 traffic. DS-1 traffic will not travel through the DS-1/VT Mapper.

DANGER Possibility of personal injury

DANGER

Risk of electrocution

Do not open the front panel of the inverter unless you removed fuses F1, F2, and F3. The inverter contains high-voltage lines. The high-voltage lines are active until you remove the fuses. You risk electrocution while the high-voltage lines are active.

DANGER

Risk of electrocution

Do not open the front panel of the inverter unless you removed fuses F1, F2, and F3. The inverter contains high-voltage lines. The high-voltage lines are active until you remove the fuses. You risk electrocution while the high-voltage lines are active.

WARNING Possibility of equipment damage

WARNING

Damage to the backplane connector pins

To avoid bending the backplane connector pins, align the card before you seat the card. Use light thumb pressure to align the card with the connectors. Use the levers on the card to seat the card into the connectors.

WARNING

Damage to the backplane connector pins

To avoid bending the backplane connector pins, align the card before you seat the card. Use light thumb pressure to align the card with the connectors. Use the levers on the card to seat the card into the connectors.

CAUTION Possibility of service interruption or degradation

CAUTION
Possible loss of service
Make sure that you remove the card from the inactive unit of the peripheral module before you continue. If you remove a card from the active unit, loss of subscriber service occurs.

CAUTION
Possible loss of service
Make sure that you remove the card from the inactive unit of the peripheral module before you continue. If you remove a card from the active unit, loss of subscriber service occurs.

How commands, parameters, and responses are represented

Commands, parameters, and responses in this document conform to the following standards.

Input prompt (>)

An input prompt (>) indicates that the following information is a command:

```
>BSY
```

Commands and fixed parameters

Commands and fixed parameters that you enter at a MAP terminal appears in uppercase letters:

```
>BSY CTRL
```

Variables

Variables appear in lowercase letters:

```
>BSY  CTRL  ctrl_no
```

You must enter the letters or numbers that the variable represents. A list that follows the command string explains each variable.

Responses

Responses correspond to the MAP display. Responses appear in a different type:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed.
```

The following sample from a procedure shows the command syntax used in this document:

1 To manually busy the CTRL on the inactive plane, type

>BSY CTRL ctrl_no
and press the Enter key.

where

ctrl_no is the number of the CTRL (0 or 1)

Example of a MAP response:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed.
```

Maintenance overview

This chapter introduces the double shelf network equipment (DSNE) frame and the enhanced network (ENET), two components of the Digital Multiplex System (DMS) SuperNode series. This chapter has the following sections:

- Operating description
- Fault conditions
- Automatic maintenance
- Quick reference to manual maintenance

The Operating description section includes information on cards, voice and data flows, and intermodule communications for peripheral modules (PM).

The Fault conditions section provides descriptions of the type of errors that can result from design of the product.

The Automatic maintenance section shows how audits and system actions attempt to locate and correct fault conditions. This section also shows how maintenance audits and system actions attempt to correct the fault so that manual intervention is not required.

The Quick reference to manual maintenance section indicates when you must perform manual maintenance activities.

Operating description

The Operating description section contains information on the DSNE and ENET.

Double shelf network equipment

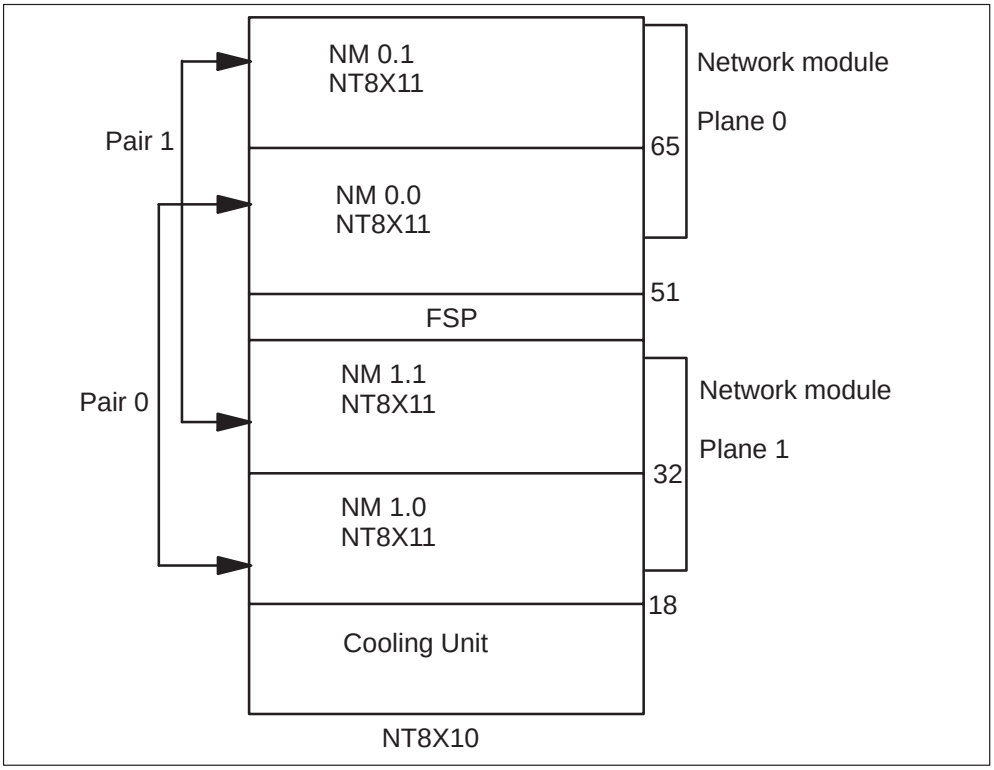
Another name for the DSNE (NTX8X11AD) is the junctored network (JNET). The DSNE is a hardware replacement for the network frame (NTX0X48AJ). The DSNE also replaces the network combined (NETC) frame (NTX5X13AA). The peripheral, serial junctor, and central message controller (CMC) interfaces are electrically identical to the earlier network modules. The DSNE is based on an improved switching design. The name for this improved design is *two way commuted-two way matrix switching*.

The DNSE provides a completely non-blocking network. The DSNE does not change the network capacity. The DMS-100 switch network configuration remains at 32 network module (NM) pairs maximum. Each network module pair has 64 speech link ports. The maximum applies to the NT0X48AJ and NT5X13AA networks.

The junctored network has two purposes. The network provides the path for speech or pulse code modulation (PCM) to travel between two PMs. The network also provides the path for message signals between PMs and the central control complex (CCC). Pairs of NMs form the network. The NMs provide the path for both information and message signals. An NM consists of cards and wires that route two-way speech signals between PMs, or two-way message signals between the CCC and PMs. Each NM occupies one shelf on the DSNE. The network has two duplicated halves: plane 0 (shelves 51 and 65), and plane 1 (shelves 18 and 32).

These planes duplicate information and message switching to provide call processing reliability. Each NM in plane 0 has a corresponding mate in plane 1, for reliability. Because each NM duplicates the NM in the opposite plane, the NETC contains a minimum of two NMs. One NM is in plane 0 and the other (redundant) NM is in plane 1. The two corresponding NMs are called a network module pair or NT8X11 network. You can identify an NM by the plane number, followed by the network number. Network module 0.1 is in plane 0. Network module 1.1 is in plane 1. These two NMs form network 1, identified by the last digit in the NM number. A single NT8X11AA network occupies two shelves in the DSNE. The DSNE can hold two NT8X11AA networks. Figure 1-1 shows the DSNE frame design.

Figure 1-1
DSNE frame design



Speech and message links

When speech comes from the PM across the digital signal (DS30) links, the speech travels through planes 0 and 1 of an NM pair. Message links connect both planes in an NM pair to the CCC. The CC sends duplicate messages to the PM across both of these planes or paths. Each PM sends messages to and from the CCC through the network. Through the control processor, the network inserts or extracts messages to and from the PM. DS30 links carry information from the PM to the network. In the network, crosspoints connect the incoming and outgoing paths through time switch. The time switch assigns speech slots from one channel to another channel. The network message controller (NMC) controls crosspoints speech connections between PMs.

Reliability

Duplicated planes allow the PM and the CCC to use an NM pair as a signaling path when one NM is out of service (OOS). The network can operate when one plane is OOS. If both NMs are OOS, the PM and the CCC can not send speech and message signals through the network. The transmitting PM sends speech through both planes. The receiving PM selects only one plane to process the call. If the PM uses a plane that has

faults, the PM automatically switches to the duplicated plane. The duplicated plane receives the same messages. The duplicated plane does not process these messages.

Sides

Each NM has an A-side (receive) and a B-side (transmit). To establish a two-way conversation, the A-side must connect with the B-side of the network. Speech goes from a PM through speech links to the A-side of an NM. The A-side switches the speech to the B-side. The B-side receives input from the A-side of the same or different NM. The B-side transmits these signals to the PM. The B-side connects to the speech links that carry speech away from the network to the PM.

Crosspoints

Crosspoints connect the incoming and outgoing paths of a time switch so that signals can switch. The crosspoint card contains the non-blocking time switch. This device switches any input channel to any output channel. Time switches reassigns voice samples to available input and output channel times.

Junctors

Junctors provide communication connections inside the network. Junctors can connect the A-side to the B-side of a different NM of the same plane, or to the same NM. A junctor connects the crosspoints in the A-side to the crosspoints in the B-side. Junctors are external (serial) or internal (parallel or serial). External junctors connect the A-sides of the NM to the B-sides of another NM. Internal junctors connect the A-sides and B-sides of the same NM. Because 64 junctors connect 32 NM pairs, a minimum of two junctors connect each NM to itself or to all other NMs.

Double shelf network equipment cards

This section describes the cards that form the DSNE.

Several types of cards form the DSNE. The list of cards follows:

- serial port card (NT8X12AA)
- crosspoint card (NT8X13AA)
- network control processor (NT3X74BA)
- peripheral side (P-side) processor (NT3X75BA)
- clock card (NT3X76AB)
- test code card (NT8X14AA)

Serial port card

Each of four peripheral and four junctor port cards provide 16 bi-directional transformer coupled, serial 2.56 Mb DS30 interfaces.

These cards provide:

- peripheral and junctor interface
- serial to parallel conversion
- parallel to serial conversion
- test code insertion and removal

You can use one W72 formatter integrated circuit to implement the serial to parallel conversion. You can use another W72 formatter integrated circuit to implement the parallel to serial conversion.

Crosspoint card

The DSNE has four crosspoint cards. Two of the four crosspoint cards are for each direction of the switch. Two crosspoint cards provide a non-blocking 2048 channel time switch. The four circuit cards provide the function performed by eight circuit cards in the NT5X13AA network. Speech data enter the crosspoint card on four 10-bit wide parallel buses. Each parallel bus carries 512 channels. These buses are written into alternate data memories as controlled by input frame multiplexers. These multiplexers switch on odd and even frames.

Network control processor

The network control processor has two main functions. The network control processor provides message interface to the central control (CC). The network control processor also controls network operations. For example, the processor controls setting connection memories, test code insertion, and test code removal in response to CC messages.

As a message interface, the network control processor implements the DS30 message protocol used on the two CMC links. The DS30 message protocol examines received messages to determine if these messages are for a PM or the network. Messages for peripherals pass to the P-side processor for transmission using channel 0 of the correct port.

The network control processor acts on messages for the network. The network control processor has control buses to the crosspoint cards, test code card, clock card, and the P-side processor. To set up network connections, write data memory addresses into the connection memories of the correct crosspoint cards on both sides of the NM.

Peripheral side processor

The P-side processor is responsible for message transfer between the network and the network peripherals. On the P-side, the processor sits across four parallel speech buses on the A-side and B-side of the network. The parallel speech buses connect the crosspoint cards and the four serial port cards that serve the peripherals. The P-side processor can access all channel 0s that go to and come from the peripherals. The P-side processor uses the standard DS30 message protocol to send and receive peripheral messages over the channel 0s. The P-side processor can handle four message transactions at a time. The P-side processor can handle one speech transaction at a time on each bus.

The processor has access to a message buffer on the network control processor. This access is available on the network side of the P-side processor. Messages received from peripherals are deposited in this buffer. The control processor relays these messages to the CC. The P-side processor also scans this buffer for messages to send to the peripherals.

Clock card

The clock card provides the DS30 transmission interface of the network to the CC. The clock card also provides clock and frame signals to other circuit cards. The clock card provides two DS30 interfaces. The clock card provides one DS30 interface to CMC 0 and one DS30 interface to CMC 1. Control messages are sent and received over both ports. All 32 channels are in use because the two ports are used for messaging only. The transfer rate is 256 kbyte/s.

Test code card

The test code card inserts and removes test code data used to verify the continuity of a network path. Each NM requires one test code card.

Enhanced network

The basic DMS SuperNode system configuration consists of DMS SuperNode system components and DMS-100 Family equipment. Equipment is available for the following ENETs:

- 16K (SuperNode SE)
- 32K (SuperNode and SuperNode SE)
- 64K (SuperNode)
- 128K (SuperNode)

The following forms a basic DMS SuperNode system:

- DMS SuperNode components
  - — DMS-core component

  - — DMS-bus component
  - — DMS-link component
- DMS-100 Family equipment
  - — Input-output equipment
  - — PM
  - — NM
- ENET

The DMS SuperNode system can use DMS-100 Family NMs or the ENET to provide switch functions for the PMs.

The primary function of ENET is to provide connectivity from the DMS-bus component to the PMs, and from PM to PM. The ENET provides voice and data connections between PMs and message paths to the DMS-bus component. The DS512 fiber optic links connect the ENET and the SuperNode DMS-bus component. The connections between ENET and other peripherals can use DS30 copper links or DS512 fiber optic links. The ENET is available in a 128K two-cabinet configuration or a 64K single-cabinet configuration for reduced footprint. The ENET does not store and forward messages between the DMS switch CC and PMs as previous networks do. The ENET supports direct links between the message switch (MS) and PMs as nailed-up network connections. The ENET is only equipped in offices with an enhanced core. For example, ENET is equipped in a DMS SuperNode office.

The ENET provides the following features:

- non-blocking single-stage time switch
- nailed-up connections
- compatibility with A-rule and M-rule companding
- support of services that require bandwidths greater than 64 kbytes/s

The ENET is compatible with all DMS-100 Family PMs, including the fiber Series II PMs. You can convert series II PMs to connect to the ENET through DS512 fiber links. An example of a series II PM is a digital trunk controller (DTC). This conversion allows the connection of the maximum number of PMs to a single ENET shelf. The ENET uses the same cabinet hardware, power, electromagnetic interference, and cooling design as the DMS SuperNode system.

The ENET uses the standard DMS SuperNode cabinet. Each cabinet can hold a maximum of four ENET shelves, a frame supervisory panel (FSP), and a cooling unit.

Each ENET shelf contains the following:

- central processing unit (CPU)
- memory card
- clock and messaging card
- crosspoint cards
- transmission and interface cards
- four power converter cards

For reliability, two duplicated ENET planes are always configured. Each plane has two shelves in the single-cabinet configuration. In the two-cabinet configuration, each cabinet has one to four shelves with one plane for each cabinet. The single-cabinet ENET has a minimum of one shelf for each plane. The single-cabinet ENET can expand to two shelves for each plane. Each shelf can support one plane a maximum of 32K channels. The single-cabinet ENET can be configured for a minimum of 8K channels. The single-cabinet ENET supports 64K channels. The two-cabinet ENET can support 128K channels. Peripherals have access to both planes of the ENET, which operate in parallel and separately. Peripherals select the active plane based on each connection.

Figure 1-2 displays an ENET cabinet design (double configuration). Figure 1-3 shows the configuration of a DMS SuperNode system configured with the 128K two-cabinet ENET components.

Figure 1-2
ENET two–cabinet design

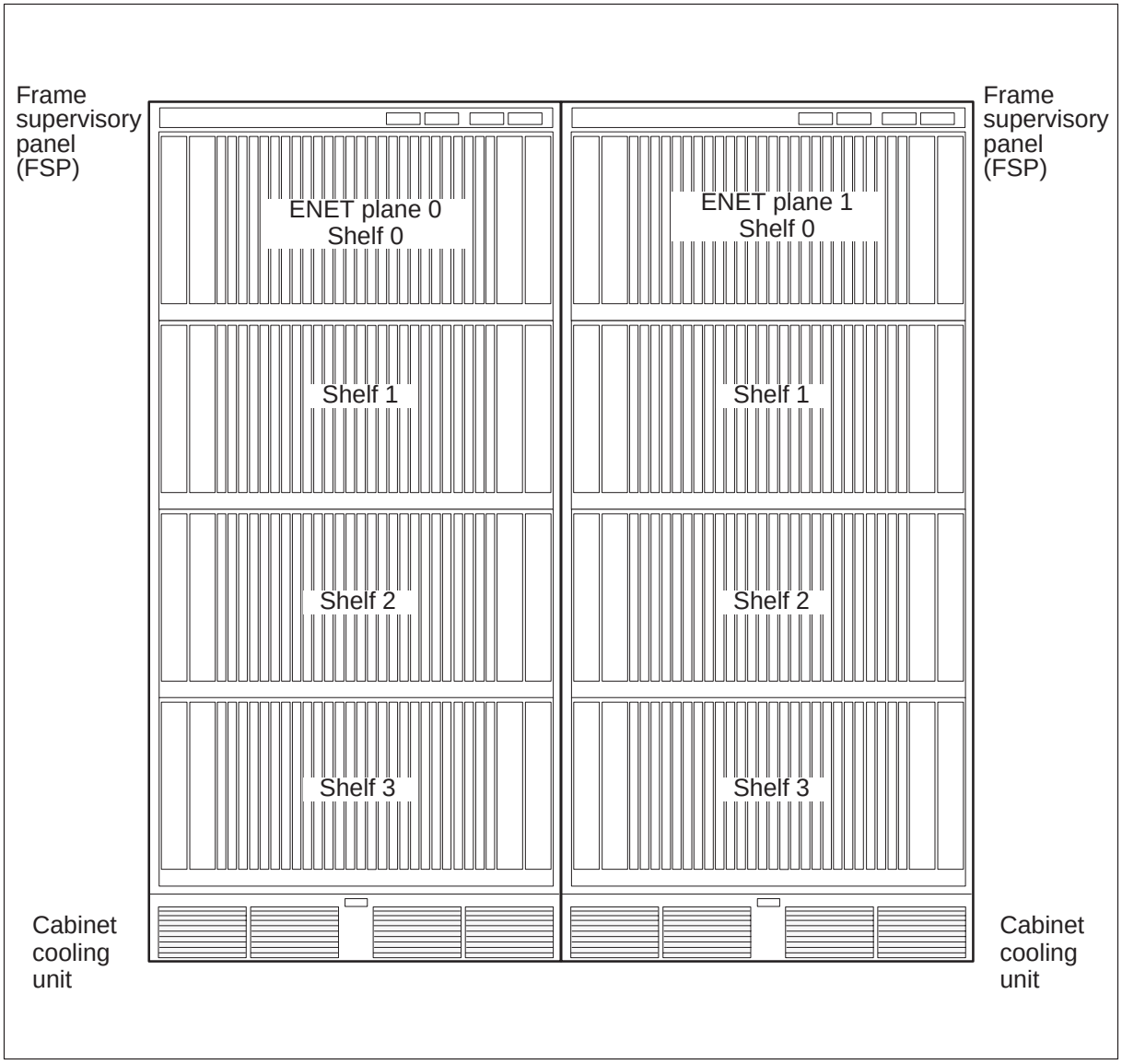
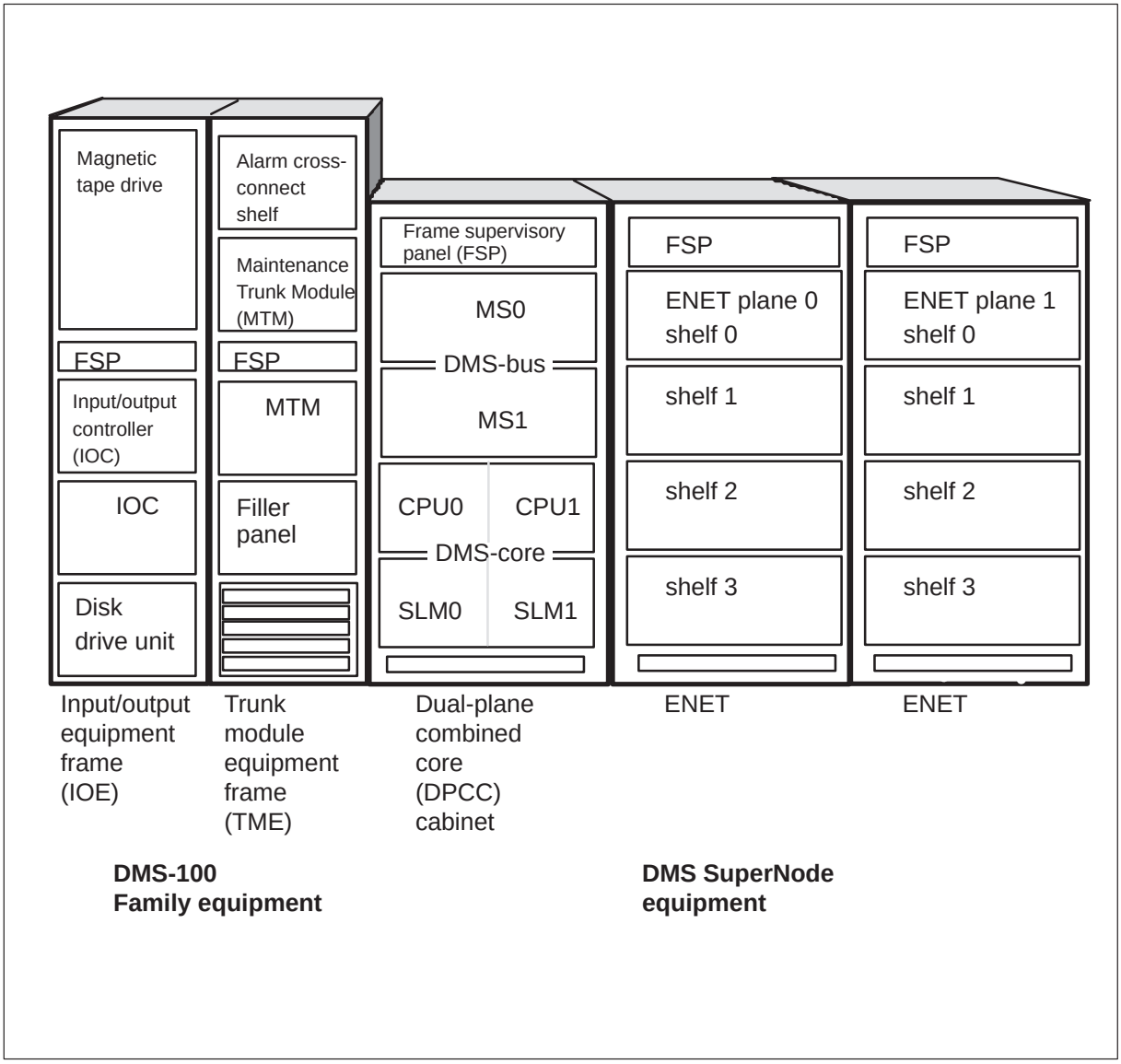


Figure 1-3
Example of a two-cabinet 128K ENET configuration



Enhanced network operation

The basic building block of the ENET is a double buffering, 16K by 16K time switch crosspoint card. All switch paths have a constant delay of 125 µs in all switched paths as a result of the double buffering.

Channels that enter through the peripheral interface paddleboard transport between shelves on vertical buses. The buses offer the channels to all crosspoint cards in that column and the mate column. The crosspoint card takes incoming channels or channels that are not switched. The card selects

the channels that will enter through peripheral links on that shelf. The crosspoint card places the channels on a horizontal bus for the shelf. From this horizontal bus, outgoing or switched channels transmit through the paddleboard to the peripherals.

Enhanced network systems

This section describes the operating systems that are in the ENET.

The following operating systems make up the ENET:

- processor and memory (NT9X13FA, NT9X13KA, NT9X26AA, NT9X26AB)
- clock and messaging (NT9X36BA)
- crosspoint matrix (NT9X35BA, NT9X35CA)
- crosspoint and interface (NT9X35FA, NT9X40BA, NT9X40BB, NT9X40DA, NT9X41BA, NT9X45BA)
- power converter (NT9X30AA, NT9X30AC, NT9X31AA, NT9X31AB)

Processor and memory

The processor and memory system consists of the CPU card (NT9X13) and the remote terminal interface (RTIF) paddle board (NT9X26). The system provides operation and diagnostic control for the shelf. The CPU card holds 4-Mbytes (NT9X13FA) or 16-Mbytes (NT9X13KA) of random access memory (RAM). The RAM contains operating software for the ENET. The CPU card holds 128 kbytes of read-only memory (ROM) firmware. The ROM firmware holds bootloading and initialization procedures.

Clock and messaging

The clock and messaging system consists of the clock and message card (NT9X36), and a quad DS512 fiber interface paddle board (NT9X40). The NT9X36 card provides input and output control, and provides the clock source for the shelf. The NT9X40 card provides two channelized fiber links to the DMS–bus component for messages. Shelf processor and PMs that connect to the shelf share the messaging on the links. The DMS-bus component and the shelf processor specify a link. One link provides the clock source for synchronization to the DMS-bus component. The DMS-bus component and the shelf processor specify this link.

Crosspoint

The crosspoint system consists of the NT9X35BA and NT9X35CA cards. These cards form the switching matrix. The horizontal bus connects the crosspoint cards to the other cards on the shelf. The vertical bus connects the crosspoint cards to the cards on other shelves.

A completely provisioned ENET plane has eight vertical buses and eight horizontal buses. One completely equipped plane of the ENET consists of four shelves. Each shelf contains 16 crosspoint cards. Each crosspoint card can switch a maximum of 2K of input data from the link interface paddle board. The capacity of the switching matrix for a completely configured ENET is four shelves by 16 crosspoints by 2K for each crosspoint = 128K.

The primary function of the crosspoint card is to transfer data between the eight vertical buses and the eight horizontal buses. These buses form the ENET switching matrix. The NT9X35BA and NT9X35CA crosspoint cards can switch 16K of input channels to 16K of output channels. Input data can come from a link interface paddle board, or any other card in the vertical bus. The switch data is output on the horizontal bus.

Switch complex vertical buses

Each vertical bus consists of two crosspoint cards in each shelf. The crosspoint cards align vertically in the ENET plane. These two cards in each shelf of a vertical bus are called mate cards.

A crosspoint card in the vertical bus performs the following functions:

- receives data from the link interface paddle board of the vertical bus
- receives data from other cards in the vertical bus, including the mate card of the vertical bus
- transmits data to other cards in the vertical bus, including the mate card
- switches data onto an horizontal bus

Switch complex horizontal buses

The two horizontal buses on a shelf are called the even and odd horizontal buses. To represent the ENET switching matrix in logic, the 16 crosspoint cards in an ENET shelf are numbered. The crosspoint cards are numbered 3 to 10 and 19 to 26. Cards with even numbers attach to the even horizontal bus for that plane. Cards with an odd number attach to the odd horizontal bus for that plane.

A crosspoint card in the horizontal bus performs the following functions:

- transmits data to other cards on the horizontal bus of the crosspoint card
- receives data from other cards on the horizontal bus of the crosspoint card
- transmits data to a PM through the link interface paddle board of the crosspoint card

Transmission and interface

The transmission and interface system consists of one or both of the following:

- DS512 fiber interface paddle boards (NT9X40)
- DS30 interface paddle boards (NT9X41)

The DS30 links connect PMs to the ENET through NT9X41 paddle boards. The DS512 links connect XMS-based peripheral modules (XPM) to the ENET through NT9X40 paddle boards. These paddle boards are the transmit and receive interfaces between the PMs and the crosspoint cards in the ENET. Series I PMs connect to the ENET through current copper links. Series II PMs connect to the ENET with DS512 fiber links. Each fiber link is the transmission equivalent of 16 DS30 copper links because a total of 512 channels are in each fibre link.

Power

Two NT9X30 +5V, 80A power converters and two NT9X31 –5V, 20A power converters provide the power. One of each type of converter is at each end of the shelf and provides power for one half of the shelf.

C-side extended messaging

Messaging channels contain the following:

- a channel from the XPM to the ENET
- a channel from the ENET to the MS

Without C-side extended messaging, the DMS system provides two channels between the XPM and the ENET plane. C-side extended messaging increases the messaging capacity of host XPMs. C-side extended messaging allows operating company personnel to provision an additional 0 to 12 message channels for each XPM unit. Operating company personnel accomplish this by provisioning the channel 0s not used on 12 of the 16 logical ports on a DS-512 fiber optic link. The additional channels use DMS–Y data link protocol instead of the standard DMS I/O protocol. This allows both the computing module (CM) and the XPM to send messages at the same time. The operating company personnel provisions the new extended messaging channels in table LTCINV.

Note that C-side extended messaging does not increase the number of message channels between the ENET plane and the MS. As the number of provisioned extended message channels increases, the number of supported XPMs decreases.

C-side extended messaging requires the following cards:

- NT6X40FC – This card is a variant of the NT6X40FB DS-512 interface card. The NT6X40FC routes 14 DS-0 channels between the DS-512 fiber optic link and two NT6X69QA messaging cards in the XPM.
- NT6X69QA – This card is a variant of the base NT6X69LB messaging card. The NT6X69QA contains a more powerful protocol processor circuit and the hardware resources to terminate 14 C-side message channels. The NT6X69QA also implements the downloadable tones feature found on the NT6X69LB card.

You can deploy the NT6X40FC and NT6X69QA in any XPM application that has one of the following processors:

- NTMX77AX
- NTAX74AA or NTAX74AB
- NTSX05AA

The NT6X69QA card is not backwards compatible with the NT6X45 series XPM processor cards.

You must meet the following minimum hardware requirements before you can enable C-side extended messaging capability for an XPM:

- The DMS-core must be a SuperNode CM, with an MS.
- The network must be an ENET
- To use a DS-512 fiber optic link between the target XPM and the ENET, the target XPM must be a fiber optic XPM (FXPM)
- The messaging card must be an NT6X69.

Product design and development restricts the PMs you can convert to fiber-optic host XPMs. You cannot upgrade the following PMs to provide C-side extended messaging capability:

- host-based XPMs that use DS-30 copper links to junctored networks (JNET) or ENET
- host-based common peripheral modules (CPM), for example, ESMA (enhanced subscriber carrier module–100 acess) or Global Peripheral Platform (GPP)
- any remote PM, for example, remote cluster controller (RCC) , remote cluster controller 2 (RCC2), or remote line concentrating module (RLCM)
- any Series 1 PM, for example, maintenance trunk module (MTM), digital carrier module (DCM), line module (LM), or office alarm unit (OAU)

- any Spectrum peripheral module (SPM)
- host-based XPMs that provide a host interface to extended distance switch remotes, for example, extended distance RLCM or extended remote switching center–SONET (RSC-S)

Even with C-side extended messaging deployed, two C-side DS-30 message channels that use DMS I/O link protocol remain active. These channels provide backward compatibility to the base XPM platform for maintenance and diagnostic functions.

You can deploy C-side extended messaging in all host XPM applications that meet the requirement described earlier. You can deploy C-side extended messaging only in host XPM applications that have call completion performance restricted by CM/XPM message channel throughput

Fault conditions

Fault conditions are the type of errors that can result from product design.

Double shelf network equipment

Hardware, CC software, PM software, or manual office activity can cause accuracy failures. Network modules also cause fault conditions.

Hardware induced accuracy failures

Hardware induced accuracy failures can result from hardware problems in one of the following areas:

- along the accuracy transmit or receive path
- in either of the two PMs involved in the call
- in the network or networks involved in the call

Three vintages of networks are present. The card codes involved in each network are different for an equivalent path. The most common network cards involved in accuracy failures are network to PM interface cards. Other diagnostics do not detect these cards.

Four PM types are present. These PM types interface directly to the network and can be involved in accuracy failures. These PMs are:

- trunk modules (TM)
- digital carrier modules (DCM)
- line modules (LM)
- line trunk controllers (LTC)

Channel supervision message trunk module cards

The following is a list of TM cards:

- NT2X45AB – network interface card
- NT2X53AA – control card
- NT0X70AA – processor card
- NT4X65AB – On the cost reduced TM, the three cards listed above combine on a single card. The single card is the NT4X65.

Channel supervision message digital carrier module cards

The following is a list of DCM cards:

- NT2X36AA – network interface card
- NT2X34AA – supervision card
- NT2X33AB – control card

Channel supervision message line module cards

The following is a list of LM cards:

- NT2X36AA – network interface card
- NT2X22AB – connection memory and transmit multiplexer card
- NT2X34AA – peripheral processor message processor card
- NT2X33AE – CC message processor card

Channel supervision message line trunk controller cards

The following is a list of LTC cards:

- NT6X40BA – PM to network DS30 interface card
- NT6X41AA – formatter card
- NT6X42AA – channel supervision message (CSM) card

Additional network cards

Some network cards are not on the card list generated at the network accuracy level of the MAP display. These cards are common to multiple paths. The cards are not *high runners* in terms of contribution to office accuracy failures.

- NT3X73AA – serial to parallel formatter
- NT3X86AA – parallel to serial formatter
- NT3X74BA – network central side (C-side) processor

Central message controller

A defect in the CMC that prevents the function of the duplex message transmission mechanism can result in accuracy failures. A background CMC audit checks this mechanism. The CMC diagnostics quickly identifies the mechanism.

Central control software induced accuracy failures

The CC software problems can create accuracy failures if correct protocols are not followed. The system does not always report accuracy failures on the call that first set up the network path. For example, a call is set up between call A and call B. At the termination of the call, call B can continue the search for accuracy. According to CC software, the network connections are free, but the network hardware connection is not released. When a new network connection is established, the connection can use that same network path again or part of that network path again. This connection disrupts the CSM from the previous call. If the original endpoints are not part of the new call, the result is a NET101 log. The result is a NET101 log because the PM port and channel do not have a connection. The channel reports the accuracy failure. If one of the original endpoints is part of the new call, the result is a NET102 log. When the accuracy failure report generates, the new connection is in the CC software MAPs area. This report is an accuracy failure.

Peripheral module software induced accuracy failures

Maintenance actions on a PM, or messages to a PM lost during call assembly or disassembly, can result in accuracy failures. Commands to transmit an accuracy value or commands to look for accuracy are part of other call set up functions. Because commands are part of other call set up functions, lost messages cause failures in other aspects of call set up. Slow mapping of the CSM to one end of a call causes a failure mode that results in NET101 logs. When CC receives an on-hook message, CC releases the network connection. With the connection free, the connection is available for use again by another call. The CC receives and processes the on-hook message, and the original network connection is available for use again. An accuracy failure generates if two conditions occur at the same time. One condition is if the call at the other end did not receive a request to stop looking for accuracy. The second condition is if another call uses part of the original network connection again.

During a call set up that can be on a separate PM, the PM receives instructions to transmit a specified accuracy value. According to traffic and message loads, delays in the CC, network, PM, or processing of these messages can occur. If long delays occur, one PM can start to look for accuracy before the second PM transmits the new accuracy value. The system generates a NET101 or NET102 log report.

Manual activity accuracy failures

When you or the system sets a network OOS, the network continues to monitor calls in progress for accuracy on the OOS speech path. Due to the potential number of calls on a network, the system does not attempt to notify all PMs involved. The system also does not attempt to inform each terminal that the network, link, or junctor is OOS. Problems do not occur for original calls when the OOS network is not subject to additional actions. All new calls receive requests to look for accuracy on the in-service (InSv) network plane that remains.

When additional maintenance on the OOS network occurs, all calls in progress when you or the system set the network to OOS continue. Accuracy failures on this plane can occur for the calls that monitor for accuracy.

The OOS network diagnostic can induce accuracy failures because the connection memories change as part of the diagnostic.

Network module faults

The following cause network module defects:

- pair faults
- junctor faults
- link faults
- in-service trouble (ISTb) faults

Pair faults

A pair fault occurs when both NMs in a pair become busy at the same time. When a pair fault occurs, incoming and outgoing calls sent through this pair cannot be processed. The capacity of the switch reduces if a pair fault forces an NM pair OOS. The PM calls are routed to other NM pairs.

Junctor faults

When a junctor fault occurs in a card, 1 to 16 ports can be OOS. The number of OOS ports depends on the severity of the defect of the card. Each OOS port reduces the number of paths through the NM that has faults and that can carry speech between PMs. Junctors that have faults limit communication between the A- and B-sides of an NM. Junctors that have faults also reduce the capacity of the A- and B-sides of an NM.

Link faults

If a link fault occurs, the PMs that connect to the NM that has faults cannot use the port or ports affected by the fault. A link fault results in loss of the redundant connection for the link that has faults.

In-service trouble faults

Accuracy failures are a major source of ISTb faults. The transmitting PM continuously sends an accuracy code to the receiving PM. If part of the network fails, the accuracy code can distort. This distortion causes an accuracy failure.

Intermittent faults

For most faults, the DMS system automatically removes the NM or NM P-side port from service. To remove the module or port, the system changes the module or port state to system busy (SysB). To remove the module or port, the system also tests and returns to service (RTS) the module or port. Some faults occur at intervals. For the first occurrence of an intermittent fault, the system does not make the NM or NM port SysB. When the fault repeats, the fault is not continuous. For the NM maintenance, an intermittent fault causes a warm reset. For the NM P-side port maintenance, the system flags a port error. When either action occurs again, the correct hardware becomes SysB.

Warm resets by the network

When the firmware of a network detects a fault, the NM performs a warm reset. To perform a warm reset, the NM closes all P-side ports, logs the event, and and opens the ports again. Call processing begins again. If the warm reset occurs a second time, the network changes to SysB. When a maximum of five resets occur, the system generates log NETM146.

Network module P-side port fault

Another type of intermittent fault can occur during the messaging sent to and from a PM. This fault can occur when the system detects a fault on an NM P-side port. The NM closes the port, logs the event, and opens the port again. If the port continues to have a fault or the fault occurs a second time, the NM port changes to SysB. When a maximum of five port errors occur, the system generates log NETM147.

Enhanced network

When you access the Maintenance level (MTC), an alarm banner appears across the top of the display. This banner provides a basic status field for each major operating subsystem of the switching system. The alarm status field for the ENET subsystem appears under the alarm header NET. The system continuously updates the alarm status field for the subsystem so that the most severe fault condition always appears. Refer to appendix A in tables 11-1 to 11-3 for system, matrix, and shelf field values. Appendix A in table 11-4 also describes alarm codes for the ENET system.

Accuracy

Accuracy verifies the sanity of the speech path between two PMs. To monitor path accuracy, each PM checks for channel parity and checks the accuracy byte of the CSM. The reasons for accuracy faults fall into four groups:

- hardware
- call processing software
- PM software
- manual activity

The receiver PM detects accuracy faults. When a PM detects an accuracy mismatch, the PM reports the mismatch to the ENET accuracy fault handler. The fault handler maintains accuracy statistics to monitor the performance of the ENET and to help resolve accuracy faults. When a receiving PM detects a fault, the PM changes planes to receive from the other plane of the ENET. If the PM cannot establish accuracy after planes switch, the PM loses accuracy and call processing terminates the connection. The PM loses the call.

Hardware

Hardware failures or software logic errors can result in loss of the connection. Link or network related faults can be recovered because the network plane has a duplicate path. Hardware induced accuracy failures can occur in any position along the transmit or receive path of the call. These faults can occur in either of the two PMs involved in the call or in the network. These faults appear as parity errors.

Call processing software

Problems with computing module (CM) software or call processing software can induce accuracy failures. These failures occur when correct protocols are not followed. Call processing software must inform a PM to stop monitoring for accuracy when a connection disassembles. If call processing software does not inform the PM due to a problem with the call processing software, the system generates an accuracy failure report. The system generates the report when a new connection overwrites the old connection and sets a new accuracy value.

Lost messages to a PM during call setup or disassembly can cause accuracy failures. If the network loses messages as a result of call processing software problems, an accuracy failure occurs. Other phases of the call can fail.

Network diagnostics use call processing software. Network diagnostics can overwrite connection memories. Network diagnostics also can cause accuracy failures.

A call processing software problem can cause an improperly disabled path test. An improperly disabled path test can continue to insert data on a channel used by a call. The result is that accuracy failure occurs.

Peripheral module software

The PM software can report accuracy faults during periods of heavy traffic. Slow mapping of the CSM can cause faults. For example, if the network does not inform PM1 immediately that PM2 terminates a call, PM1 continues to check for accuracy after the connection terminates. A new connection and accuracy value are established. The result is that PM2 reports an accuracy fault.

Under heavy traffic, the receiving PM can begin to monitor for accuracy before the originating PM begins to send the call. The receiving PM reports an accuracy failure.

Manual activity

When you or the system sets a network OOS, the PM continues to monitor calls in progress for accuracy. As long as the system does not take action on the OOS network, problems do not occur with these calls. If the system takes maintenance action on the network, accuracy faults can occur on any calls in progress.

Improvements

Accuracy verifies the sanity of the speech path between two PMs. Each PM monitors the accuracy of calls through the network. When a mismatch occurs, the PM reports the accuracy fault to the ENET accuracy fault handler that diagnoses the reported path. The system pegs accuracy counters based on the result of accuracy diagnostics. Accuracy fault handling improves. When the system reports a new accuracy fault while the current fault handler handles another accuracy fault report, the accuracy path buffer stores the new report. The system does not peg a counter and does not generate a log.

The ENET accuracy fault handler implements the ENET path test to diagnose a path with a reported accuracy fault. The system always aborts the path test on a trunk as a result of the reserved channel. The system reports path test results in log ENCP102 “ENET Accuracy Diagnostics.” To reduce the amount of ENCP102 logs, the system changes the ENET accuracy fault handler to check if the reported path is on a trunk. The system changes the ENET accuracy fault handler before a path test is

submitted. If the path is on a trunk, a path test is not submitted and the system does not generate an ENCP102 log for this path.

The display designs of the following logs change:

- ENCP100
- ENCP101
- ENCP102

The design of the accuracy ENCP logs changes as follows:

- The fields are rearranged to display information in the following order:
  - — Information provided by the PM.
  - — Path information.
  - — Connection verification result.
  - — Path test result.
- Display detailed connection verification and reverification results.

Automatic maintenance

The NET maintenance subsystem automatically performs network fault detection and recognition. The fault detection mechanisms monitor the performance on InSv network hardware. The fault detection mechanisms also take action to isolate the item that has faults and does not affect call processing. The fault recognition mechanisms inform the software of a defect in OOS hardware. The fault recognition mechanisms also provide an indication to maintenance personnel of the specified location of the problem.

Double shelf network equipment

This section describes DSNE fault detection mechanisms. Fault detection mechanisms operate for the following:

- internal messages
- connection accuracy
- system-scheduled OOS tests
- network audit

Internal messages

Internal messages monitor the flow of internal messages between the CMC and the NM. Internal messages also monitor the flow of internal messages between the NM and the PM. The system compares the accuracy of a received message with the original message transmitted.

Connection accuracy

Connection accuracy monitors the accuracy byte of the CSM.

System-scheduled OOS tests

The system periodically performs system-scheduled OOS tests on OOS message links.

Network audit

On a 10-min cycle, the audit mechanism tests all InSv P-side message links and the network accuracy buffer.

Fault recognition, network audits, and error counters are additional automatic maintenance capabilities.

Fault recognition

When the system recognizes a fault, the system attempts to return the network that has faults to service. The system performs the loopback message and P-side processor communication tests. If the network passes these tests during the 10-min auditing cycle, the network is RTS. If the test fails, the system performs the complete OOS test. If the complete test fails, another attempt to RTS occurs during the 10-min audit cycle. The network SysB counter records the number of times that the test fails during the 10-min auditing cycle. This counter increases when the system sets the network to the SysB state. The auditing cycle resets this counter to 0 every 10 min, or when the command RTS passes. If the counter increment reaches a threshold value of 3, the system generates log NETM128. This log identifies the network that has faults.

Network audit

The auditing cycle checks the network clock control register and the PM for normal values. The auditing cycle also participates in the fault detection process. Network performance counters record a number of events on the C- and P-sides of each NM. The audit reads the counts every second day for each network. The audit prints the counts to the network logs. The audit also resets all counters to 0. The number of accuracy and parity errors appear for each plane of each pair. The log system generates a daily summary of this information every day at 8:00 a.m. in the form of a NET103 report.

Net log messages

The network SysB counter records the number of times that the test fails during the 10-min auditing cycle. This counter increases when the network changes to SysB state and the auditing cycle resets the counter to 0 every 10 min. The counter also increases when you enter the command RTS.

Error counters

Network firmware increases error counters to allow analysis of not continuous problems. Network firmware supports different error counters. Error counters are useful in the analysis of network problems, including transient or not continuous problems. Table 1-1 lists the counters available for access from the network level of the MAP display. These counters display error conditions and must be set to 0 during normal error-free operation. The C-side counters appear for each CMC. The P-side counters (only one set) appear for each NM.

Table 1-1
Network error counters

Error counter	Description
BUFFER	Buffer errors. P-side counter
BUFFULL	Buffer full counter. C-side counter. The CMC attempts to send a message to the network before the NM replies with the *send* signal. The CMC checks that a message buffer is available to store the received message. If all buffers are full, the network delays the *send* to the CC until a buffer becomes available. The network pegs a counter to flag the delay.
INCDEL	Incoming message delayed. C-side counter.
MSGIGN	Messages ignored. P-side counter. The only normal check on an incoming message during message reception is on the message length. If the network encounters a message with length less than 10 bytes or greater than 64 bytes, the network will not continue to process the message. The network pegs the MSGIGN counter and proceeds to scan other ports.
NACK1	Single NACKs received. C- and P-side counters. If a message is received with a wrong checksum, the receiver replies with a NACK to the sender. The sender pegs the message in the NACK1 counter and attempts to send the message a second time.

—continued—

Table 1-1
Network error counters (continued)

Error counter	Description
NACK2	Double NACKs received. C- and P-side counters. If the network receives a NACK on the second attempt to transmit the message, the network does not continue to transmit that message. The network pegs the NACK2 counter.
NACKS	NACKs sent. C- and P-side counters. Counts the number of times the network was the receiver. Counts the number of times the network detected message checksum problems. Counts the number of times the network sends NACK signals to the CMC or peripheral as correct.
OPCOOR	OPCODE out of range. C-side counter. The network encounters an out-of-range network operation code when the network processes messages.
RETRY	Retry counter on writes to connection memory. C-side counter.
RMKILL	Return message killed. C-side message. A reply message from a network operation. The network cannot send the message to a PM or the CC by either CMC. The network pegs this counter, and discards the message.
WFACK	Wait for acknowledgment. C- and P-side counters. The sending node transmits the message to the receiving node. The receiver confirms that the checksum calculated over the message bytes matches the checksum byte appended to the message. If the checksum matches, a positive acknowledgment (PACK) transmits to the sender. If the checksum does not match, a negative acknowledgment (NACK) transmits to the sender. The sender waits to receive for the WFACK time-out period for a PACK or NACK. If the sender does not receive a PACK or NACK, the network pegs the WFACK counter.

—continued—

Table 1-1
Network error counters (continued)

Error counter	Description
WFSND	Wait for send time-out. C- and P-side counters. The standard DS30 protocol for message transfer between nodes is that the sending node transmits a may I send to the receiving node. The sending node waits for a period of time for a *send* signal from the receiving node. If the WFSND time-out period expires, the network pegs the WFSND time-out counter. The network pegs the counter for the CMC or P-side link as correct.
WSOM	Wait for start of message time-out. C- and P-side counters. After the receiver detects the may I send from the sender, the receiver transmits a *send* signal. If the sender does not start to transmit the message within WSOM time-out period, the receiver pegs the WSOM time-out counter.
	—end—

Network error counters are network performance indicators, operational measurements (OM), and LOGUTIL reports. You must monitor the C- and P-side counters for all of the network pairs in early morning and late afternoon. In early morning, monitor the network performance through the night. If the performance is bad, replace the problem card in a network before heavy traffic load begins. In late afternoon, monitor the network performance through the day. If the performance is bad, replace problem cards later in the evening when heavy traffic load decreases.

Enhanced network

This section describes the ENET automatic maintenance.

Use the accuracy level of the MAP display to analyze errors that occur along the speech links between PMs and the ENET.

Each PM monitors the accuracy of links through the network. The PM monitors through a continuous exchange of PCM samples for calls in progress and CSMs for signal accuracy. When a mismatch occurs, the network informs the ENET maintenance system.

The DMS SuperNode system peripheral loader is a software module located in the CM. When a peripheral requires loading, the CM resident code of the peripheral sends a request to the loader to start booting. The loader process begins to transfer load records from the file system to the peripheral. Improvements were added to determine if a load file is correct. The following is a list of improved loader logs. The improvements provide easy determination of nodes which passed and failed:

- Boot100 (loader pass log)
- Boot101 (loader fail log)

Quick reference to manual maintenance

Audible and visual alarms indicate that correcting action is required. The level of alarm (minor, major, or critical), indicates the need for correcting action.

- Minor alarms indicate a condition that does not affect or threaten service.
- Major alarms indicate a service degrading condition to several customers. Major alarms also indicate that another failure can cause service power failure to several customers.
- Critical alarms indicate a service power failure condition to a larger number of customers. Critical alarms also indicate that another failure can result in service power failure. The service power failure can affect a large number of customers or all customers in the office.

Log messages indicate trouble conditions when the following are present:

- sudden increases in volumes of logs
- message `not printed` reports
- large numbers of logs

When OMs are evaluated against established values, use OMs to identify the following:

- trouble conditions
- service levels
- equipment performance
- need for maintenance activity

Preventive maintenance methods

Routine procedures are procedures that you perform according to a schedule. Routine procedures help to make sure that the hardware and software of a network are free of faults. These procedures also help to make sure that you can easily correct faults in the network.

Description of routine maintenance procedures

Table 2-1 contains suggested routine maintenance procedures and schedules. For detailed information on routine maintenance procedures of Networks, refer to *Routine Maintenance Procedures*.

Table 2-1
Routine Maintenance

Procedure	Schedule
Preventing dust accumulation in a 42–in. cabinet	Perform this procedure at 45-day intervals.
Replacing a cooling unit filter in a 1.07–m (42–in.) cabinet	Perform this procedure at six-week intervals.
Returning a card or assembly	Perform this procedure as required.
Recording an ENET image on an SLM disk	Perform this procedure when an ENET software upgrade or patch occurs.
Testing wrist-strap grounding cords	Perform this procedure every month.
—end—	

Network-related logs

You must maintain a network that is accurate, valid, and free from defects. Network performance is a key element to desired switch performance. Logutil is one of the Digital Multiplex System (DMS) *subsystems* that indicates network performance.

The DMS switch prints output messages in the form of log reports, when one of the following actions occur:

- you enter a command that changes the state of a network module (NM)
- you enter a command that changes the state of the NM component
- specified events occur

Log reports provide a record of events that take place inside a DMS switch. Table 3-1 lists logs that associate with the Enhanced Network (ENET) and double shelf network equipment (DSNE) frame. For an explanation of all logs, refer to the *Log Report Reference Manual*.

Table 3-1
Network-related logs

Log name	Causes	Response
ENCP100	The ENET call processing subsystem generates this report when an accuracy fault occurs, and the connection was not terminated.	No action required. Information purposes only.
ENCP101	The ENET call processing subsystem generates this report when a peripheral module (PM) reports an accuracy mismatch for a terminated connection. The ENC101 generates when the accuracy fault handler begins to analyze the report for the terminated connection.	No action required. Information purposes only.

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENCP102	The ENET call processing subsystem generates this report when a PM reports an accuracy fault, and the connection was not terminated.	Replace the cards in the card list. Run the ENET path test again to check for an correct replacement.
ENCP103	The ENET call processing subsystem generates this report every hour when an accuracy fault audit runs. This report is a summary of the number of accuracy faults reported for the switch.	Take the in-service trouble (ISTb) cards out of service (OOS). Run diagnostics.
ENCP104	The ENET call processing subsystem generates this report when a request to clear the accuracy counters occurs.	No action required. Information purposes only.
ENCP105	The ENET call processing subsystem generates this report when changes are made to the values of the accuracy thresholds and PM thresholds. The subsystem also generates ENCP105 when ENET accuracy logs or ENET accuracy audits are turned on or off.	No action required. Information purposes only.
ENCP131	The ENET call processing subsystem generates this report when an ENET connection is created that overwrites a current connection.	No action required. Information purposes only.
ENCP132	The ENET call processing subsystem generates this report when an ENET connection occurs that attempts to overwrite a current connection.	No action required. Information purposes only.
ENCP133	The ENET call processing subsystem generates this report when an ENET connection log audit runs.	No action required. Information purposes only.
ENCP134	The ENET call processing subsystem generates this report when an attempt is made to reverse an ENET path not connected in hardware.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENCP135	The ENET call processing subsystem generates this report when an attempt is made to reverse an ENET path that cannot be reversed.	No action required. Information purposes only.
ENCP136	The ENET call processing subsystem generates this report when an attempt is made to create an ENET connection. The subsystem generates this report when the hardware for the connection is OOS in both planes.	No action required. Information purposes only.
ENCP143	The ENET call processing subsystem generates this report when it encounters a discrepancy with the nailed-up connection map compared to the connection map.	No action required. Information purposes only.
ENCP150	The ENET call processing subsystem generates this report when a connection is freed. The subsystem generates this report when the specified *from end* is not equal to the *from end* that connection control stored.	No action required. Information purposes only.
ENDB101	The ENET Synchronous Optical Network (SONET) DMS database audit subsystem generates this report when a data mismatch occurs. The subsystem generates this report when a data mismatch occurs between the master version and the node, and the audited version.	If ENDB101 generates too many logs for the same node, perform a return to service (RTS) on the affected node. Under normal conditions, no action is required.
ENET100	The ENET subsystem generates this report when the specified ENET node changes state from manual busy (ManB) or system busy (SysB) to OK.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET101	The ENET subsystem generates this report when the specified ENET node changes state from OK to ManB.	No action required. Information purposes only.
ENET102	The ENET subsystem generates this report when an ENET node changes state from central side (C-side) busy, SysB, or offline (OFFL) to ManB.	No action required. Information purposes only.
ENET103	The ENET subsystem generates this report when an ENET node changes state from OK to SysB.	Follow standard office procedures for maintenance of a SysB ENET.
ENET104	The ENET subsystem generates this report when an ENET node changes state from C-side busy to SysB.	Follow standard office procedures for maintenance for a SysB ENET.
ENET105	The ENET subsystem generates this report when an ENET node changes state from OK, ManB, or SysB to C-side busy.	If the ENET recovery fails, follow the ENET RTS procedures.
ENET106	The ENET subsystem generates this report when an ENET node changes state from ManB or unequipped to OFFL.	No action required. Information purposes only.
ENET107	The ENET subsystem generates this report when an ENET node changes state from OFFL to unequipped.	No action required. Information purposes only.
ENET108	The ENET subsystem generates this report when an ENET node sets or clears an ISTb.	Follow standard office procedures on how to handle an ISTb.
ENET110	The ENET subsystem generates this report when a test runs on the ENET node and passes.	No action required. Information purposes only.
ENET111	The ENET subsystem generates this report when an ENET node test runs and fails.	Replace and test the cards listed in the card list after each test.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET112	The ENET subsystem generates this report when an ENET system RTS attempt fails.	No action required. Information purposes only.
ENET114	The ENET subsystem generates this report when an ENET parallel system recovery action occurs.	Follow the standard office procedures for ENET node recovery failures.
ENET120	The ENET subsystem generates this report when an ENET routine exercise (REx) test on a shelf fails. This failure is a result of an error with the sanity or availability of the ENET boot file.	Follow the standard office procedures for ENET boot file failure.
ENET200	The ENET subsystem generates this report when the ENET card changes state from ManB or SysB to OK.	No action required. Information purposes only.
ENET201	The ENET subsystem generates this report when the ENET card changes state from OK to ManB.	No action required. Information purposes only.
ENET202	The ENET subsystem generates this report when the ENET card changes state from C-side busy, SysB, or OFFL to ManB.	No action required. Information purposes only.
ENET203	The ENET subsystem generates this report when the ENET card changes state from OK to SysB.	Follow standard office procedures on how to handle SysB ENET cards.
ENET204	The ENET subsystem generates this report when the ENET card changes state from C-side busy to SysB.	Follow standard office procedures on how to handle SysB ENET cards.
ENET205	The ENET subsystem generates this report when the ENET card changes state from OK, ManB, or SysB to C-side busy.	Follow standard office procedures on how to handle C-side busy ENET cards.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET206	The ENET subsystem generates this report when the ENET card changes state from ManB or unequipped to OFFL.	No action required. Information purposes only.
ENET207	The ENET subsystem generates this report when the ENET card changes state from OFFL to unequipped.	No action required. Information purposes only.
ENET208	The ENET subsystem generates this report when the ENET card is set or cleared in ISTb.	From the logs, determine the reason for the trouble. Test the node while InSv. Replace the cards produced by the card list.
ENET210	The ENET subsystem generates this report when tests run and pass on an ENET card. The generation of the log depends on the software that performs the tests.	No action required. Information purposes only.
ENET211	The ENET subsystem generates this report when tests run on the ENET card fail.	Manually test the failed cards. If the failure occurs again, replace the card.
ENET220	The ENET subsystem generates this report when a matrix test of the switching matrix of the ENET passes.	This log is for information purposes only.
ENET221	The ENET subsystem generates this report when a matrix test of the switching matrix of the ENET fails.	Replace cards that have faults and run the matrix test again. If the test fails and continues to indicate the same cards have faults, contact the next level of maintenance.
ENET222	The ENET subsystem generates this report when a node is RTS. The system finds a minimum of one card that has faults during the RTS of the cards.	Replace the cards that have faults, and try to RTS them. If the RTS fails and indicates the same cards have faults, contact the next level of maintenance.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET230	The ENET subsystem generates this report when the crosspoint or ripple open test finds a crosspoint or interface card that was in the wrong hardware state.	Test the cards that have faults again. Use normal card replacement procedures to replace any cards that have faults.
ENET300	The ENET subsystem generates this report when a peripheral side (P-side) link changes state from ManB or SysB to OK.	No action required. Information purposes only.
ENET301	The ENET subsystem generates this report when a P-side link changes state from OK to ManB.	No action required. Information purposes only.
ENET302	The ENET subsystem generates this report when a P-side link changes state. The report generates when the state changes state from OFFL, SysB, C-side or P-side busy to ManB.	No action required. Information purposes only.
ENET303	The ENET subsystem generates this report when a P-side link changes state from OK to SysB.	Follow standard office procedures on how to deal with SysB P-side links.
ENET304	The ENET subsystem generates this report when a P-side link changes state from C-side or P-side busy to SysB.	Follow standard office procedures on how to deal with a SysB P-side link.
ENET305	The ENET subsystem generates this report when a P-side link changes state from SysB, OK, ManB, or P-side busy to C-side busy.	Follow standard office procedures on how to handle C-side busy P-side links.
ENET306	The ENET subsystem generates this report when a P-side link changes state from ManB or unequipped to OFFL.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET307	The ENET subsystem generates this report when a P-side link changes state from OFFL to unequipped.	No action required. Information purposes only.
ENET308	The ENET subsystem generates this report when a P-side link is set to ISTb.	Follow standard office procedures on how to handle ISTb P-side links.
ENET309	The ENET subsystem generates this report when a P-side link changes state from OK, ManB, SysB or C-side busy to P-side busy.	Follow standard office procedures on how to handle P-side busy links.
ENET310	The ENET subsystem generates this report when a P-side link test runs and passes.	No action required. Information purposes only.
ENET311	The ENET subsystem generates this report when a P-side link test fails.	Follow standard office procedures on how to deal with failed P-side link tests.
ENET312	The ENET subsystem generates this report when the PM message path through the ENET plane switches from one C-side fiber link to another.	No action required. Information purposes only.
ENET313	The ENET subsystem generates this report when too many recent faults on the specified path prevent message path reswitching because the specified path has too many recent faults.	This log indicates that the specified message switch (MS) card and port have faults.
ENET314	The ENET subsystem generates this report every hour. The report provides a summary of ENET P-side link audit corrections during this period.	No action required. Information purposes only.
ENET315	The ENET subsystem generates this report when the use of the ALTTEST command changes a P-side maintenance default parameter.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET401	The ENET subsystem generates this report when the system finds a fault with C-side links.	Follow standard office procedures on how to deal with failed C-side link tests.
ENET402	The ENET subsystem generates this report if any C-side link faults occurred on an InSv ENET port during the last audit cycle.	No action required. Information purposes only.
ENET500	The ENET subsystem generates this report when the scheduled invocation of the ENET REx test changes.	No action required. Information purposes only.
ENET501	The ENET subsystem generates this log report to indicate that the system disabled automatic ENET REx testing through the entries in table REXSCHED.	Operating company personnel must determine if the REx testing must be disabled. If required, operating company personnel changes the entries in table REXSCHED to enable the REx testing.
ENET502	The ENET subsystem generates this report when you or the system requests the ENET REx test to run, and the test cannot run.	No action required. Information purposes only.
ENET503	The ENET subsystem generates this report when the ENET REx test begins.	No action required. Information purposes only.
ENET504	The ENET subsystem generates this report when the ENET REx test passes.	No action required. Information purposes only.
ENET505	The ENET subsystem generates this report when the ENET REx test fails.	Replace the cards in the card list.
ENET506	The ENET subsystem generates this report when the system aborts the ENET REx test.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET507	The ENET subsystem generates this report when the ENET REx test is not complete as a result of an internal error.	No action required. Information purposes only.
ENET508	The ENET subsystem generates this report when the ENET REx test passes without severe failures.	If required, replace the cards in the card list.
ENET510	The ENET subsystem generates this report when the ENET nodeREx test starts, cannot run, is aborted, or is not complete.	No action required. Information purposes only.
ENET511	The ENET subsystem generates this report when the ENET nodeREx test passes on the specified shelf.	No action required. Information purposes only.
ENET512	The ENET subsystem generates this report when the ENET nodeREx test passes or fails with ISTb.	If necessary, replace the cards in the card list.
ENET520	The ENET subsystem generates this report when the ENET matrixREx test starts, cannot run, is aborted, or is not complete.	No action required. Information purposes only.
ENET521	The ENET subsystem generates this report when the ENET matrixREx test passes.	No action required. Information purposes only.
ENET522	The ENET subsystem generates this report when the ENET matrixREx test passes or fails with ISTb.	If required, replace the cards in the card list.
ENET600	The ENET subsystem generates this report when you start a bit error rate test (BERT).	No action required. Information purposes only.
ENET601	The ENET subsystem generates this report when the ENET BERT is complete.	Test suspect paths to determine the cause of errors.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
ENET700	The ENET subsystem generates this report when one of the following commands issues a warning, or must issue a warning: • BSY • RTS • TST • OFFL • ABTRK • LOADEN • LOADENALL	No action required. Information purposes only.
IOAU112	The input/output audit subsystem generates this log report to inform operating company personnel of changes in the system REx test schedule.	Verify the affected tuple entries in table REXSCHED and adjust the schedule parameters, if required. If the log report indicates automatic ENET REx testing is disabled, operating company personnel must determine if the REx testing must be disabled. If required, operating company personnel must change entries in table REXSCHED to enable the REx testing.
NET100	A receiving peripheral detects an accuracy mismatch. The network path has a defined path, but resources are not available to diagnose the problem.	Collect and compare following accuracy messages to determine the cause of the accuracy failures. Use the NET INTEG level of the MAP display to assist in the process.
NET101	A receiving peripheral detects an accuracy mismatch. The system cannot recover the path data because the call disconnects before the network can freeze the connection for diagnostic purposes.	Collect and compare following integrity messages to determine the cause of the accuracy failures. Use the NET INTEG level of the MAP display to assist in the process.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NET102	A receiving peripheral detects an accuracy fault. An accuracy fault can be a parity failure or an accuracy mismatch.	Collect and compare following accuracy messages to determine the cause of the accuracy failures. Use the NET INTEG level of the MAP display to assist in the process.
NET103	The network subsystem generates this report to summarize the accuracy faults in the switch.	If any counter exceeds 80, refer to the NET INTEG level of the MAP display to investigate this potential problem.
NET104	The network subsystem generates this report when NET PATH diagnostics find cards that have faults.	Replace cards in the list of faults. Run the NET PATH test again to check for a correct replacement.
NET105	The network subsystem generates this report when the AUTO NET PATH test passes or is aborted.	If the test is aborted, refer to the ABORTED REASONS table for NET105 to find the correct action. The table is in the *Log Report Reference Manual*. Repeat the test.
NET106	Provides the status of the scheduled NET PATH tests.	Test the paths manually. After batch change supplement (BCS) applications or restarts, the scheduled tests are aborted. Implement the scheduled tests again.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NET130	The network subsystem generates this report as a result of a system request when the system cannot find a network path.	No action required if the system generates one or two logs each day. Take the following action if a pattern develops or the number of logs increases. • If the JNET is in the process of installation or expansion, contact NORTEL installation. • Check for JNET H/W faults, particularly junctors. Junctors that have faults can result in NET130 logs. • If the JNET is free of faults, and blockage is a concern, contact NORTEL TAS.
NET131	The network subsystem generates this report when one connection writes over another connection.	No action required. Information purposes only.
NET132	The network subsystem generates this report when the subsystem detects attempts to connect a network path end that has an allocated path.	No action required. Information purposes only.
NET133	The network subsystem generates this report when a network attempts to make a connection that is not reserved.	If this log persists, notify the next level of maintenance support.
NET134	The network subsystem generates this report to signal a call processing sequence that is not permitted.	Contact the next level of maintenance.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NET135	The network subsystem generates this report under one of the following conditions: • when the system attempts to reverse a reserved path • when a path is not present • when *to* pathend is present, and the other end is not found. • when the number of connections is other than one	Report to the next level of maintenance support.
NET136	The network subsystem generates this report when the subsystem detects an attempt to connect two ports that do not have InSv planes available.	RTS the correct network, plane, or junctor.
NET155	The network subsystem generates this report when a network plane pair uses the wrong MS for the clock source.	If this log persists, notify the next level of maintenance support.
NETM103	The network maintenance subsystem generates this report when an NM is RTS as a result of a manual or system request.	No action required. Information purposes only.
NETM104	The network maintenance subsystem generates this report when an NM becomes SysB. An NM becomes SysB when links between the central message controller (CMC) and the specified network are busy.	Refer to the *Index to Maintenance Procedures Documents*, 297-1001-500 for information on how to clear the alarm.
NETM105	The network maintenance subsystem generates this report to indicate that the specified NM was ManB.	No action required. Information purposes only.
NETM106	The network maintenance subsystem generates this report to record that the NM was set to the OFFL state.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NETM107	The network maintenance subsystem generates this report to record when the network changed state to unequipped.	No action required. Information purposes only.
NETM108	The network maintenance subsystem generates this report when a C-side message link between the CMC and the network is RTS. The subsystem generates the report after both C-side message links are down.	Clear minor alarm. Refer to the *Index to Maintenance Procedures Documents, 297-1001-500*.
NETM109	The network maintenance subsystem generates this report to record that the two message links between the CMC and the network are OOS.	Clear minor alarm, refer to the *Index to Maintenance Procedures Documents, 297-1001-500*.
NETM110	The network maintenance subsystem generates this report every day at 8:00 a.m. Firmware performance maintenance counters for all the networks are in this log report. This log contains the printout for the NT5X13AA and NT8X11AD network C-side counter values. This log also contains the P-side counter values for networks NT0X48AJ, NT5X13AA, and NTX8X11AD.	Save these logs if large values appear in counters. The next level of maintenance support can use these logs.
NETM111	The network maintenance subsystem generates this report to display the contents of the firmware performance maintenance counter. This log contains the printout for the NT0X48AJ network C-side counter values.	Save these logs if large values appear in counters. The next level of maintenance support can use these logs.
NETM112	The network maintenance subsystem generates this report as a result of a manual or system request for diagnostic tests on the NM.	Repair the network.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NETM115	The network maintenance subsystem generates this report as a result of a manual or system requests to set links between a PM and an NM to InSv state.	No action required. Information purposes only.
NETM116	The network maintenance subsystem generates this report after a system request to set a link between an NM and a PM to SysB state.	Manually test the link.
NETM117	The network maintenance subsystem generates this report as a result of a manual request to set a link between a PM and an NM to the ManB state.	No action required. Information purposes only.
NETM118	The network maintenance subsystem generates this report after a manual request to set the message link between a PM and an NM to OFFL state.	No action required. Information purposes only.
NETM119	The network maintenance subsystem generates this report as a result of a manual request to set the link between a PM and an NM to the unequipped state.	No action required. Information purposes only.
NETM120	The network maintenance subsystem generates this report as a result of manual or system requests for a diagnostic test on a link between a PM and an NM.	Repair the link.
NETM121	The network maintenance subsystem generates this report as a result of a failed manual or system request to set the network junctor to the RTS state.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NETM122	The network maintenance subsystem generates this report as a result of a system request to set a network junctor to the SysB state.	Manually test the junctor.
NETM123	The network maintenance subsystem generates this report as a result of a manual request to set a network junctor to the ManB state.	No action required. Information purposes only.
NETM124	The network maintenance subsystem generates this report as a result of a manual request to set a network junctor to the OFFL state.	No action required. Information purposes only.
NETM125	The network maintenance subsystem generates this report as a result of a manual request to set a network junctor to the unequipped state.	No action required. Information purposes only.
NETM126	The network maintenance subsystem generates this report as a result of a manual or system request to run a diagnostic test on a network junctor.	Manually test the junctor to obtain the list of possible failed cards.
NETM128	The network maintenance subsystem generates this report when the network-hits threshold is exceeded.	No action required. Information purposes only.
NETM129	The network maintenance subsystem generates this report as a result of a system request when five or more failures occur on a network port.	No action required. Information purposes only.
NETM137	The network maintenance subsystem generates this report for information and debugging purposes only.	Report to the next level of maintenance.
NETM138	The network maintenance subsystem generates this report when you manually override the warning that a network is to become ManB.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NETM139	The network maintenance subsystem generates this report when the warning that a link is to become ManB is manually overridden.	No action required. Information purposes only.
NETM140	The network maintenance subsystem generates this report when you manually override the warning that a junctor is to become ManB.	No action required. Information purposes only.
NETM141	The network maintenance subsystem provides this report as general information.	Action depends on log reason.
NETM142	The network maintenance subsystem generates this report when data for the failure counters or threshold limits for accuracy analysis resets or starts	No action required. Information purposes only.
NETM143	The network maintenance subsystem generates this report when the nailed-up connection (NUC) audit process identifies an NUC table discrepancy. The report generates when the call does not connect as an NUC.	No action required. Information purposes only.
NETM144	The network maintenance subsystem generates this report when the NUC subsystem holds more NUCs than specified in table OFCENG (office engineering). The report generates after a restart.	No action required. Information purposes only.

—continued—

Table 3-1
Network-related logs (continued)

Log name	Causes	Response
NETM145	The network maintenance subsystem generates this report to specify that a junctor port that holds a NUC is busy. The report generates when the subsystem detects an attempt to move the connection. When the attempt fails, the connection can break because of the problem associated with the junctor port.	No action required. Information purposes only.
NETM146	The network maintenance subsystem generates this report when a warm reset of the network occurs.	Save all reports generated during the 5 min before the NETM146 report generates, and contact the next level of maintenance.
NETM147	The network maintenance subsystem generates this report when a port error occurs.	Test the link indicated by this log report.
NETM148	The network maintenance subsystem generates this report when the system detects a problem during a network link test.	If this log occurs repeatedly for a network port, run ten tests on the port. If any test fails, replace the indicated hardware. If all tests pass but logs persist (more than five a day on one port), replace the testing network interface card. Replace the network interface card if field *testxt* indicates *Spchloop–on Net*. Replace the PM interface card if field *TXT* indicates *Spchloop–on link*.
NETM149	The network maintenance subsystem generates this report when the subsystem detects a problem during a network link test.	Refer to the REASONS table for NETM149 in the *Log Report Reference Manual*.
NETM161	The network maintenance subsystem generates this report every day at 8:00 a.m. The call processing blocking counts for each network pair print.	Contact the next level of maintenance if large counts for any of the counters appear.
—end—		

Network related operational measurements

Operational measurements (OM) are resources used for monitoring events in a Digital Multiplex System (DMS). OM calculations help administer and maintain in the DMS switch. The OM counts events or the number of times the OM finds a piece of equipment in a specified state. Counts of events and states can be either call related or equipment related. Call-related OMs count events related to traffic operations. Equipment-related OMs associates with the hardware in the switch. OMs show the level of network performance. OM data helps to analyze switch performance and traffic. Table 4-1 lists OMs associated with the Enhanced Network (ENET) and the double shelf network equipment (DSNE). For an explanation of all the OMs and the registers for the OM, refer to *Operational Measurements Reference Manual*.

Table 4-1
Network operational measurements

Group	Description
PM2	Two-unit peripheral module (PM) maintenance summary provides information on the performance of a two-unit PM. This OM does not only handle network failures. But each time a NET101 or NET102 occurs, the system pegs a field in OM PM2. The PM that reports the accuracy failure is a line concentrating module (LCM) or an XMS-based peripheral module (XPM).
ENETMAT	Enhanced network matrix card monitors the performance of ENET matrix cards. ENET matrix card OMs belong to two sets. The first set is for crosspoint cards. The other set is for link paddle boards.
ENETOCC	Enhanced network occupancy provides information about the central processing unit (CPU) occupancy of each in-service (InSv) ENET in a DMS switch.
ENETPLNK	ENET peripheral side (P-side) links monitor the performance of ENET P-side links.

—continued—

Table 4-1
Network operational measurements (continued)

Group	Description
ENETSYS	Enhanced network system card monitors the performance of the following ENET system cards: • NT9X13–processor card • NT9X26–reset terminal interface (RTIF) paddle board • NT9X36–ENET messaging clock card • NT9X40–ENET + quad fiber interface paddle board • NT9X30–power converter • NT9X31–power converter
NETMSG	Network message service monitors the use of network message services.
NMC	Network module controller maintenance summary counts errors and failures from errors in the following: • InSv message links between network modules (NM) and PM • speech connections • InSv NM controllers NMC also records if out-of-service (OOS) NMs, network ports, and junctors are system busy (SysB) or manual busy (ManB).
OFZ	Office traffic summary provides information for traffic analysis. OFZ summarizes the arrangement of traffic that arrives at an office, the first route, and the route of outgoing traffic.
TM	Trunk module counts errors, faults, and maintenance state changes for trunk modules (TMs), maintenance trunk modules (MTM), and remote service modules (RSM).
TS	Time switch records the use of the P-side time switches.
	—end—

Table 4-2 lists possible service affecting OMs.

Table 4-2
Service affecting operational measurements

Group	Description
ENETMAT	ENETMAT contains registers that count the following: • errors in ENET crosspoint cards • defects in ENET crosspoint cards • ENET partitions that occur because of a SysB ENET crosspoint card • ENET partitions that occur because of a ManB ENET crosspoint card • PMs that are isolated because an ENET crosspoint card is SysB • PMs that are isolated because an ENET crosspoint card is ManB • errors in ENET link paddle boards • defects in ENET link paddle boards • ENET partitions that occur because of a SysB ENET link paddle board • ENET partitions that occur because of a ManB ENET link paddle board • PMs that are isolated because an ENET link paddle board is SysB • PMs that are isolated because an ENET link paddle board is ManB

—continued—

Table 4-2
Service affecting operational measurements (continued)

Group	Description
ENETPLNK	ENETPLNK contains registers that count the following: • errors on speech connections through the network • errors on InSv links between the network and PM • defects on P-side links • ENET partitions that occur because of a SysB ENET P-side link • ENET partitions that occur because of a ManB ENET P-side link • PMs that are isolated because an ENET P-side link is SysB • PMs that are isolated because an ENET P-side link is ManB
ENETSYS	ENETSYS contains registers that count the following: • errors in ENET system cards • defects in ENET system cards • calls denied because system cards are OOS • ENET CPU traps • ENET CPU software errors • ENET CPU warm restarts • ENET CPU cold restarts • ENET CPU reload restarts • ENET partitions that occur because of a SysB ENET system card • ENET partitions that occur because of a ManB ENET system card • PMs isolated because of a SysB ENET system card • PMs isolated because of a ManB ENET system card

—continued—

Table 4-2
Service affecting operational measurements (continued)

Group	Description
NMC	NMC counts errors and failures in the following: • InSv message links between NMs and PMs • speech connections • InSv NM controllers NMC also records when OOS NMs, network ports, and junctors are SysB or ManB.
TM	TM counts errors, faults, and maintenance state changes for TMs, MTMs, and RSMs.
	—end—

Network related data structures

Network related data structures will be provided in a future release.

Network related user interface commands

This chapter summarizes the user interface facilities provided on the maintenance and administration position (MAP) display. This chapter helps you to monitor and maintain the double-shelf network equipment (DSNE) frame and the Enhanced Network (ENET).

Information at The MAP organizes information into a series of display levels. The display levels start at the command interpreter (CI) level. At the CI level the MAPCI command accesses the highest display level of a subsystem. Subsystems have one or more levels where you can monitor and maintain hardware and software.

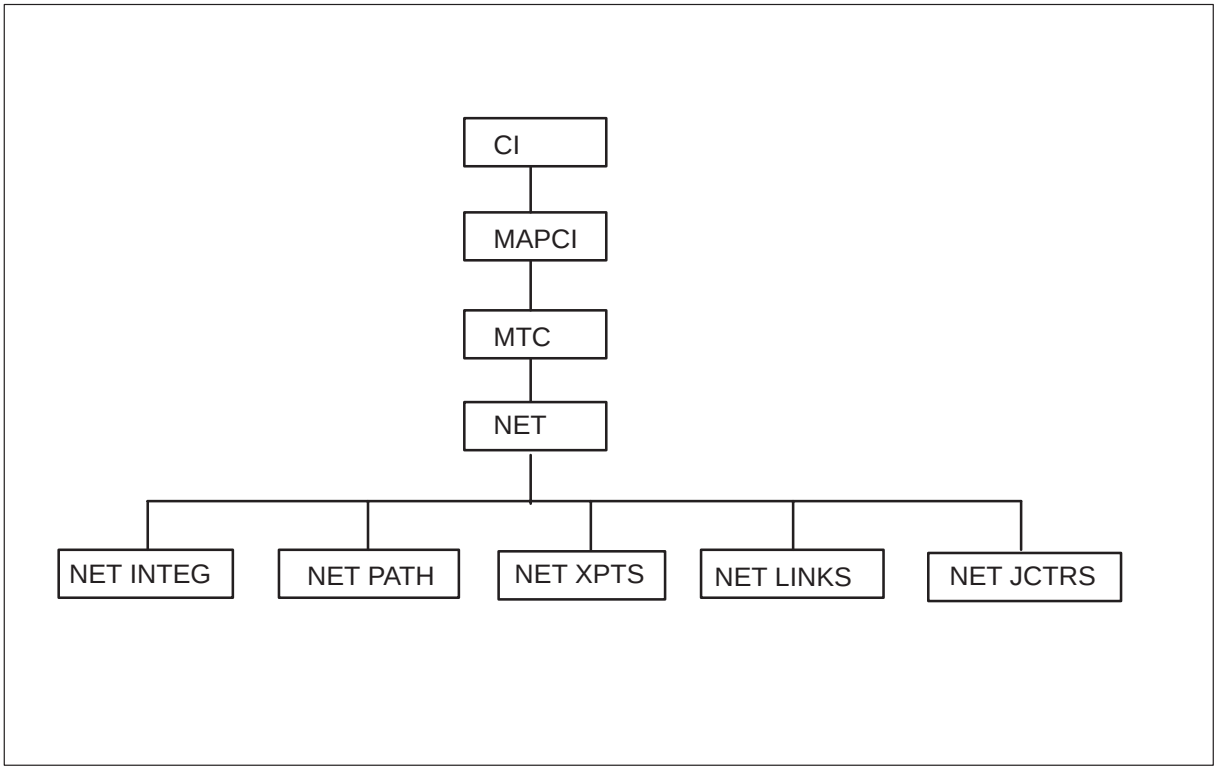
Double shelf network

From the MAPCI level, access other levels by the branches of the levels. For example, you can access the maintenance (MTC) and the network (NET) levels. Figure 6-1 represents the network maintenance subsystem for the DSNE.

The following are available from the NET level:

- network crosspoints (NET XPTS)
- network integrity (NET INTEG)
- network junctors (NET JCTRS)
- network links (NET LINKS)
- network path (NET PATH)

Figure 6-1
Double shelf network subsystem



Network level menu commands

The command syntax to reach the NET level from the CI level is as follows:

>MAPCI;MTC;NET

Figure 6-2 illustrates the MTC level MAP display. Figure 6-3 on page 6-4 illustrates the NET level MAP display. This display provides status information for a mmaximum of 32 network modules (NM), numbered 0 through 31. An ordered list of command descriptions of the menu items follow after the figure. For a complete list of command parameters and use, refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

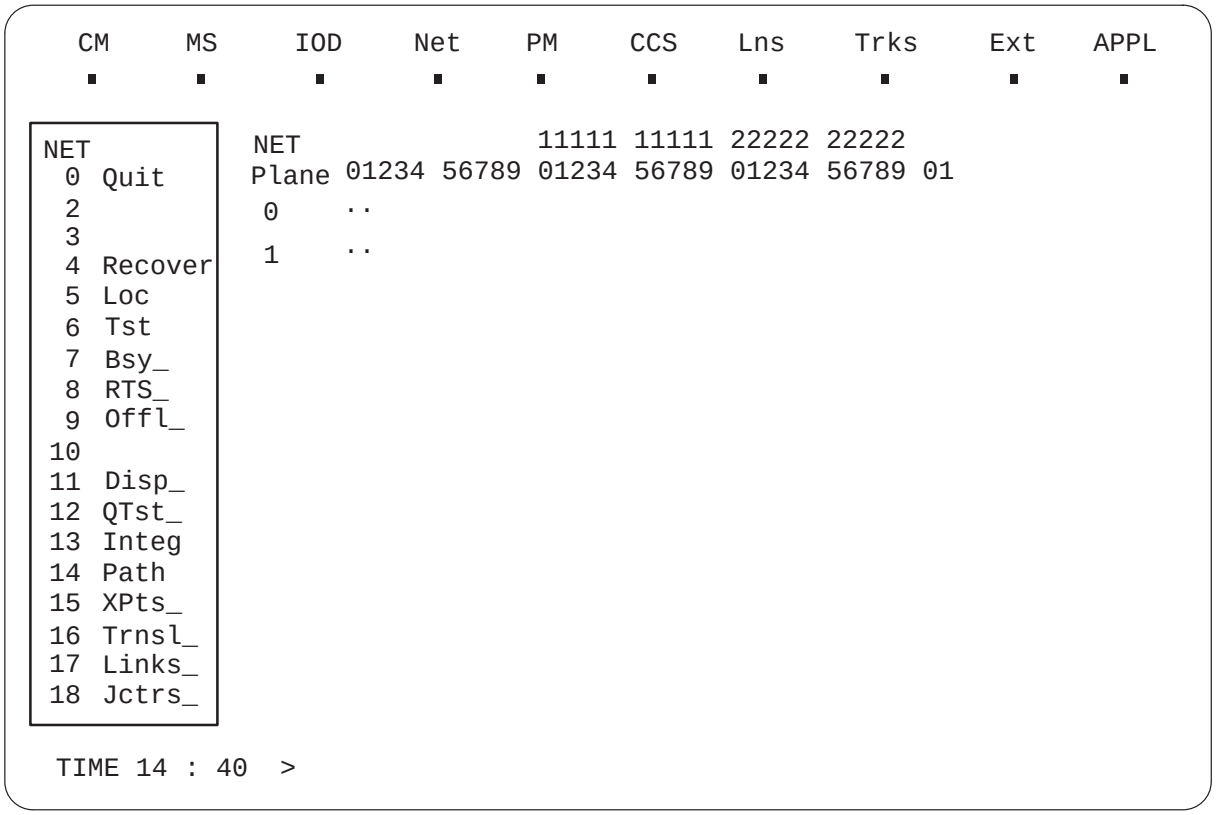
Figure 6-2
Example of DSNE MTC level MAP display

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

MTC                    MTC
 0 Quit
 2 Activity
 3 MTCNA
 4 MTrsys
 5 Bert
 6 Cpstatus
 7
 8
 9 CM
10 MS
11 IOD
12 NET
13 PM
14 CCS
15 Lns
16 Trks
17 Ext
18 Appl

 TIME 14 : 40  >
```

Figure 6-3
Example of Network level MAP display



Note: Refer to appendix F in tables 16-1, and 16-2, for descriptions of status and alarm codes for the DSNE.

The following list summarizes the NET level commands.

BSY command

The BSY command sets an NM to the manual busy (ManB) state.

DISP command

The DISP command is half of a two-part command that displays general information about one or all NMs. One of the following function words: STATUS, COUNT, or CLEAR always accompanies the DISP command.

INTEG command

The INTEG command accesses the NET INTEG level for the number of accuracy failures for each NM. The INTEG command is available in feature package Maintenance Assistance (NTX053AA).

JCTRS command

The JCTRS command accesses the NET JCTRS status level and displays the status of the junctors in both planes of the specified network.

LINKS command

The LINKS command accesses the NET LINKS level for the peripheral module (PM) links to both planes of a specified NM.

LOC command

The LOC command generates a message that gives the location of the specified NM.

OFFL command

The OFFL command sets an NM to the offline state.

PATH command

The PATH command accesses the NET PATH menu and assists in speech path maintenance. The PATH command is present only on switches with feature package Switch Path Diagnostics (NTX885AB).

QTST command

The QTST command displays the current status of the NM under test.

QUIT command

The QUIT command is common to all NET maintenance menus. When you enter the QUIT command, the command causes the level now displayed to change to the next higher level.

Note: The QUIT command is not mentioned in other command descriptions for the DSNE sections of this chapter. The QUIT command is common to all NET maintenance menus.

RECOVER command

The RECOVER command returns all NMs to service.

RTS command

The RTS command tests an NM. If the NM is correct, the RTS command returns the NM to service.

TRNSL command

The TRNSL command translates the NM number to the central message controller (CMC) port number. The TRNSL command displays the number of the CMC port. The NM is assigned to a numbered CMC port, which TRNSL displays.

TST command

The TST command tests a network plane and NM pair, and starts a test of the network module controller (NMC) for the specified NM.

XPTS command

The XPTS command accesses the NET XPTS level. The XPTS command display varies depending on the type of NM in use. The XPTS command displays the XPT status in the same way as the XPTS command at the NET level.

Non-menu network level commands

The following commands do not appear on the NET level menu, but you can enter the commands as if they appear on the menu.

The NET non-menu commands are as follows:

- CHKLNK
- RDBUFF

CHKLNK command

The CHKLNK command alters the firmware peripheral side (P-side) link sensitivity and error byte. CHKLNK does not apply to Network Frame (NT0X48AJ).

CAUTION
Service degradation
The CHKLNK command can affect the service and performance of a switch. You can drop calls in progress. Network links can be system busy (SysB).

CAUTION
Service degradation
The CHKLNK command can affect the service and performance of a switch. You can drop calls in progress. Network links can be system busy (SysB).

RDBUFF command

The RDBUFF command has a maximum of 48 bytes of NM memory buffer.

Menus related to double shelf network components

This section describes the menus and commands related to network components. For a complete description of command parameters and use, refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

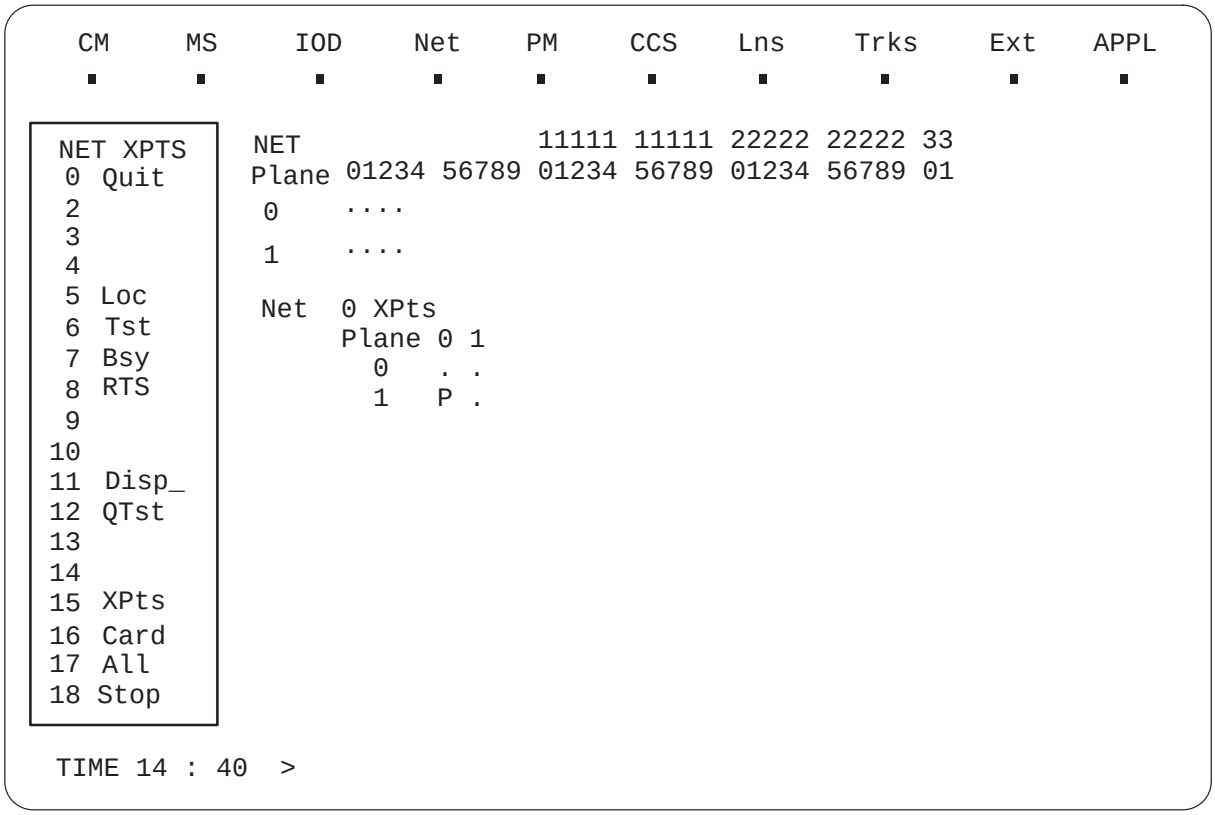
At the NET level, there are menus related to network components. The following is a list of these menus:

- NET XPTS
- NET INTEG
- NET JCTRS
- NET LINKS
- NET PATH

Network crosspoint commands

You can perform problem solving to investigate call-processing problems at the NET XPTS level. The NET XPTS menu contains the commands that are required to clear a crosspoint fault. Figure 6-4 is a sample display of the NET XPTS level.

Figure 6-4
Example of Crosspoint level MAP display



The following is a summary of the NET XPTS commands.

ALL command

The ALL command tests all crosspoint cards in the specified plane of the NM under test.

BSY command

The BSY command sets the specified crosspoint card to the P-side state. The system sets all PM links and junctors connected to the card to the ManB state at the same time.

CARD command

The CARD command specifies the number of the crosspoint card to busy. The ranges are as follows:

- 0–7 for Network Frame cards
- 0–3 for Network Combined (NETC) cards
- 0–1 for DSNE cards

STOP command

The STOP command stops the crosspoint tests on the specified plane.

DISP command

The DISP command displays the status of all the crosspoint cards in both planes of the network. The crosspoints at the NET level specify the crosspoint cards. Use this command with non-MAP devices (like Teletypes).

LOC command

The LOC command displays the location of a crosspoint card according to the plane, card number, and side of the card.

QTST command

The QTST command queries the test state of NM crosspoints and displays the current state of a network test on a specified NM.

RTS command

The RTS command tests a crosspoint card. If correct, the command returns the card to service.

TST command

The TST command controls the tests for the crosspoint cards in an NM.

XPTS command

The XPTS command accesses the NET XPTS level for the crosspoint cards in both planes of the NM.

Network accuracy commands

The NET INTEG menu is a tool you can use to diagnose network faults. In a call between two PMs, NET INTEG identifies paths where faults occur. NET INTEG monitors the network with accuracy codes and test codes.

Accuracy code

In a call, the network sends an accuracy code between two PMs. The system records an accuracy failure when the accuracy code at the receiving end is different from the accuracy code sent.

Test code

The test code card inserts and extracts PCM samples at several points in the the network connection. The test code verifies the continuity of the connection and isolates faults at the card level. A fault counter records any faults discovered by the test code.

Note: You must select and post an NM before you execute any NET INTEG command.

Figure 6-5 is a sample display of the NET INTEG level.

Figure 6-5
Example of NET INTEG level MAP display

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

 NET INTEG
 0 Quit
 2 Post
 3 Mode
 4 Setlog
 5 Trnsl
 6 RstI
 7 Buffsel
 8 Analyze
 9
10
11 Disp_
12 Clear
13 PMS
14 Counts
15 Thresh
16 Logbuff
17
18 Timer
```

```
NET                 11111 11111 22222 22222 33
Plane 01234 56789 01234 56789 01234 56789 01
 0    ..... .
 1    ..... .
Posted Net:  None  Timer:  Enabled    Mode:  Inter
Logbuff Contents:  Net102
disp master
Pair  0  Plane 1   Pair  0  Plane 1   Pair  0  Plane 1
-----------------------------------------------------
0   12        11   11    --      ---  22   --      ---
1    0         0   12    --      ---  23   --      ---
2    0         0   13    --      ---  24   --      ---
3    0         1   14    --      ---  25   --      ---
4    0         0   15    --      ---  26   --      ---
5    2         0   16    --      ---  27   --      ---
6   --        --   17    --      ---  28   --      ---
7   --        --   18    --      ---  29   --      ---
8   --        --   19    --      ---  30   --      ---
9   --        --   20    --      ---  31   --      ---
10  --        --   21    --      ---  Parity + integrity
```

```
TIME 14 : 40  >
```

The following is a summary of the NET INTEG commands.

ANALYZE command

The ANALYZE command analyzes the information in the fault counters and accuracy (parity) buffer, and generates a list of codes for faults. The list shows only the ten links and junctor ports for both ends with the highest counts. The ANALYZE command shows a fault count and location for any card with one or more accuracy (parity) faults. The ANALYZE command shows the function, shelf, slot, and fault counts of the card.

BUFFSEL command

The BUFFSEL command allows operating company personnel to select specific logs for storage in the log storage buffer.

CLEAR command

The CLEAR command clears all counters on the posted plane and pair.

COUNTS command

The COUNTS command specifies analysis of the total number of fault counts for the network cards.

DISP command

The DISP command shows and clears the accuracy failures and fault counters in the buffer. Parity and accuracy faults for each NM plane and pair appear when you execute the DISP command without parameters.

LOGBUFF command

The LOGBUFF command displays the contents of the accuracy buffer.

MODE command

The MODE command specifies one of three modes of pegging network failures.

POST command

The POST command posts a network plane and pair.

PMS command

The PM ports command displays the counts of faults for the PM ports that connects to NM ports.

RSTI command

The reset in-service trouble (ISTb) command resets the displays, but does not clear the fault counters and accuracy buffer. The RSTI command sets all counters back to zero in the selected plane and pair that meet or exceed the threshold. The RSTI command does not affect the counters that are below threshold.

SETLOG command

The SETLOG command enables, or disables the output of network accuracy log messages to a printer. The SETLOG command provides this function for a selected NM plane and pair, or for all NMs.

THRESH command

The THRESH command displays all the fault counters on the selected network plane and pair that reach the threshold limit.

TIMER command

The TIMER command allows operating company personnel to control when to clear counters. The TIMER command can enable, or disable automatic clearing.

TRNSL command

The TRNSL command identifies in which frame and row you can find the card. The TRNSL command identifies the location of a specified card.

Non-menu NET INTEG commands

The following commands do not appear on the NET INTEG menu. You can enter the commands as they appear on the menu.
The non-menu NET INTEG commands are as follows:

- FILTER
- RETH
- TRLNK
- UPTH

FILTER command

The FILTER command allows operating company personnel to query the accuracy (parity) throttle or set the parity throttle on a specified PM basis.

RETH command

The RETH command is the same as the UPTH command but the RETH command resets all thresholds to a count of 250.

TRLNK command

The TRLNK command translates a network pair, link, and channel to a PM and terminal identifier (TID).

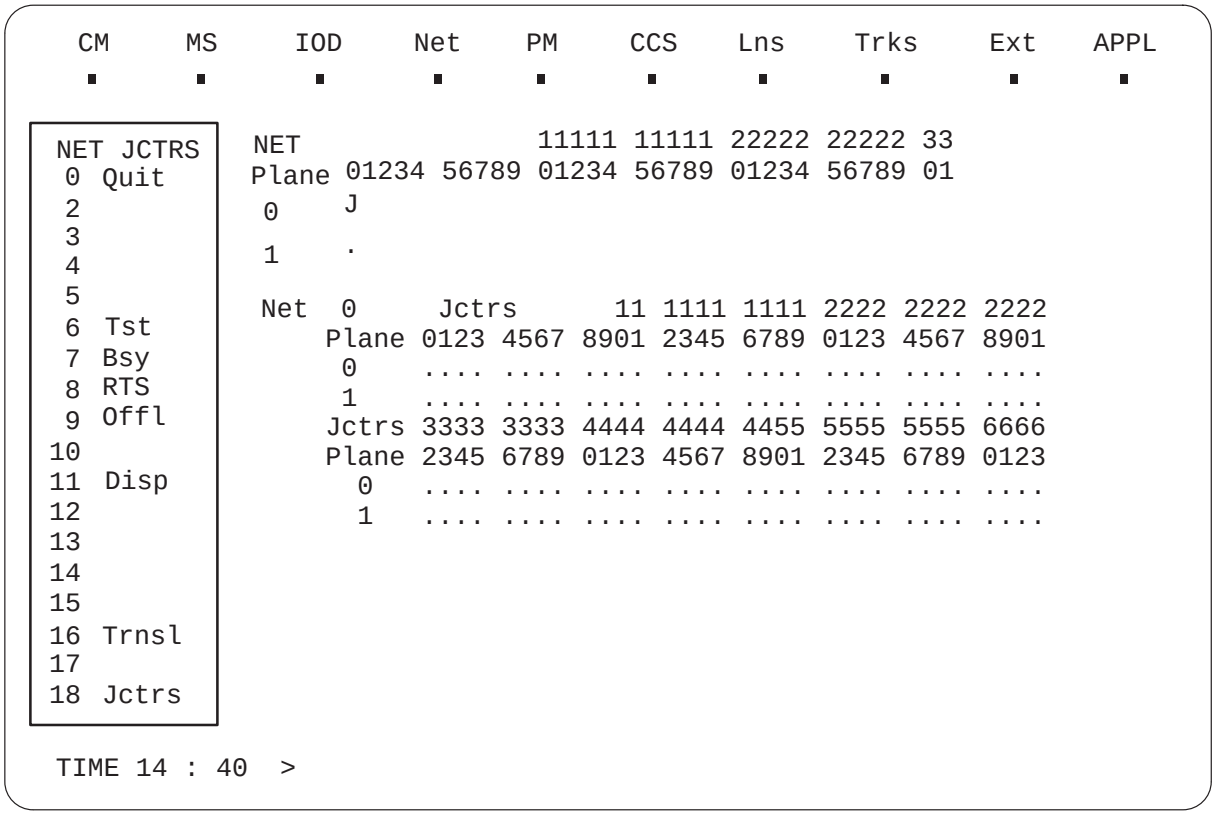
UPTH command

The UPTH command changes the thresholds for the counters. The DISP COUNTS command relies on the counters. The UPTH command allows the default threshold for links, crosspoints, and junctors to be different.

Network junctor commands

The NET JCTRS status display allows operating company personnel to troubleshoot junctor faults within a specified NM. The NET JCTRS display lists the status of the 64 junctor ports of both planes of a NM. The NET JCTRS menu contains the necessary commands to correct a NET JCTRS fault. Figure 6-6 is a sample display of the NET JCTRS level.

Figure 6-6
Example of Network junctors level MAP display



The following is a summary of the NET JCTRS commands.

BSY command

The BSY command busies both ends of a junctor and sets the junctor to the ManB state.

DISP command

The DISP command displays the status of all network junctors or their type.

The type of parameter can be an *S* or an *I*.

The *S* means that the intrajunctors connect the port.

The *I* means that the interjunctors connect the port.

JCTRS command

The JCTRS command displays junctor status in the same method as JCTRS of the NET menu.

OFFL command

The OFFL command sets both ends of a junctor to the offline state.

RTS command

The RTS command tests a junctor. If the test is successful, the RTS command returns the junctor to service.

TRNSL command

The TRNSL command translates a junctor number and identifies the other-end network, type of junctor, and junctor number.

TST command

The TST command tests a junctor and applies the test to the NM specified by the JCTRS command.

Network links command

The NET LINKS display lists the status of the 64 link ports of both planes of an NM. The NET LINKS menu contains the commands required to correct a network link fault. Figure 6-7 is a sample display of the NET LINKS level.

Figure 6-7
Example of Network link level MAP display

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

 NET LINKS
  0 Quit
  2
  3
  4
  5
  6  Tst
  7  Bsy
  8  RTS
  9
 10
 11  Disp
 12
 13
 14
 15
 16 Trnsl
 17 Links
 18

 NET                11111 11111 22222 22222 33
 Plane 01234 56789 01234 56789 01234 56789 01
  0    ....
  1    L

  Net  0    Links      11  1111 1111 2222 2222 2222
      Plane 0123 4567 8901 2345 6789 0123 4567 8901
       0    .... .... .... .... .... .... .... ....
       1    .... .... .... .... .... .... .... ....
      Links 3333 3333 4444 4444 4455 5555 5555 6666
      Plane 2345 6789 0123 4567 8901 2345 6789 0123
        0   .... .... .... .... .... .... .... ....
        1   .... .... .... .... .... .... .... ....

 TIME 14 : 40  >
```

The following is a summary of the NET LINKS commands.

BSY command

The BSY command busies the network P-side link and sets it to the ManB state.

DISP command

The DISP command displays the status of network links, or the type of link.

LINKS command

The LINKS command displays link status in the same method as links at the NET level.

RTS command

The RTS command returns network P-side links to service and tests the specified link. If the test passes, the RTS command returns the link to service.

TRNSL command

The TRNSL command identifies the operating name and number of the PM assigned to the specified link.

TST command

The TST command tests a network link and initiates the netlinks tests. The TST command applies the tests to the NM specified by the command string link pair and specified link.

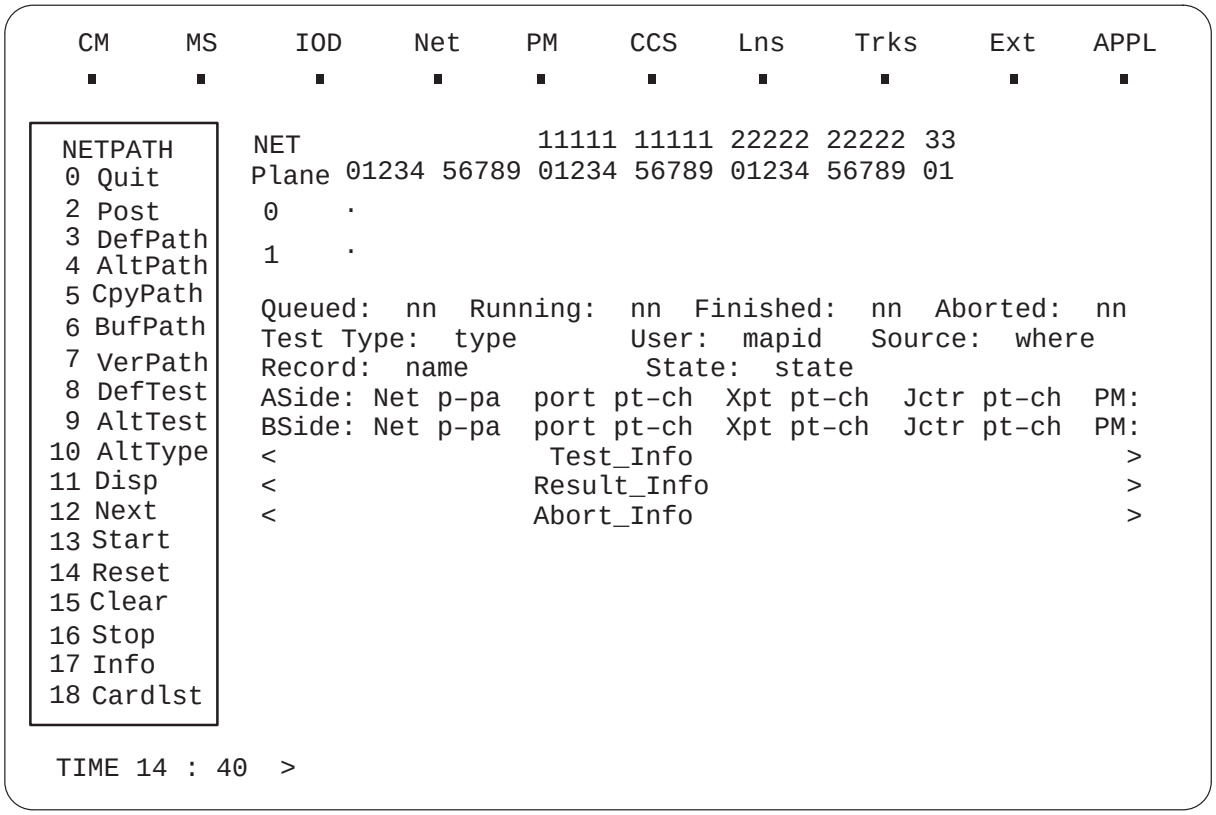
Network path commands

The network path (NET PATH) feature supports network types NETC (NT5X13AA) and DSNE (NT8X11AD). Network type NT5X13AA requires network firmware release 8 or greater. The NET PATH feature does not support Network Frame (NT0X48AJ) because of hardware restrictions. Figure 6-8 is a sample display of the NET PATH level.

The NET PATH tool performs the following actions to assist in speech path maintenance:

- identifies components that have faults that cause accuracy failures.
- confirms that suspect components have faults before you replace the components.
- tests if replacing the components correct the faults.

Figure 6-8
Example of NET PATH level MAP display



The following is a summary of the NET PATH commands.

ALTPATH command

The ALTPATH command alters a section of the path definition but does not change the rest of the path. You must POST the record in the *path data input state.*

ALTTEST command

The ALTTEST command alters the test data for a posted record. You must POST the record in the *test data input* state.

ALTTYPE

The ALTTYPE command alters the test type. Any current test data resets if you issue this command. You must POST the record in the *path data input* state.

BUFPATH command

The BUFPATH command allows you to get a path from the accuracy buffer, or the NET PATH fault buffer. The NET PATH fault buffer stores the

accuracy check traffic simulator paths. You must POST the record in the *path data input* state.

CARDLST command

The CARDLST command displays the locations of all cards between the insertion and removal points for the AUTO test. You define the insertion and removal points.

CLEAR command

Use the CLEAR command to free a test record.

CPYPATH command

The CPYPATH command copies the path data from a current record to the posted record. You must POST the record in the *path data input* state.

DEFPATH command

The DEFPATH command specifies the first path information for a new posted test record. You must POST the record in the *path data input* state.

DEFTEST command

The DEFTEST command defines the test data for the record. You must POST the record in the *test data input* state.

DISP command

The DISP command displays a posted record, or group of records.

INFO command

The INFO command displays a diagram of the cards included in the path under the test. This diagram includes the correct insert and remove points for the office. This display depends on the network type and the junctors that connect the network.

NEXT command

The NEXT command posts the next element in the post set.

POST command

The POST command has two functions. The first function is to create a new test record and provide the commands that define and submit a test. The second function is to specify a test record, or a set of records that display in the status area of the MAP display.

RESET command

The RESET command returns a posted test to a previous state.

START command

The START command starts a test that is defined or reset.

STOP command

The STOP command aborts the posted set.

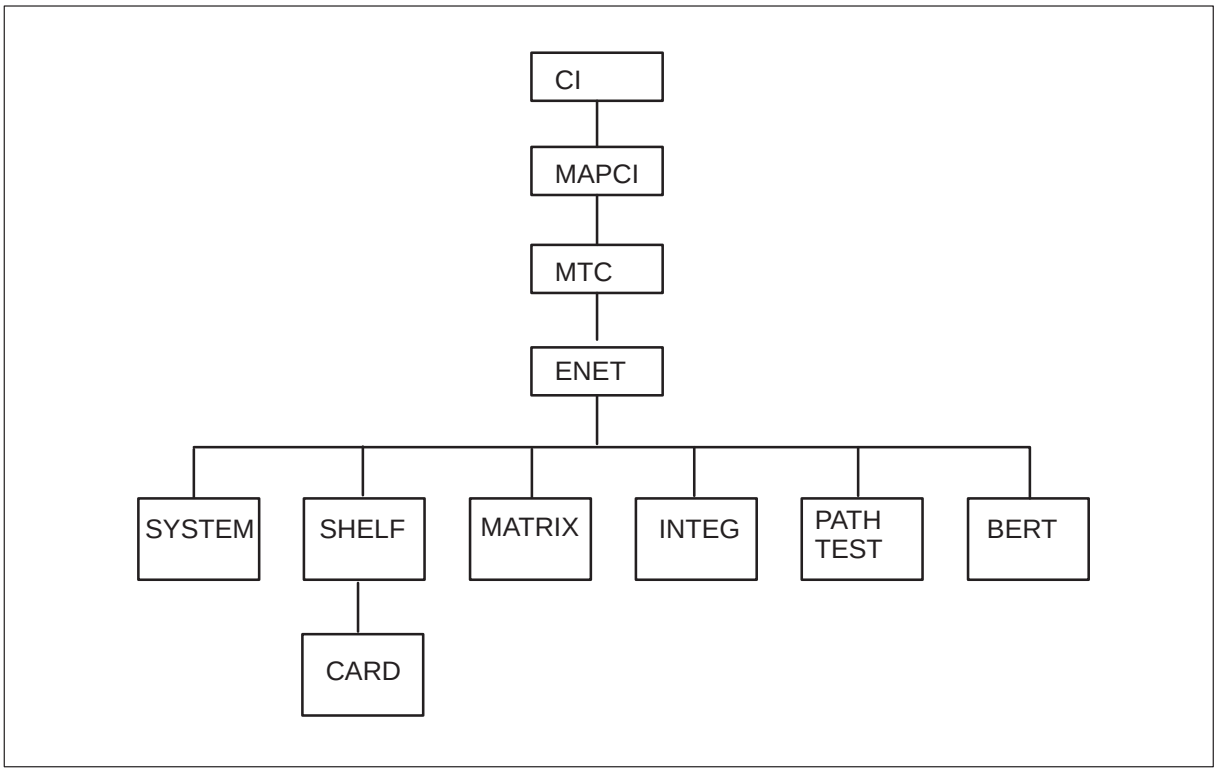
VERPATH command

The VERPATH command verifies that the path data entered is correct. You must POST the record in the *path data input* state.

Enhanced network

The ENET is a standard matrixed time switch. The ENET design achieves high density, low power and does not have switching limits. ENET maintenance facilities are a sublevel of the MTC level of the MAP display. Figure 6-9 represents the ENET maintenance subsystem. From the ENET level, you can go down to the system, shelf, matrix, accuracy, path test, or BERT sublevels. The card level is a sublevel of the shelf level.

Figure 6-9
Enhanced network subsystem

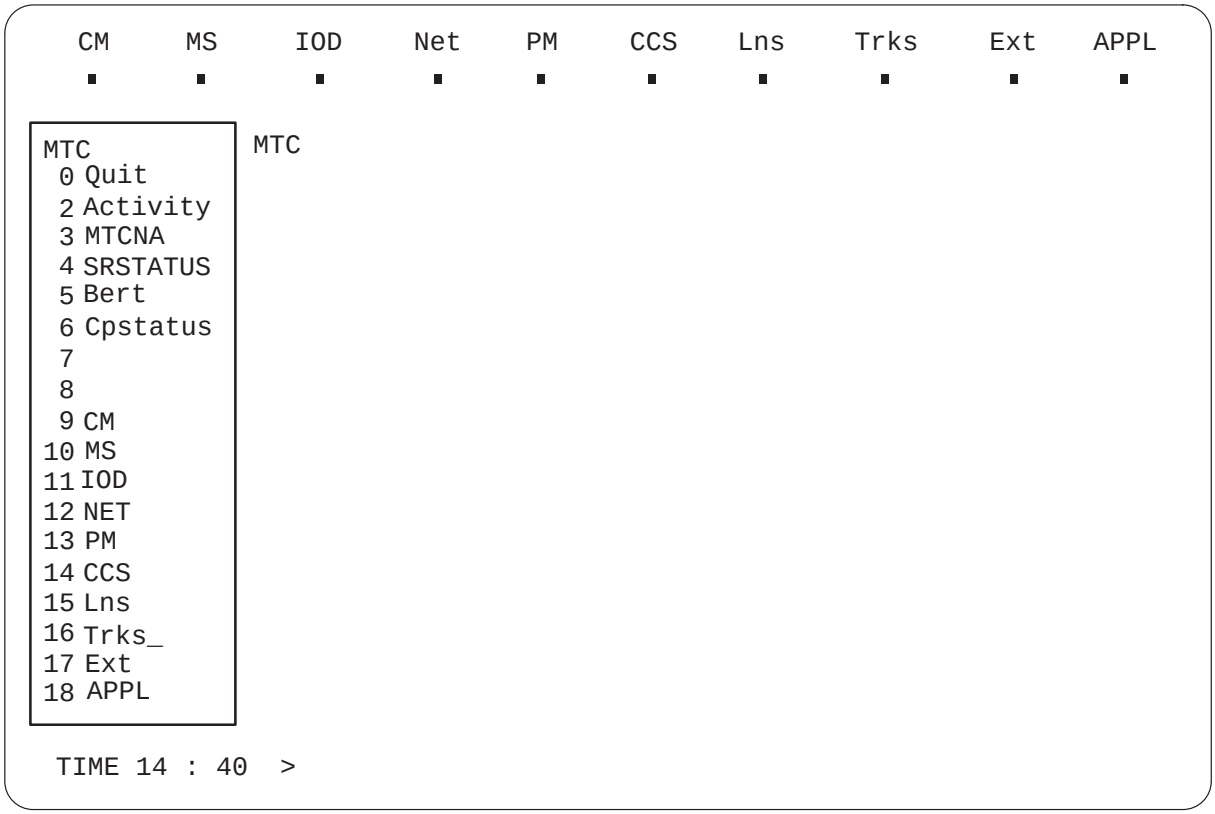


ENET maintenance facilities are a sublevel of the MTC level of the MAP display. Figure 6-10 illustrates the MTC level of the MAP display. To access the MTC level, type

>MAPCI;MTC

and press the Enter key.

Figure 6-10
Example of ENET MTC level MAP display



Improvements

You can now relocate fiber XMS-based peripheral modules (XPM) from one ENET P-side fiber link to another P-side fiber link. You can perform this task without loss of service to the fiber XPM. Modifications to the ENET software facilitate the control of P-side fiber links for each digital signal 30 (DS30). Each digital signal 30 is at the card level of the ENET MAP display.

The fiber XPM remains in-service (InSv) during the procedure. The procedure affects call processing and call outages do occur. Remove and relocate each DS30 equivalent from service on both planes, one at a time.

Call processing is not available on one DS30 equivalent during the time when it is out of service (OOS).

During the transfer procedure, move and take offline each DS30 equivalent. In the PM table control, change the entry of the single DS30 equivalent. On the new link, bring the equivalent back into service. The PM runs in simplex mode until this procedure is complete.

Several commands display at the ENET level and card level. The commands display to permit maintenance action for each DS30 equivalent, or the whole fiber link.

At the ENET level of the MAP display, the output of the following commands changes, but the input does not change.

- FINDSTATE
- SHOWBLOCK

The card level has an optional parameter for several commands. The commands are for use with fiber links from the Quad DS512 Fiber Interface Paddle Board (NT9X40). This parameter is at the card level of the MAP display. This parameter associates with fiber links. This parameter does not appear at the DS30 Interface Paddle Board (NT9X41) card level. This new parameter is an additional number after the link number that is the DS30 equivalent. The fiber links possess the flexibility required to support InSv transfer of fiber XPM. The affected commands are as follows:

- ABTK
- BSY
- OFFL
- QUERYEN
- RTS
- TRNSL
- TRY
- TST

Logs that relate to fiber links change to include DS30 equivalent information. The word *fiber* appears in the log if the reported link is on a fiber link. Maintenance action on a fiber link can be on the whole fiber, or a set of DS30 equivalents within the fiber. When maintenance action is on a set of DS30 equivalents, logs include a list of the affected equivalents. The logs do not provide a list if the maintenance action affects all DS30 equivalents within the fiber.

The following log are affected

- ENET300
- ENET301
- ENET302
- ENET303
- ENET306
- ENET307
- ENET308
- ENET310
- ENET311
- ENET312
- ENET313
- ENET700

Refer to chapter 3 of this document for the causes and the responses for these logs.

Use the ENET level of the MAP display to determine the status of the major components in the network. Use the ENET level of the MAP display to access the sublevels of the MAP display described in table 6-1.

Table 6-1
Sub-levels of the ENET level of the MAP display

Sub-level	Use
BERT	Allows operating company personnel to define and perform bit error rate tests (BERT).
CARD	Allows operating company personnel to control and query the status of a specific card slot or individual messaging links on the slot.
INTEGRITY	Allows operating company personnel to analyze messaging errors which occur along the speech links between the ENET and the PM connected to the ENET.

—continued—

Table 6-1
Sub-levels of the ENET level of the MAP display (continued)

Sub-level	Use
MATRIX	Allows operating company personnel to control and query the status of the ENET crosspoint cards based on their location in the switching matrix.
PATHTEST	Allows operating company personnel to test each path in the network, and through PMs that connect to the network.
SHELF	Allows operating company personnel to control and query the status of the network elements in a specified shelf of the ENET.
SYSTEM	Allows operating company personnel to control and query the network status for each node. Each ENET node has a processing complex. The processing complex consists of the Local Shelf CPU card (NT9X13), the Network Clock and Message card (NT9X36), the Reset Terminal Interface (RTIF) Paddle Board (NT9X26), and the NT9X40.
—end—	

Enhanced network level menu commands

To access the ENET level from the MTC level, type

>NET

and press the Enter key, or choose item 12 from the MTC level command menu.

Figure 6-11 illustrates the ENET level MAP display. The MAP display provides status information on the major operating blocks of the network:

- system cards (processor, RTIF, clock and messaging, and DMS-Bus interface)
- switching matrix
- ENET shelves

The figure lists command descriptions of the menu items in alphabetical order. For a complete description of command parameters and their use, refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

Figure 6-11
Example of ENET level MAP display

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

NET                ENET       System    Matrix   Shelf  0  1  2  3
 0 Quit             Plane 0      .         .             .  .  .  .
 2                  Plane 1      .         .             .  .  .  .
 3 QueryEN
 4 Locate          ENET:
 5 Deload
 6
 7
 8
 9
10
11 RExTst_
12 Bert
13 Integ
14 Pathtest
15 System
16 Matrix
17 Shelf_
18

 TIME 14 : 40  >
```

Note: Refer to appendix A for values of status fields for functional blocks system, matrix, and shelf at the ENET level.

BERT command

Use the BERT command to access the BERT level of the MAP display.

DELOAD command

Use the DELOAD command at the ENET level to query the deload status of all the crosspoint cards in a plane. Use the DELOAD command at the ENET level to control the deload status of all the crosspoint cards in a plane. When you set a plane to a deload status, the system attempts to use the crosspoints in the other plane for call connections. The DELOAD command minimizes the possibility of connection integrity problems. Allow 20 min after you issue the DELOAD command. This procedure allows most of connections in progress on the deloaded plane to complete.

INTEG command

Use the INTEG command to access the accuracy level of the MAP display. Use the integrity level of the MAP display to analyze errors that occur along the speech links. The speech links are located between the PMs and the ENET.

LOCATE command

Use the LOCATE command to display the location of the ENET cabinets and shelves.

MATRIX command

Use the MATRIX command to access the matrix level of the MAP display. The matrix level provides you with maintenance and diagnostic facilities for the switching matrix of the ENET.

PATHTEST command

Use the PATHTEST command to access the path test level of the MAP display. Use the path test level to define and execute tests on separate, one-way paths through the ENET switching matrix. Another option is to use the path test level to define and execute tests through an XPM linked to the ENET.

QUERYEN command

Use the QUERYEN command to determine the number of crosspoints provisioned for each plane. Use the QUERYEN command to determine the switching capacity for each plane.

QUIT command

The QUIT command is common to all ENET maintenance menus. Use the QUIT command to cause the current level to change to the next higher level.

Note: Other command descriptions for ENET sections of this chapter do not mention the QUIT command because the command is common to all ENET menus.

REXTST command

Use the REXTST command to manipulate the normally scheduled routine exercise (REX) test, or to run a manual REX test.

SHELF command

Use the SHELF command to access the shelf level of the MAP display. The shelf level allows operating company personnel to maintain the network on a separate shelf condition. Operating company personnel can obtain information about cards on a specified shelf and alter the state of a card. Another option is that operating company personnel can perform tests on a

card. With the shelf level, operating company personnel can specify maintenance actions on all cards in a specified state on a given node.

SYSTEM command

Use the SYSTEM command to access the system level of the MAP display. The system level of the MAP display allows operating company personnel to maintain the ENET for each node.

Unlisted enhanced network menu commands

The following commands do not appear on the ENET level menu. You can enter the following commands as the commands appear on the menu.

The ENET menu commands that do not appear:

- ALARM
- CONNLOG
- CPU
- DISP
- ENCLOCK
- FINDSTATE
- LOGFORMAT
- MEMORY
- QUERYREX
- SHOWBLOCK
- ZOOM

ALARM command

The ALARM command specifies when the alarms RexOff and ISTb appear under the NET header of the MAP display. Use the ALARM command to control and query the display attributes of the network alarms RexOff and ISTb.

CONNLOG command

Use the CONNLOG command to control or display the status information logs for enhanced network call processing.

CPU command

Use the CPU command to display a summary of system CPU level information for an ENET shelf.

DISP command

Use the DISP command to display the current contents of the ENET level display and the NET header of the MAP display. Use the DISP command for non-MAP devices like Teletypes.

ENCLOCK command

Use the ENCLOCK command to control, or query the clock source for a minimum of one ENET nodes.

FINDSTATE command

Use the FINDSTATE command to locate hardware components in a specified state. You can limit the range of the command to a plane, shelf, or slot.

LOGFORMAT command

Use the LOGFORMAT command to control logs ENET111 and ENET211 when they display in long, or short report format.

MEMORY command

Use the MEMORY command to display a summary of the system memory occupancy for an ENET shelf.

QUERYREX

Use the QUERYREX command to display results of the last run ENET REx test.

SHOWBLOCK command

Displays any shelves, slots, and links that cause, or can cause blockage.

ZOOM command

Use the ZOOM command to access the shelf, or card level that corresponds to the location in the specified crosspoint matrix.

Sublevels of the enhanced network

The remainder of chapter 6 examines the many sublevels of the ENET.

The sublevels are as follows:

- SYSTEM
- SHELF
- CARD
- MATRIX
- INTEGRITY

- PATHTEST
- BERT

System level

The system level of the MAP display allows operating company personnel to maintain the ENET for each node. A processing complex that consists of the following components controls each ENET node. The components are as follows:

- NT9X13 card
- NT9X26 card
- NT9X36 card
- NT9X40 card

Note: A node refers to a single plane, or shelf configuration of the ENET. Plane 0 shelf 3 is an example of a node.

Three versions of the system level are present. The commands available on all three versions are identical. The type of information displayed is different in each version. To access the system level correctly, obtain an *overview* of all the ENET processing complexes. Also, obtain *information* on the use of memory for a specified shelf. Another option is to obtain *information* on the use of the central processing unit (CPU) for the shelf.

You can access the system level from the ENET, shelf, card, matrix levels of the MAP display. You can access the system level from the system level.

To obtain the status overview of all the processing complexes in the ENET, type

>SYSTEM

and press the Enter key.

To obtain detailed information on memory use for a specified shelf, type

>SYSTEM shelfno MEMORY

and press the Enter Key.

(for example, for shelf 1, enter >SYSTEM 1 MEMORY).

To obtain detailed information on processor use for a specified shelf, type

>SYSTEM shelfno CPU

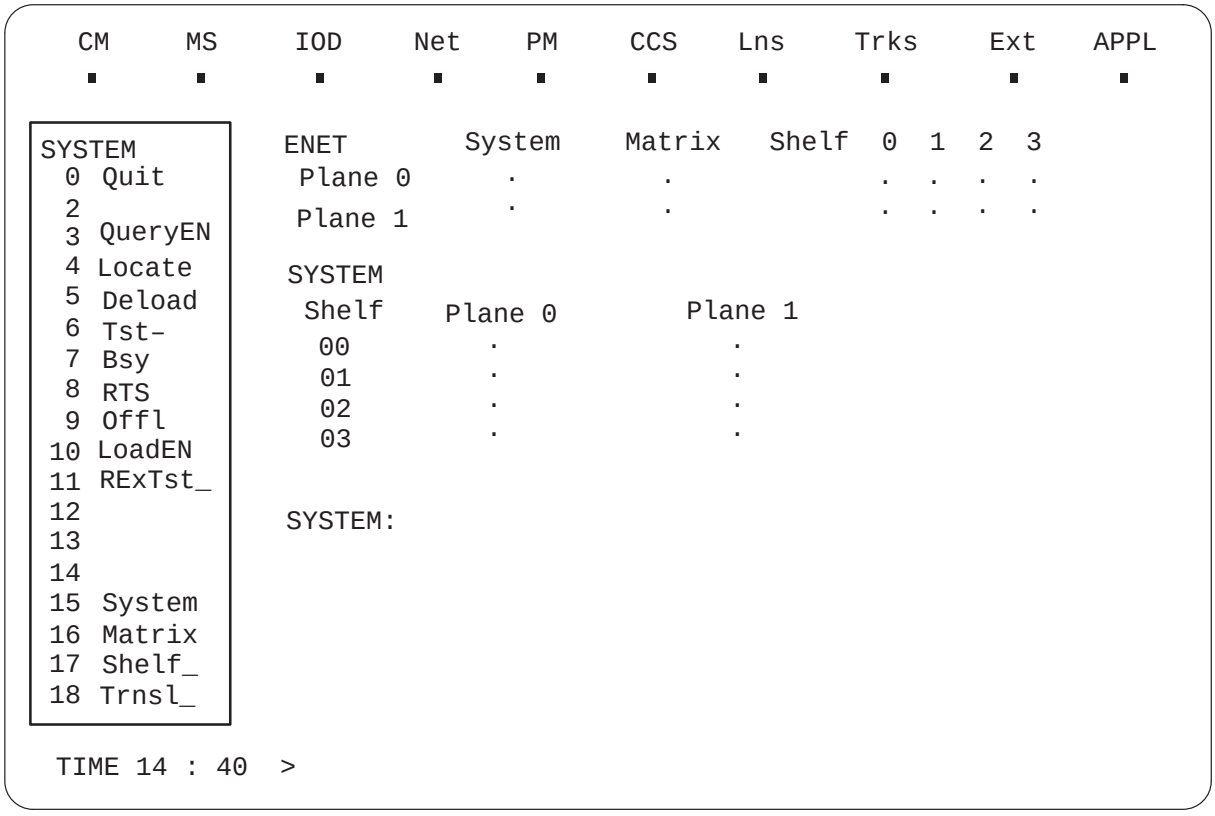
and press the Enter key.

(for example, for shelf 1, enter >SYSTEM 1 CPU).

Display format status overview version

Figure 6-12 illustrates the status overview version of the system level. For information on the fields in this display, refer to appendix B in tables 12-1 and 12-2.

Figure 6-12
Example of status overview version of the ENET System level MAP display



Display format memory use version

Figure 6-13 shows an example display of the memory version of the system level. For an explanation of the fields in this display, refer to appendix B in table 12-3.

Figure 6-13
Example of memory use version of the ENET system level MAP display

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

SYSTEM
 0 Quit
 2
 3 QueryEN
 4 Locate
 5 Deload
 6 Tst_
 7 Bsy
 8 RTS
 9 Offl
10 LoadEN
11 RExTst_
12
13
14
15 System
16 Matrix
17 Shelf_
18 Trnsl_

ENET       System    Matrix   Shelf  0  1  2  3
 Plane 0      .         .             .  .  .  .
 Plane 1      .         .             .  .  .  .

SYSTEM
 Shelf    Plane 0                 Plane 1
  00        .                       .

Loadname ENET35BB                    ENET35BB
Memory (Kbytes)
   Time: 20.03:25                    20:03:25
DS Used: 1819 85%              Used:  1810 85%
  Avail: 325 Total:2144        Avail: 325 Total: 2144
PS Used: 1770 95%              Used:  1770 95%
  Avail:  86 Total:1856        Avail: 86 Total: 1856


SYSTEM:

 TIME 14 : 40  >
```

Display format CPU use version

Figure 6-14 shows an example display of the CPU use version of the system level. For an explanation of the fields in this display, refer to appendix B in table 12-4.

Figure 6-14
Example of CPU use version of the ENET system level MAP display

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

SYSTEM
 0 Quit
 2
 3 QueryEN
 4 Locate
 5 Deload
 6 Tst-
 7 Bsy
 8 RTS
 9 Offl
10 LoadEN
11 RExTst_
12
13
14
15 System
16 Matrix
17 Shelf_
18 Trnsl_

ENET       System    Matrix   Shelf  0  1  2  3
 Plane 0      .         .              .  .  .
 Plane 1      .         .              .  .  .  .

SYSTEM
 Shelf    Plane 0                    Plane 1
  00         .                          .

Loadname ENET35BB                    ENET35BB
Traps
# / min :  0                         0
Total   :  0                         0
# CPU occupancy
Call Pro :  75                       72
 Total  :    80                      81


SYSTEM:

 TIME 14 : 40  >
```

System level menu commands

Command descriptions of the menu items occur in alphabetical order. For a complete description of command parameters and their use, refer to the *Non–menu Commands Reference Manual*, 297-1001-820, and the *Menu Commands Reference Manual*, 297-1001-821.

BSY command

The BSY command removes a minimum of one ENET node from service.

DELOAD command

Use the DELOAD command to query and control the deload status of all the crosspoints in a node. The system attempts to use the node in the other plane of the shelf for call connection. The system will attempt this when you set the crosspoints in a node to a deloaded status.

Note: Use the DELOAD command at the system level before you perform a major manual maintenance action on a node.

LOADEN command

Use the LOADEN command to load software into the memory of an ENET node. The shelf that you will load must be in a ManB state.

LOCATE command

Use the LOCATE command to display the location of ENET processing complex cards.

MATRIX command

Use the MATRIX command to access the matrix level of the MAP display. The ENET matrix level provides you with maintenance and diagnostic facilities for the switching matrix of the ENET.

OFFL command

Use the OFFL command to set the state of the system cards in a node to offline.

QUERYEN command

Use the QUERYEN command to display information about the system cards in an ENET node.

REXTST command

Use the REXTST command to control, or query the system-run REx tests, or to run a manual REx test.

RTS command

Use the RTS command to initiate a return-to-service (RTS) attempt on manual or system busy nodes.

SHELF command

Use the SHELF command to access the shelf level of the MAP display. The SHELF level allows operating company personnel to maintain the network for each shelf. Use the shelf command to obtain information about cards on a specified shelf and to alter the state of a card. Another option is to use the command to perform tests on a card. Operating company personnel can specify maintenance action on all cards in a specified state on a given node.

SYSTEM command

Use the SYSTEM command to access the system level of the MAP display. The system level allows operating company personnel to maintain the ENET for each node.

TRNSL command

Use the TRNSL command to determine which port of both message switches (MS) links to the specified node by a fiber cable.

TST command

Use the TST command to run diagnostic tests on a single ENET node. Another option is to use the command on all ENET nodes in a given plane.

System level non menu commands

The following commands do not appear on the system level menu. You can enter the following commands as they appear on the menu.
The non-menu system level commands are as follows:

- ABTK
- DISP
- LOADENALL
- TRY

ABTK command

Use the ABTK command to abort an in-progress maintenance action on the processing complex of an ENET shelf.

DISP command

Use the DISP command to display the current contents of ENET and system levels of the MAP display. Use the DISP command to display the current contents of the NET alarm banner. This command is for use on non-MAP devices like Teletypes.

LOADENALL command

Use the LOADENALL command to load software into all ManB nodes on one or both planes.

TRY command

Use the TRY command to determine which warnings will be displayed if you enter a command. This command allows operating company personnel to check the potential impact of a maintenance action *before* you perform the maintenance action

Shelf level

To access the shelf level from the ENET, system, or matrix levels, type

>SHELF shelf_number

and press the Enter key.

where

shelf-number is 0 through 3, to specify a given shelf on the ENET

Display format

As figure 6-15 shows, the display for this level includes the display described for the ENET level. Below the display you will find additional shelf-specific information. The slot status fields for each crosspoint card represent two cards. The first card is the crosspoint card in the front of the slot. The second card is the link interface paddle board at the rear of the shelf.

The commands available at the shelf level allow operating company personnel to maintain the card slots of the ENET for each shelf. The display for the shelf level includes status information for all the slots in both nodes of the displayed shelf.

Appendix C in table 13-1 lists possible values for the slot status fields of the shelf level display.

Figure 6-15
Example of shelf level MAP display

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

SHELF          ENET        System     Matrix     Shelf  0  1  2  3
 0 Quit         Plane 0       .          .             .  .  .  .
 2              Plane 1       .          .             .  .  .  .
 3 QueryEN       SHELF 02   Slot      1111111    11122222 22222333 333333
 4 Locate                  123456  78 90123456    78901234 56789012 345678
 5 Deload       Plane 0     .  .  .. ........    -------- ........  . .
 6 Tst          Plane 1     .  .  .. ........    -------- ........  . .
 7 Bsy_          SHELF:
 8 Rts_
 9 Offl_
10
11 RExTst
12
13
14
15 System
16 Matrix
17 Card_
18 Trnsl_

 TIME 14 : 40  >
```

Shelf level menu commands

Command descriptions of the menu items occur in alphabetical order. For a complete description of command parameters and their use, refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

BSY command

The BSY command removes a minimum of one crosspoint card on the selected shelf from service. This command can busy a system card and remove the whole shelf from service.

The following system cards in an ENET node are important to the operation of the node:

- –5V 20A Power Converter (NT9X31) card
- +5V 80A Power Convertor (NT9X30) card
- NT9X13 card
- NT9X26 card
- NT9X36 card

- NT9X40 card

If you busy any of these cards, all system cards in the node can become manually busy that removes the node from service.

CARD command

Use the CARD command to access the card level of the MAP display for a specified slot.

DELOAD command

Use the DELOAD command to query and control the deload status of crosspoint cards in the displayed shelf. The system can attempt to use the crosspoint in the other node of the shelf for call connection. The system uses the crosspoint in the other node when you set a crosspoint in a node to a deloaded status.

LOCATE command

Use the LOCATE command to display the location of a card slot.

MATRIX command

Use the MATRIX command to access the matrix level of the MAP display. The ENET matrix level provides operating company personnel with maintenance and diagnostic facilities for the switching matrix of the ENET.

OFFL command

Use the OFFL command to make sure you cannot access:

- a card slot in either node of a displayed shelf
- all manual busy crosspoints in either node
- all cards in either node

The following system cards in an ENET node are important to operation of the node:

- NT9X31
- NT9X30
- NT9X13
- NT9X26
- NT9X36
- NT9X40

All the cards in a node go offline if you set any of these cards to offline.

QUERYEN command

Use the QUERYEN command to display information about a card slot in an ENET shelf.

REXTST command

Use the REXTST command to control and query the parameters in operation of the system-run REx tests. Use this command to run a manual REX test.

RTS command

Use the RTS command to return a minimum of one crosspoint card on the selected shelf to service. If you specify one of the system cards on the shelf, you can use this command to return the whole shelf to service.

The following system cards in an ENET node are important to operation of the node:

- NT9X31
- NT9X30
- NT9X13
- NT9X26
- NT9X36
- NT9X40

If you return any system card to service in a manually busy node, the system attempts to return the whole node to service.

SYSTEM command

Use the SYSTEM command to access the system level of the MAP display. The system level of the MAP display allows operating company personnel to maintain the ENET for each node.

TRNSL command

Use the TRNSL command to translate the location of an ENET crosspoint card to the corresponding horizontal and vertical matrix coordinates of the card. Use this command to display the MS ports associated with the node that contains a system card.

TST command

Use the TST command to run a series of tests on the specified cards.

Shelf level non-menu commands

The following commands do not appear on the shelf level menu. You can enter the following commands as the commands appear on the menu.

The shelf level non-menu commands are as follows:

- ABTK
- DISP
- TRY

ABTK command

Use the ABTK command to cancel an in-progress maintenance action on a slot. The ABTK command stops any maintenance action except an in-progress change to the ManB state from another state.

DISP command

Use the DISP command to display the contents of the MAP display for the shelf sublevel. Use this command to display the contents of the MAP display for the NET header of the alarm banner. Use this command on non-MAP devices like Teletypes.

TRY command

Use the TRY command to display the warnings that occur if you enter commands. The TRY command allows operating company personnel to check the potential impact of a maintenance action before you perform the maintenance action.

Card level

Use the card level to perform actions on separate hardware elements associated with a specified card slot. Use the card level to retrieve information about separate hardware elements associated with a specified card slot.

Examples of this hardware are:

- a paddle board that occupies the slot
- a message link on the paddle board
- all messaging links in a specified state

To access the card level from the shelf level, or from the card level display for another slot, type

>CARD card_number

and press the Enter key.

where

card-number specifies a slot (1 to 38), in the displayed shelf

Note: Use the ZOOM command to access the card level from the matrix level.

When operating company personnel access the card level, the command menu changes to card-related commands. When operating company personnel access the card level, the system adds card-related status information to the display area. The display area appears under the shelf status information. The card level gives information for both planes like the shelf level. The status display depends on the function of the hardware that occupies the specified card slot.

There are given variants of the card level for the following types of ENET cards:

- power converter cards
- processor card and RTIF
- clock and messaging card, and associated interface
- crosspoint cards and interfaces (DS30 or DS512)

How to maintain ENET system cards

The system cards in an ENET node are as follows:

- NT9X31
- NT9X30
- NT9X13
- NT9X26
- NT9X36
- NT9X40

All system cards in an ENET node are important for the node to operate. If you perform a state change on a system card, you perform the procedure on all the other system cards at the same time. The system cards are in the node. A change to manually busy is an example of this procedure. If you remove a system card from service, you remove the node from service.

Card level for the CPU and RTIF paddle board

Use the card level to maintain the CPU card and the RTIF paddle board of the ENET shelf. Figure 6-16 shows an example card level display for the RTIF card.

Figure 6-16
Example of ENET level MAP display

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

NET                  ENET       System    Matrix   Shelf  0  1  2  3
 0 Quit               Plane 0      .         .             .  .  .  .
 2                    Plane 1      .         .             .  .  .  .
 3 QueryEN
 4 Locate            ENET:
 5 Deload
 6
 7
 8
 9
10
11 RExTst_
12 Bert
13 Integ
14 Pathtest
15 System
16 Matrix
17 Shelf_
18

 TIME 14 : 40  >
```

The status display has two status fields: Processor and RTIF. The fields indicate the status of the processor card. The fields also indicate the reset terminal paddle board on the selected shelf number for each plane. These cards are required for shelf operation and the status of these planes reflects the status of the shelf. Appendix D in table 14-1 describes the values that can appear in these fields.

Card level for the clock/messaging card and clock interface

Use the card level to maintain the clock and messaging card. Use the card level to maintain the DMS-Bus interface paddle board in slot 8 of the ENET shelf. Figure 6-17 shows an example of a card level display for the slot that contains the clock and messaging card.

Figure 6-17
Card level for clock/messaging card and interface

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

CARD          ENET        System     Matrix     Shelf  0  1  2  3
 0 Quit        Plane 0       .           .             .  .  .  .
 2             Plane 1       .           .             .  .  .  .
 3 QueryEN
 4 Locate      SHELF 02   Slot      1111111    11122222 22222333 333333
 5 Deload                123456  78 90123456    78901234 56789012 345678
 6 Tst         Plane 0     .  .  .. ........    -------- ........  . .
 7 Bsy_
 8 Rts         Plane 1     .  .  ..  ........   -------- ........  . .
 9 Offl_
10             CARD 08   Front:     Back        Cside Ports      Clock
11 RExTst                Clock/Msg   I/F          0    1        Source
12
13             Plane 0       .          .        Open   MTCOPEN      0
14             Plane 1       .          .        CLOSED OPEN          1
15 System
16 Matrix_
17 Card_       Card:
18 Trnsl_

 TIME 14 : 40  >
```

The status display for the slot 8 card level has four status fields. The Clock/Msg and I/F fields display the statuses of the front and back of the card slot. The values that can appear in these fields are described in appendix D in table 14-1. The values that appear in the C-side port fields are explained in appendix D in table 14-2. These values indicate the status of the links that connect the ENET shelf to the MS. The Clock source field indicates the MS. The MS is the clock source for the ENET shelf.

Card level for power converter cards

Use the card level to identify and locate the +5V and –5V power converters which occupy card slots 1 through 6 and 33 through 36 on the ENET shelf. Figure 6-18 shows an example of the card level for the –5V power converter in slot 1. Figure 6-19 on page 6-43 shows an example of the card level for the +5V power converter in slot 4. Refer to appendix D in table 14-3 for an explanation of field values.

The card level display area for power converter cards has a single status field on the right of each plane number. This field allows operating company personnel to verify that the system software recognizes the power

converter card. The correct version of the card occupies the card slot. The system reads the version from the identification programmable read-only memory (ROM) chip on the card. The system compares the version to the card version entered for the card slot in table ENCDINV (enhanced network card inventory).

Figure 6-18
Card level for –5V power converter

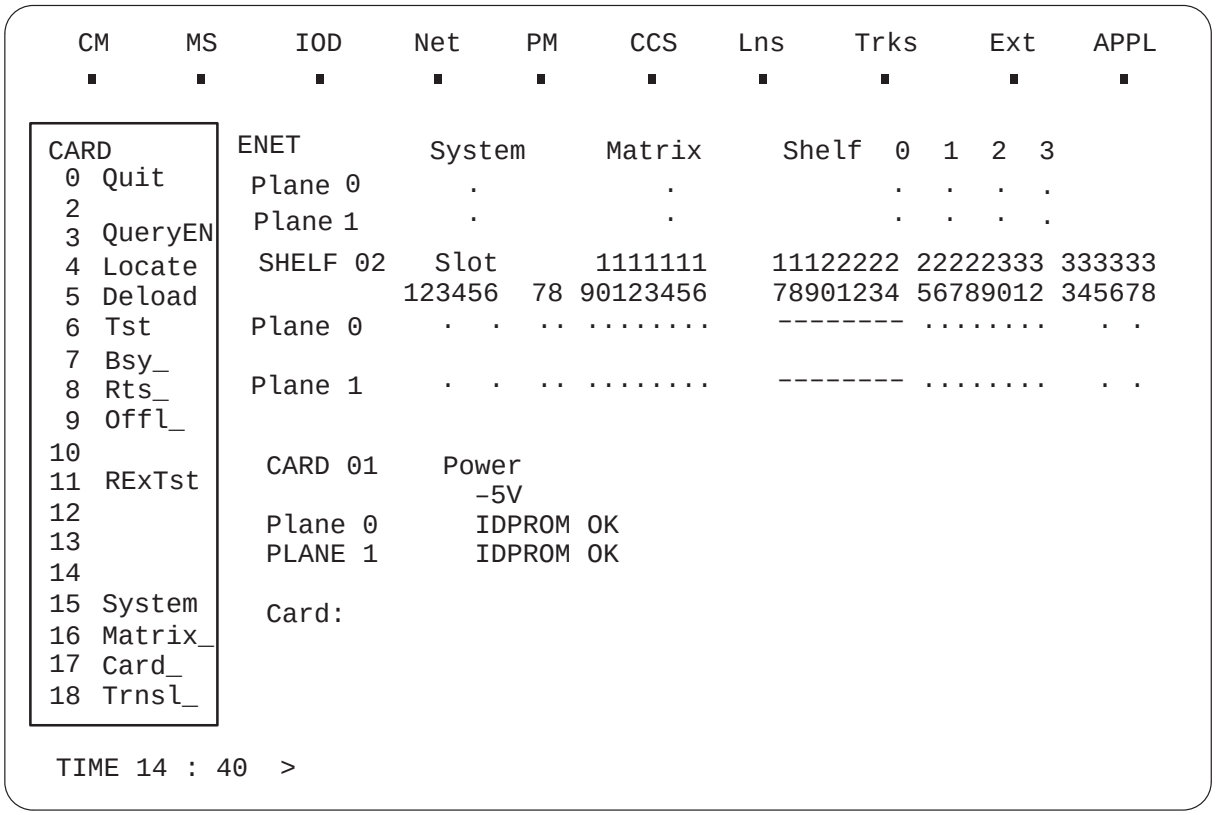


Figure 6-19
Card level for +5V power converter

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

CARD          ENET        System     Matrix     Shelf  0  1  2  3
 0 Quit        Plane 0       .           .             .  .  .  .
 2             Plane 1       .           .             .  .  .  .
 3 QueryEN
 4 Locate      SHELF 02   Slot      1111111    11122222 22222333 333333
 5 Deload                123456 78  90123456    78901234 56789012 345678
 6 Tst         Plane 0    .  .  ..  ........    -------- ........  . .
 7 Bsy_
 8 Rts_        Plane 1    .  .  ..  ........    -------- ........  . .
 9 Offl_
10
11 RExTst      CARD 04    Power
12                          +5V
13            Plane 0       IDPROM OK
14            PLANE 1       IDPROM OK
15 System
16 Matrix_    Card:
17 Card_
18 Trnsl_

 TIME 14 : 40  >
```

How to maintain enhanced network crosspoint and interface cards

Use the card level to maintain crosspoint cards and their associated DS30 and DS512 interface paddle boards, or separate interface links. These cards and paddle boards occupy slots 9 through 32 on the ENET shelf.

The command menu available for crosspoint cards allows operating company personnel to test, busy, RTS, or OFFL exact hardware entities. These entities are associated with the card slot. The entities can include the front (crosspoint card) or back (interface paddle board) of the card slot, or both. Operating company personnel can select separate links on a paddle board, or all links in a given state, like system busy.

Additional commands allow operating company personnel to identify and locate the hardware that occupies the card slot. These commands allow operating company personnel to access other ENET MAP levels.

The card level display for crosspoint cards includes the following status fields:

- front (front of the card slot)

- back (rear of the card slot)
- links (links associated with the card slot)

Note: The Links status field has the title DS30 Links, or DS512 Links. The titles DS30 Links and the DS512 Links are for NT9X41 and NT9X40 link interface paddle boards, in the order given.

Figure 6-20 shows an example of the card level display for a card slot. A crosspoint card and an NT9X41 interface paddle board occupy the card slot. Figure 6-21 shows an example of a card level display for a card slot. A crosspoint card and an NT9X40 interface paddle board occupy the card slot. Refer to appendix D in table 14-4 through 14-6 for an explanation of field values.

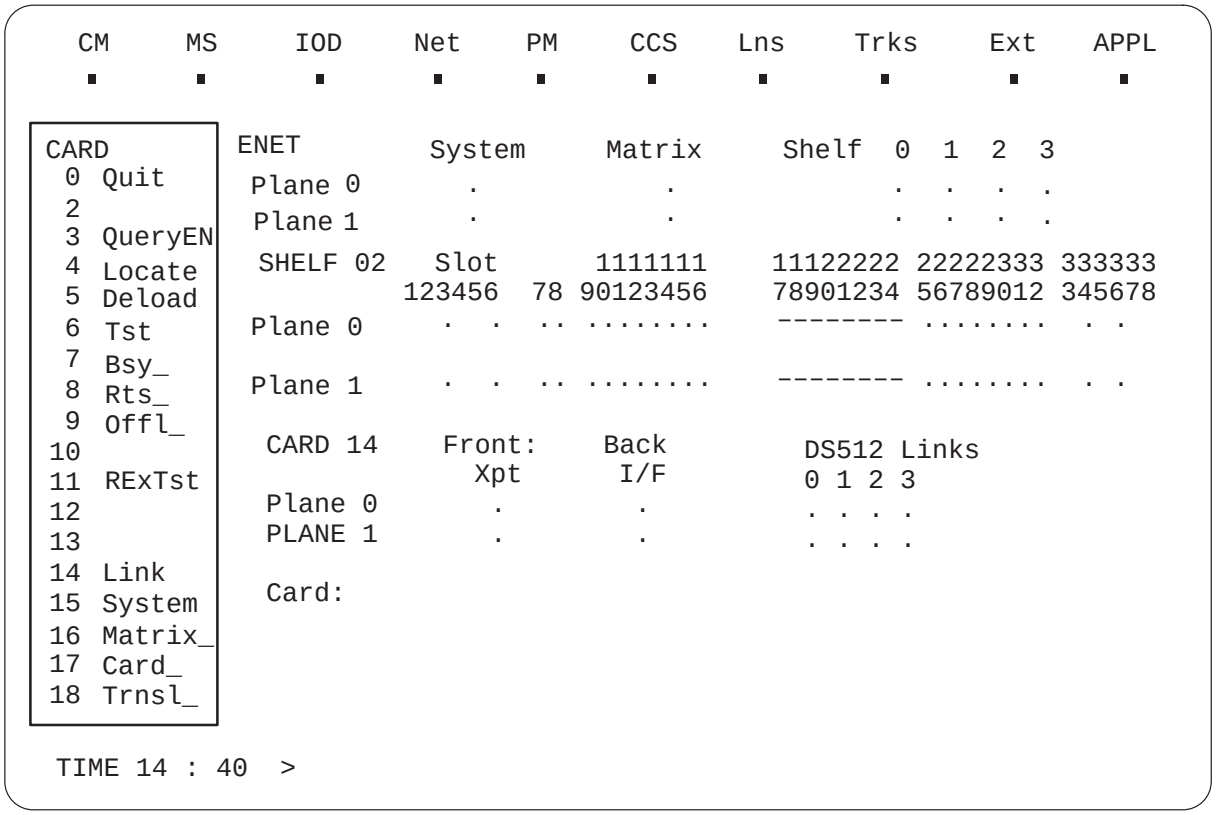
Figure 6-20
Card level for crosspoint card with DS30 interface

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

CARD                ENET        System     Matrix     Shelf  0  1  2  3
 0 Quit              Plane 0      .           .             .  .  .  .
 2                   Plane 1      .           .             .  .  .  .
 3 QueryEN
 4 Locate            SHELF 02   Slot      1111111    11122222 22222333 333333
 5 Deload                      123456  78 90123456    78901234 56789012 345678
 6 Tst
 7 Bsy_              Plane 0     .  .  .. ........    -------- ........  . .
 8 Rts_
 9 Offl_             Plane 1     .  .  .. ........    -------- ........  . .
10
11 RExTst             CARD 14    Front:    Back        DS30 Links 111111
12
13                                 Xpt       I/F          0123456789012345
14                   Plane 0        .         .           ................
15 System            PLANE 1        .         .           ................
16 Matrix_
17 Card_             Card:
18 Trnsl_

 TIME 14 : 40  >
```

Figure 6-21
Card level for crosspoint card with DS512 interface



Card level menu commands

Command descriptions of the menu items occur in alphabetical order. For a complete description of command parameters and their use, refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

BSY command

Use the BSY command to remove ENET cards, paddle boards, or links from service.

CARD command

Use the CARD command to access the card level of the MAP display for a specified slot.

DELOAD command

Use the DELOAD command to query and control the deload status of a crosspoint card. The system prefers the corresponding crosspoint card of the deload card on the other plane to establish connections.

LINK command

Use the LINK command to display the DS30 equivalent for a DS512 link.

LOCATE command

Use the LOCATE command to display the location of the hardware in a minimum of one ENET card slot.

MATRIX command

Use the MATRIX command to access the matrix level of the MAP display. The ENET matrix level provides maintenance and diagnostic facilities for the switching matrix of the ENET.

OFFL command

Use the OFFL command to set the state of an ENET card, paddle board, or link offline.

QUERYEN command

Use the QUERYEN command to display information about an exact hardware entity like a card, or a link.

REXTST command

Use the REXTST command to control and query the parameters for the operation of the system-run REx test. Use the REXTST command to run a manual REx test.

RTS command

Use the RTS command to return the ENET cards, paddle boards, or links specified to service.

SYSTEM command

Use the SYSTEM command to access the system level of the MAP display. The system level allows operating company personnel to maintain the ENET on a separate node.

TRNSL command

Use the TRNSL command to translate the link specified in either the C-side or P-side direction. Use the TRNSL command to determine the logical numbering for the displayed card in the ENET switching matrix.

TST command

Use the TST command to initiate a series of tests on the card, paddle board, or links specified.

Card level non-menu commands

The following commands do not appear on the card level menu. Enter the following commands as the commands appear on the menu.

The card level non-menu commands are as follows:

- ABTK
- ALTTEST
- DISP
- TRY

ABTK command

Use the ABTK command to abort an in-progress maintenance action on the entity specified.

ALTTEST command

Use the ALTTEST command to alter or query the ENET P-side maintenance default parameters.

DISP command

Use the DISP command to display the current contents of the ENET subsystem MAP display. Use the DISP command to display the current contents of the NET header of the alarm banner. You can use this command for non-MAP devices like Teletypes.

TRY command

Use the TRY command to display the warnings that occur if you enter commands. The TRY command allows operating company personnel to check the potential impact of a maintenance action before you execute the command.

Matrix level

The ENET switching matrix is a nonblocking, single stage circuit switch. It supports the connections of call processing PMs for DS512 optical fibers and DS30 copper cables.

To access the matrix level from the ENET, system, shelf, or card levels, type

>MATRIX

and press the Enter key.

Figure 6-22 shows an example of the MAP display for the matrix level. For an explanation of the matrix level fields, refer to appendix E in table 15-1.

Figure 6-22
Example of MAP display for matrix level

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

MATRIX          ENET          System      Matrix      Shelf  0  1  2  3
 0 Quit          Plane 0         .           .              .  .  .  .
 2 Zoom          Plane 1         .           .              .  .  .  .
 3 QueryEN
 4 Locate        Matrix  V-bus Plane 0          V-bus   Plane 1
 5 Deload                   0 1 2 3 4 5 6 7           0 1 2 3 4 5 6 7
 6 Tst            H-bus   0 . . . . . . . .         . . . . . . . .
 7 Bsy_                   1 . . . . . . . .         . . . . . . . .
 8 RTS_                   2 . . . . . . . .         . . . . . . . .
 9 Offl_                  3 . . . . . . . .         . . . . . . . .
10                        4 . . . . . . . .         . . . . . . . .
11 RExTst                 5 . . . . . . . .         . . . . . . . .
12                        6 . . . . . . . .         . . . . . . . .
13                        7 . . . . . . . .         . . . . . . . .
14
15 System       MATRIX
16
17 Shelf
18 Trnsl_

 TIME 14 : 40  >
```

This display provides status information on every element in both planes of the switching matrix. There are eight horizontal bus status fields. The bus status fields show the even and odd horizontal buses for each shelf.

> ***Note:*** Each cross point of a horizontal bus and vertical bus in the display represents a crosspoint card. Each cross point represents the link interface paddle board of the crosspoint card.

Matrix level menu commands

Command descriptions of the menu items occur in alphabetical order. For a complete description of command parameters and their use, refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

BSY command

Use the BSY command to remove ENET crosspoint cards from service.

DELOAD command

Use the DELOAD command at the matrix level to control and query the deload status of elements in the ENET switching matrix. When you deload

a matrix element, the system prefers the corresponding element in the other plane to establish call connections.

LOCATE command

Use the LOCATE command to display the location of a minimum of one crosspoint card on the plane specified.

OFFL command

Use the OFFL command to place a manually busy element of the crosspoint matrix in the offline state.

QUERYEN command

Use the QUERYEN command to display information about the hardware that forms an element of the switching matrix.

REXTST command

Use the REXTST command to control and query the parameters for the operation of the system-run REx tests. Use the REXTST command to run a manual REx test.

RTS command

Use the RTS command to return a SysB, or ManB element of the switching matrix to service.

SHELF command

Use the SHELF command to access the shelf level of the MAP display. The ENET shelf level allows operating company personnel to maintain the network for each shelf.

SYSTEM command

Use the SYSTEM command to access the system level of the MAP display. The system level allows operating company personnel to maintain the ENET for each node.

TRNSL command

Use the TRNSL command and provide the matrix coordinates of a crosspoint card to determine the location of the card. Use the TRNSL command and provide the location of the crosspoint card to determine the matrix coordinates of the card.

TST command

Use the TST command to run diagnostic tests on an element of the ENET switching matrix.

ZOOM command

Use the ZOOM command to access the shelf, or card level that corresponds to the location in the crosspoint matrix specified.

Matrix level non-menu commands

The following commands do not appear on the matrix level menu. You can enter the following commands as the commands appear on the menu.

The matrix level non-menu commands are as follows:

- ABTK
- DISP
- TRY

ABTK command

Use the ABTK command to cancel an in-progress maintenance action on a matrix element.

DISP command

Use the DISP command to display the current contents of the ENET subsystem MAP display and the NET header of the alarm banner. Use this command for non-MAP devices like Teletypes.

TRY command

Use the TRY command to print the warnings that occur if you enter commands that change states. This command allows operating company personnel to determine the potential impact of a maintenance action *before* you execute the maintenance action.

Integrity level

Use the integrity level of the MAP display to analyze errors that occur along the speech links between the PMs and the ENET.

Each PM monitors the integrity of links through the network. To monitor the integrity of links through the network, the PMs exchange pulse code modulation (PCM) samples for calls in progress. The PMs also exchange channel supervision messages (CSM) for signal integrity. If a mismatch occurs, the PMs inform the ENET maintenance system.

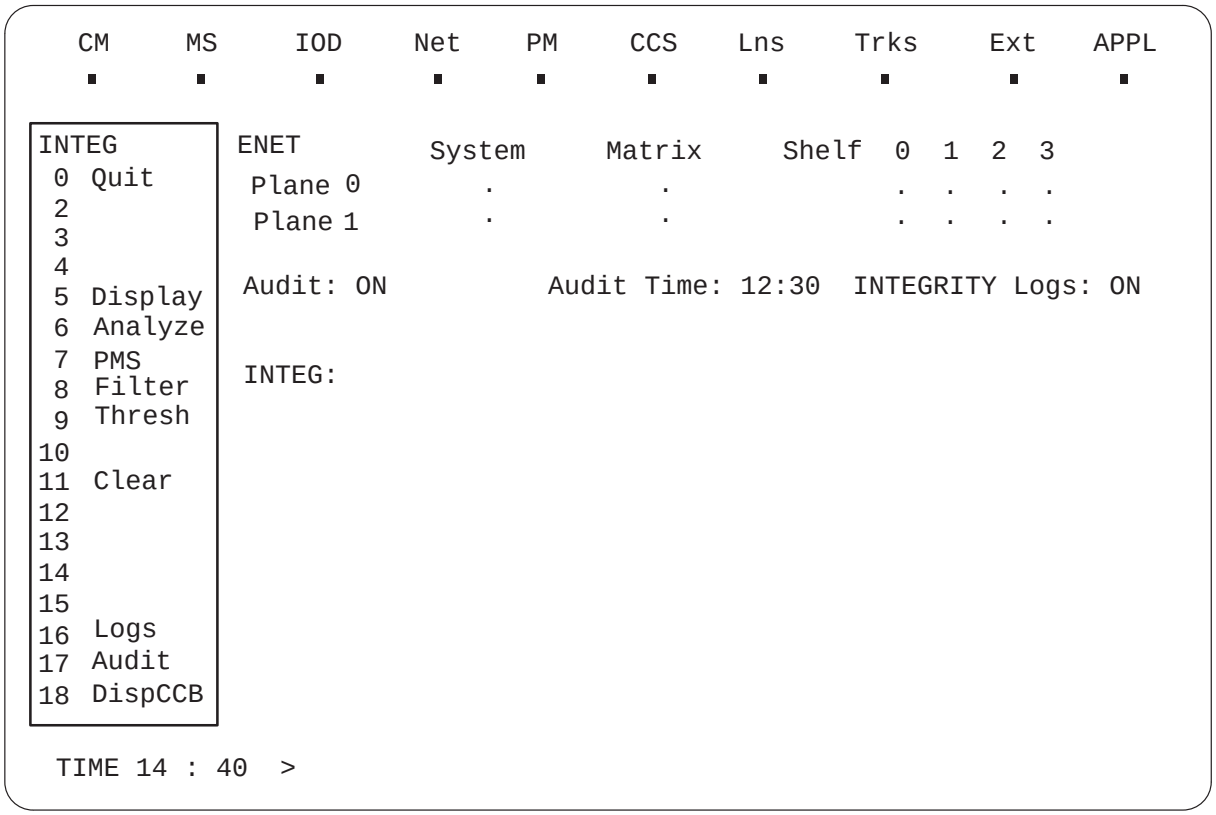
To access the integrity level from the ENET level of the MAP display, type

>INTEG

and press the Enter key, or choose item 13 from the ENET menu.

Figure 6-23 shows an example of the display for the integrity level of the MAP display. The display indicates if the features are enabled or disabled. For headings, Audit and INTEGRITY Logs, the possible values are ON and OFF. The figure displays the time the audit takes to clear the integrity counters.

Figure 6-23
Example of integrity level display



Integrity level menu commands

Command descriptions of the menu items occur in alphabetical order. For a complete description of command parameters and their use, refer to *DMS–100 Family Commands Reference Manual*, 297-1001-822.

ANALYZE command

Use the ANALYZE command to display integrity statistics for all cards on the specified ENET plane.

Note: Appendix E in table 15-2 describes the values that can appear under the shelf status header of the Analyze display.

AUDIT command

Use the AUDIT command to turn the daily integrity audit on or off, or to change the time that the daily audit runs.

CLEAR command

Use the CLEAR command to reset the integrity counters to zero and empty the integrity path buffer.

DISPLAY command

Use the DISPLAY command to view the ENET integrity fault counters for the system, plane, and slot. Use the DISPLAY command to display the contents of the path buffer.

DISPCCB command

Use the DISPCCB command to print the call condense block (CCB) information for the specified call.

FILTER command

Use the FILTER command to query the value of the XPM integrity and parity thresholds. Use the FILTER command to set the value of XPM parity threshold and XPM integrity thresholds.

LOGS command

Use the LOGS command to turn the integrity log reports on, or off.

PMS command

Use the PMS command to display the integrity fault counts for the PM ports connected to the ENET ports.

THRESH command

Use the THRESH command to update, reset, or query the integrity count thresholds.

Path test level

Use the ENET path test level to define and execute tests on separate one-way paths through the ENET switching matrix. Use the ENET path test to define and execute tests on separate one-way paths through an XPM linked to the ENET.

To access the path test level, type

>PATHTEST

and press the Enter key, or choose item 14 from the ENET menu.

Figure 6-24 shows an example of a MAP display for the path test level.

Figure 6-24
Example of path test level

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

PATHTEST          ENET          System     Matrix     Shelf  0  1  2  3
 0 Quit            Plane 0        .           .             .  .  .  .
 2 Post            Plane 1        .         Istb            .  .  F  .
 3
 4 Define         PATHTEST PENding SUSpended RUNning FINished ABorted
 5 Info                    03      00        01      02       00
 6 AltPath
 7 AltTest        PATHTEST:
 8 CpyBuf
 9 CpyPath
10
11 DispBuf
12
13 Snapsht
14 Status
15 Start
16 Stop
17 Clear
18 Reset

 TIME 14 : 40  >
```

The fields of the path test level indicate the number of defined path tests. The fields also identify specified states. The total number of tests defined equals the sum of the five status fields. Five possible test states correspond to the five status fields of the path test level display. Refer to appendix E in table 15-3 for descriptions of the five status fields.

Path test level menu commands

Command descriptions of the menu items occur in alphabetical order. Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822, for a complete description of command parameters.

ALTPATH command

Use the ALTPATH command to alter the path definition section of a test record.

ALTTEST command

Use the ALTTEST command to alter the test options section of a path test record.

CLEAR command

Use the CLEAR command to erase the information from a path test record.

CPYBUF command

Use the CPYBUF command to copy the originating and terminating points of a path from the path saved buffer into the test record specified.

CPYPATH command

You can use the CPYPATH command to copy the test record of a defined test to a new test. You can also use the command to overwrite the path section of a current test.

DEFINE command

Use the DEFINE command to define the parameters for the operation of a path test. You must specify a name for the test and a path definition that consists of a pair of path ends. You can use optional parameters to change the supplied default options for a test.

DISPBUF command

Use the DISPBUF command to display the current contents of one of the following buffers:

- path saved buffer
- integrity buffer
- BERT buffer

INFO command

Use the INFO command to display path definition, test option, and result information. The INFO command can display a single test record, all defined tests, or all tests in a specified state.

POST command

Use the POST command to access the path test post level for a test record. This command is a sublevel of the path test level. This command provides control of a single posted record.

RESET command

Use the RESET command to return a test that is in the aborted or finished state to the pending state.

SNAPSHT command

Use the SNAPSHT command to capture data from the integrity or BERT buffer. The command writes the data into the buffer for the path test level.

START command

Use the START command to initiate a test in the pending state.

STATUS command

Use the STATUS command to query test state information. Operating company personnel can request state information for all tests, or for a specified test. Operating company personnel also can request a display of the names of all tests in a specified state.

STOP command

Use the STOP command to stop a test that is in the running state.

BERT level

The ENET BERT level of the MAP display provides a facility for operating company personnel to perform network BERTS.

The BERT level supports the definition of eight BERT records. A maximum of five of these tests can run at the same time. As a result, several users can use BERT level at the same time.

To access the BERT level from the ENET, type

>BERT

and press the Enter key, or choose item 12 from the ENET command menu.

To enter the BERT level and automatically post a defined BERT test, type

>BERT test_number

and press the Enter key.

where

test_number is 0 through 7, to specify a defined BERT

Figure 6-25 shows an example of a MAP display for the BERT level. Refer to appendix E in table 15-4 for an explanation of BERT level status fields.

Figure 6-25
Example MAP display for BERT level

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

 BERT          ENET          System     Matrix     Shelf  0  1  2  3
 0 Quit          Plane 0       .           .             .  .  .  .
 2 Post          Plane 1       .           .             .  .  .  .
 3 Display
 4 Define      BERT 0   Observed     Elasped      Percent    Optimum
 5 Clear
 6 Start              Error Rate  Time (hhh:mm)  Complete  Error Rate
 7 Stop                  10E-09      001:30          50       10E:09
 8
 9
10
11              BERT:
12
13
14
15
16
17
18

 TIME 14 : 40  >
```

BERT level menu commands

Command descriptions of the menu items occur in alphabetical order. Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822, for a complete description of command parameters.

CLEAR command

Use the CLEAR command to perform the following actions on a BERT record:

- clear all information in the BERT record.
- clear any given port from the BERT record.
- clear any user definition from the BERT record.

DEFINE command

Use the DEFINE command to perform the following actions:

- initialize a BERT record that is not defined.
- add user definitions to the BERT record. Ports specified in this method are considered for inclusion in the connection map, if BERT starts as a USER type test.
- set the looparound type for following user definitions.
- write hit information for a completed BERT to the corresponding BERT buffer.

DISPLAY command

Use the DISPLAY command to obtain information about a specified BERT, or about all BERT records.

POST command

Use the POST command to select a BERT record as the current test record. If you post a command, the following actions occur:

- The status fields of the BERT level MAP display reflect information that relates to the posted BERT.
- For any command that requires you to enter an optional BERT number, the posted record switches to the default BERT.

START command

Use the START command to start a defined BERT.

STOP command

Use the STOP command to stop a BERT in the running state.

Network-related card requirements

Circuit card removal and replacement procedures can be stand-alone procedures or they can become part of a larger procedure. As a stand-alone procedure, you insert a spare circuit into a unit to make sure that the card functions correctly. You can also use card replacement steps as a part of a larger procedure, for example, alarm clearing.

Refer to *Card Replacement Procedures* for descriptions of card replacement procedures for the double shelf network equipment (DSNE) and the enhanced network (ENET).

Problem isolation and correction

You must maintain a network that is accurate, correct, and free from faults. Network performance is a key element for desired switch performance.

Description of problem solving procedures

To maintain a clean network, monitor the network performance. Operational measurements (OM), log report, and alarms indicate the network performance and any problem conditions.

The OMs monitor and count events in the system. The OMs can detect current and potential system problems. You can use log reports as an analysis tool to provide detailed information on call errors, diagnostic results, and system status. Audible and visual alarms indicate that you must take correcting action. The level of the alarm (minor, major, or critical) indicates alarm severity and corresponding need for correcting action.

The following sections of this chapter discuss:

- fault location and clearance
- fault isolation tests
- diagnostic tests
- product-specific test tools

How to locate and clear faults

This section describes fault location and clearance in terms of problem indicators and problem conditions. Table 8–1 lists problem indicators for the enhanced network (ENET) and the double shelf network equipment (DSNE).

Table 8-1
Network problem indicators

Problem indicator	Meaning	Tool
OMs for ENET and DSNE:		
ENETMAT	Monitors the performance of ENET matrix cards.	Refer to *Operational Measurements Reference Manual*.
ENETOCC	Provides information about the central processing unit (CPU) occupancy of each in-service (InSv) ENET.	Refer to *Operational Measurements Reference Manual*.
ENETPLNK	Monitors the performance of ENET peripheral side (P-side) links.	Refer to *Operational Measurements Reference Manual*.
ENETSYS	Monitors the performance of the ENET system cards.	Refer to *Operational Measurements Reference Manual*.
NETMSG	Monitors the use of network message services.	Refer to *Operational Measurements Reference Manual*.
NMC	Counts maintenance errors and failures.	Refer to *Operational Measurements Reference Manual*.
OFZ	Summarizes the arrangement of traffic that arrives at an office. Summarizes the first routing, and the routing of outgoing traffic.	Refer to *Operational Measurements Reference Manual*.
PM2	Provides information on the performance of two-unit peripheral modules (PM).	Refer to *Operational Measurements Reference Manual*.

—continued—

Table 8-1
Network problem indicators (continued)

Problem indicator	Meaning	Tool
TM	Counts errors, faults, and maintenance state changes for trunk modules (TM), maintenance trunk modules (MTM), and remote service modules (RSM).	Refer to *Operational Measurements Reference Manual*.
TS	Records the use of the P-side time switches.	Refer to *Operational Measurements Reference Manual*.
Log reports:		
ENET logs DSNE logs		Refer to the *Log Report Reference Manual*. Refer to the *Log Report Reference Manual*.
ENET alarms:		
Net CBsy major	A minimum of one ENET node is in a central side (C-side) state. A blocked messaging path to the DMS-bus component causes a C-side busy ENET node to be out of service.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net CBsy major”.
Net CdPr critical	A minimum of one card pair is OOS in an ENET shelf.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net CdPr critical”.
Net CSLk minor	A C-side link from an ENET node to a message switch (MS) is OOS.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net CSLk minor”
Net ISTb on a crosspoint card	A crosspoint card in the ENET has problems and remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net ISTb on a crosspoint card”.

—continued—

Table 8-1
Network problem indicators (continued)

Problem indicator	Meaning	Tool
Net ISTb on a link	A P-side link component of the ENET has problems and remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net ISTb on a link”.
Net ISTb on a system card	A minimum of one system card is within an ENET node has problems, but remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net ISTb on a system card”.
Net LOAD	You cannot open the image file. The table PMLOADS contains wrong entries or the file has faults.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net LOAD minor”.
Net MBCd	The number that precedes MBCd indicates the number of crosspoint cards that are manually busy (ManB). The system generates this alarm in response to manual action on a minimum of one ENET component.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net MBCd minor”.
Net MBsy minor	A minimum of one ENET node is ManB. The number that precedes MBsy indicates the number of nodes that are ManB.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net MBsy minor”.
Net PSLk minor	A minimum of one P-side link between the ENET and a PM is OOS.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net PSLk minor”.
Net REX minor	A routine exercise (REx) test runs on the plane of the ENET. The number that follows *REX* indicates the plane of the ENET.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net REX minor”.

—continued—

Table 8-1
Network problem indicators (continued)

Problem indicator	Meaning	Tool
Net RExSch minor	The system disabled automatic REx testing through entries in table REXSCHED.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net RExSch minor”.
Net REXOff no alarm	A scheduled REX test was manually disabled.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net REXOff no alarm”.
Net SBCd major	The system removed a minimum of one crosspoint card from service.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net SBCd major”.
Net SBsy major	The system removed a minimum of one ENET node from service.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net SBsy major”.
Net Shlv critical	Both planes of an ENET shelf are OOS.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net Shlv critical”.
No alarm	A component in the ENET has problems, but remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net ISTb no alarm”.
DSNE alarms:		
Net Bsy minor	The specified number of network modules (NM) are in the ManB or C-side state.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net Bsy minor”.
Net ISTb minor	The indicated number of NMs are in the InSv state.	Refer to *Alarm and Performance Monitoring Procedures*. See section “Net ISTb minor”.

—continued—

Table 8-1
Network problem indicators (continued)

Problem indicator	Meaning	Tool
Net Jctr minor	The alarm indicates the number of network junctors that are in one of four states. The four states are system busy (SysB), ManB, C-side busy, and P-side busy.	Refer to *Alarm and Performance Monitoring Procedures*. See section "Net Jctr minor".
Net Link minor	The number of NMs indicated have links that are in one of the following states: SysB, C-side busy, and ManB.	Refer to *Alarm and Performance Monitoring Procedures*. See section "Net Link minor".
Net Pair critical	The number of NM pairs indicated are OOS.	Refer to *Alarm and Performance Monitoring Procedures*. See section "Net Pair critical".
Net SysB minor	The number of NMs indicated are SysB.	Refer to *Alarm and Performance Monitoring Procedures*. See section "Net SysB minor".
—end—		

Fault isolation tests

This section describes fault isolation tests for the DSNE and ENET.

Two-shelf network equipment

The Digital Multiplex System (DMS) has a maintenance level named INTEG. The INTEG maintenance level can isolate a transient network integrity fault to a card. The INTEG analysis program identifies paths between connected PMs where errors occur. The errors consist of an integrity byte mismatch or parity errors that the maintenance system detects. The INTEG status program stores information on paths that have faults in fault counters and integrity buffers. The network (NET) log system can display the information in the counters and buffers. The MAP display also can display the information.

The DSNE tests consist of two groups: InSv and OOS tests. Perform the InSv tests while the NM is in the InSv state. The InSv tests do not affect the NM call processing ability. The OOS tests require the NM to be in the ManB or SysB state.

In-service tests

You can use the command TST to perform InSv tests at the NET level when the NM state is InSv. The InSv group consists of the following tests.

Loopback message test

This test checks each central message controller (CMC) link. If one link fails, the status code under the header CMC changes from InSv to SysB. If both links fail, the system generates the Log NET104. If either link passes, the InSv test continues.

P-side processor communication test

This test checks the P-side processor and confirms acceptance and execution of the message. If the test fails, the network status changes to SysB. Log NET112 indicates the cause of the failure.

C-side buffer test

This test checks for defects in the buffer used for the integrity and parity counts. The integrity and parity counts are for the network combined (NETC) (NT5X13AA) and DSNE (NT8X11AD). The buffer test does not run, if you use the command RTS FORCE. If the test fails, the network plane status changes to in-service trouble (ISTb). If you manually executed the failed test, the number and location of the faults appear with a card list of the cards that have faults.

Out-of-service tests

The OOS tests consist of a large series of tests. The following tests occur in sequence. The tests occur at the NET level when the NM state is SysB or ManB, and you use the TST command.

Reset functionality test

This test checks if the C-side and P-side processors are correctly reset when the system sends a reset message. The system sends a looparound message, and confirms that the message arrived at the specified address. Reset messages set the processors to zero to confirm that the reset functions operate correctly.

Buffer check

This test checks tests for mismatches of values in the network internal buffers.

Loopback message test

The loopback message test is the same as the InSv loopback test.

C-side buffer test

This test cycles through different C-side buffer locations in the C-side processor card. This test checks if the buffers retain *zeroes* and *ones*.

P-side functionality test

The P-side functionality test determines if the P-side processor (NT3X75BA) functions. Network type NTOX48AJ is an exception. For network NTOX48AJ, the P-side functionality test tests the buffer read and write functions of the P-side processor (NT3X23AB).

P-side processor communication test

The P-side processor communication test is the same as the equivalent InSv test.

Clock port switchover test

If both CMC links are OK, you must perform this test. This test switches the synchronization of the network clock card for the current CMC to the mate CMC. The test switches the synchronization back from the mate CMC. If the test fails on the RTS command, the NET maintenance header shows ISTb. The NM is set InSv.

Basic connection memory test

This test verifies access of the network module controller (NMC) to the connection memory on each crosspoint card.

Basic interface cards test

This test verifies NMC access to test code insertion and removal points on each interface card. The interface card is on the peripheral and junctor faces.

Basic crosspoint cards test

This test verifies test code insertion and removal on a path through each equipped crosspoint card.

NET crosspoint tests

When you use the TST command, the system applies the network crosspoint tests to the crosspoint codes in network types NT5X13AA and NT8X11AD. The crosspoint codes are at the NET XPTS level. Perform the tests on the NM specified by the XPTS command at the NET level. To avoid interference with call processing, the specified NM must be in the ManB state before you execute the TST command.

Firmware crosspoint card test

The system performs this test on a specified side of an NM, when you enter the TST CARD command. This test sets up a connection between the first

stage time switch and the second stage time switch of a specified crosspoint card. The specified NM and side contain the specified crosspoint card. This test verifies correct connection between time switch stages and helps to guarantee correct access and integrity.

Firmware crosspoint test all crosspoint

This test is like the TST CARD sequence. The exception is that the system applies this test to all crosspoint cards in both sides of the specified NM when you enter the TST ALL command. The system performs a quick test of all crosspoint cards for permanent failures. After this test, the system uses this test code to perform detailed tests on every crosspoint card in the NM.

NET link tests

The system performs network links tests at the NET LINKS level when you use the command TST or RTS. The system applies the tests on a specified NM, plane, and P-side link number. You can run the tests on links in the OK or ManB state. You can test the links at the same time. You cannot test the same link on both planes at the same time.

Three types of link tests occur: two types for speech and one type for message. The tests vary according to the type of PM that connects to the network. The tests also vary according to the type of signals that the link accepts. You can use link signals for both message and speech or speech only.

To check the message channel of a link, send a looparound message. The loop around message travels from the central control (CC) to the associated PM and back to the CC. Speech tests are in two formats according to the type of PM.

Integrity loopback

The system establishes a loopback connection between the network and a PM. The network and PM must both be InSv. The PM sends and receives an integrity signal on a channel of a link. The test confirms integrity when the PM receives the same signal as the signal loops back from the network.

Speech looparound

A PM on node type line trunk controller (LTC) establishes a loop-back connection. This connection occurs on channel 16 of the network. The network uses the specified link and the PM channel 16 looparound to send and receive a test code signal. The network selects channel 16 because the system uses channel 16 only for interperipheral message links in offices that have Common Channel Interoffice Signaling No. 6 (CCIS6).

NET junctor tests

When you use the commands RTS or TST, the system performs the NET junctor tests at the NET JCTRS level. The tests apply to a specified NM, plane, and junctor number. You can run the tests on junctors in the InSv or ManB state.

The junctor test sequence first finds a path from the A-side of the specified NM (called the FROM network). The path runs through an idle junctor channel to the B-side of the same or another NM (called the TO network). If the system cannot find a path for the test, the test terminates and the message: `TEST ABORTED--reason` appears.

The system sets up transmit and receive connections between the FROM and TO networks and verifies the selected path. If the system cannot verify the test path, the system frees the connection and terminates the test. The message: `TEST ABORTED--reason` appears. If the system confirms verification, the test continues.

After the system verifies the test path, the test cards in the FROM and TO networks perform test code insertion and search. The test code insertion and search occurs between the A-side originating port and the B-side terminating port.

If the test fails over the full path, the system repeats the test over small segments of the path. The system continues to repeat the test until the test identifies the failing stage. The message `TEST FAIL` and a card list appears at the MAP display. The system also generates Log NETM126 that provides the reason for the failure with associated data.

Enhanced network

Use the ENET path test level to define and execute tests on separate one-way paths. The paths run through the ENET switching matrix, or through an XMS-based peripheral module (XPM) linked to the ENET.

How to use path tests

The path test level provides a method to perform fault isolation and integrity verification on the ENET components of a speech path.

To perform fault isolation, run a path test along a one-way path through the ENET switching matrix.

If the system detects errors during the test, the system returns a list of suspected hardware that has faults with the test results. You can replace these cards and run the test until the test passes.

Run path tests in response to the following problem indicators:

- integrity faults, indicated by the ENET integrity auditor. You can use path tests to pinpoint the source of the integrity error. Use information directly from the integrity buffer to pinpoint the service of the integrity error.
- errors detected during a network bit error rate test (BERT). A path test can determine if a network component that has faults is the source of the error. The path test uses information directly from one of the BERT buffers to determine the source of the error.
- any other suspect paths in the ENET switching matrix you detect or the the system indicates.

The required form of a path test is the insertion of data at an input point of the ENET switching matrix. The required form is also a check of the integrity of the data that the system returned to an output point. The input and output points are on ENET link interface paddle boards. The test definition specifies the pulse code modulation (PCM) channels the test uses.

The user can define the type of path that the test data takes during the test. You can use a path test to test a connection through the ENET switching matrix, a PM attached to the ENET, or both.

Note: The connection established by all types of path tests is a one-way connection. The system does not perform a loopback of the test data. A two-way connection requires the use of another path in the switching matrix. If you use another path, you use additional hardware components. This procedure is not a supported option for an ENET path test.

Three types of path tests occur:

- NET (internal network test option)
- P-side (ENET interface p-side test option)
- LOOP (ENET interface loop test option)

Note: You can define and submit path tests that use the same path at the same time. The system automatically places the tests in a queue and will run the tests in a sequence.

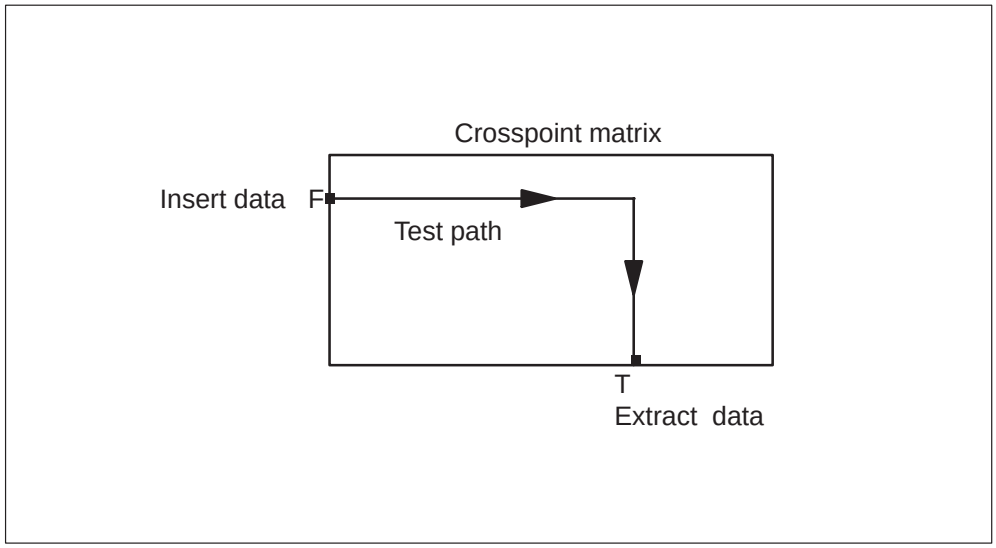
The NET test option

Use the NET test option to test a single one-way path through the ENET switching matrix.

As illustrated in figure 8-1, this test inserts test data at a user-specified originating end point (F) which you can specify. The test extracts this data

at a terminating end point (T). These endpoints, or *path ends*, define a path through the ENET switching matrix.

Figure 8-1
Net test option



Parameters

The operating company personnel supply a test path and can change the supplied default test options. For a NET test, these test options include the following:

- duration – the length of time that the test will run
- data type – a user-specified value that is constant, or random data supplied by the system.
- test data – the data used for the path test
- threshold – the maximum number of allowable hits or data errors for the test
- setup connection – a flag that indicates if you need to establish the connection along the path.

Note 1: NET is the default test option for a path test.

Note 2: The NET test is the only path test option that allows you to test all channels on a crosspoint card.

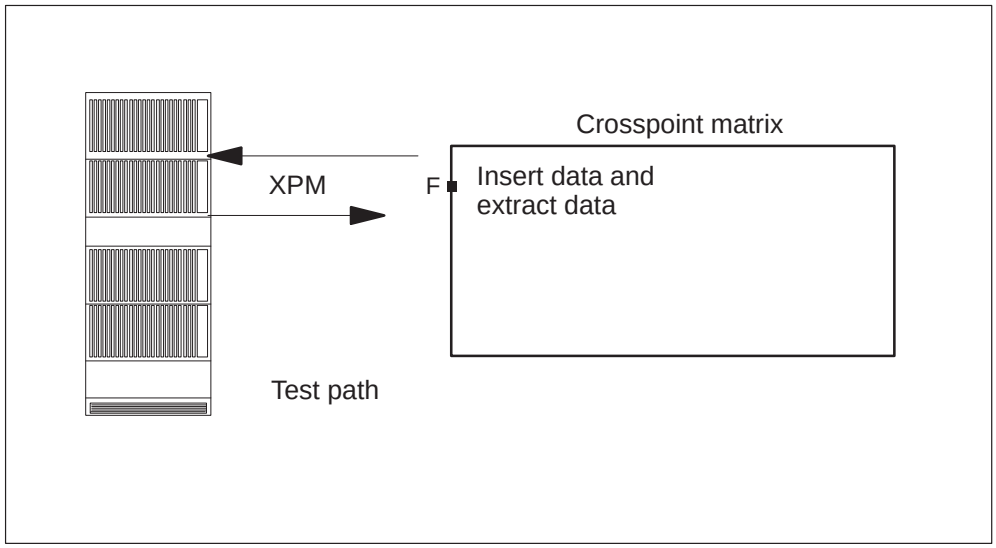
Note 3: The NET test is the only path test option that allows you to test a fiber end. The NET test is also the only test option that allows you to test all 512 channels of a DS512 fiber link.

The P-side test option

Use the P-side test option to establish a test path. The test path starts from an originating end point on a link interface paddle board. The path runs through a PM with an XPM, and back over a link to the originating point.

As illustrated in figure 8-2, this test inserts test data at a user-specified originating end point (F). The data travels on the links to a PM and returns to the same point (F) for removal.

Figure 8-2
P-side test option



Parameters

The operating company personnel supply an originating path end and can change the supplied default test options. A P-side test includes the following:

- duration – the length of time that the test will run
- data type – a user-specified constant value or random data supplied by the system.
- threshold – the maximum number of allowable hits or data errors for the test

Note 1: The P-side test option does not allow you to test a fiber end. An example of a fiber end is a block of 511 PCM channels that form the DS512 fiber link.

Note 2: The P-side test option does not allow you to test all available channels on a crosspoint card.

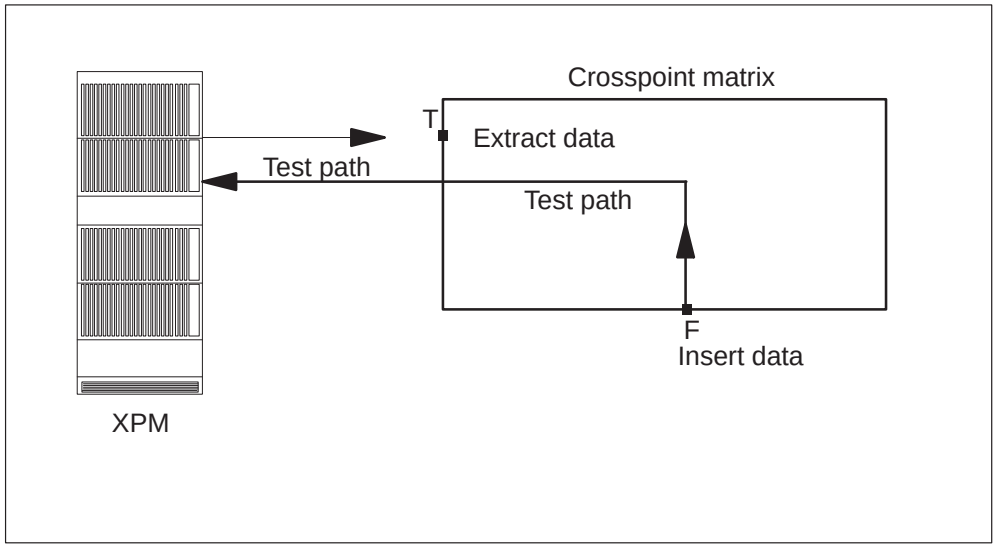
Note 3: You must set the setup connection flag to NO for a P-side test.

The loop test option

Use the loop test option to test a complete one-way path. The integrity auditor monitors this path. This test includes the path through the ENET switching matrix. The test also includes the links through a PM with an XMS-based processor.

As illustrated in figure 8-3, this loop test inserts test data at a user-specified originating end point (F). The test data travels a path through the switching matrix, and the test inserts the test data on to the links to a PM. The test data returns to a terminating end point (T) for removal.

Figure 8-3
Loop test option



Parameters

The operating company personnel supply an originating path end and can change the supplied default test options. A LOOP test includes the following:

- duration – the length of time that the test will run
- data type – this data can be a user-specified constant value, or random data supplied by the system.
- threshold – the maximum number of allowable hits or data errors for the test

Note 1: The LOOP test option does not allow you to test a fiber end. For example, this option does not allow you to test the block of 511 PCM channels that form the DS512 fiber link.

Note 2: The LOOP test option does not allow you to test all available channels on a crosspoint card.

Test preemption

The system can preempt ENET path tests for the following reasons:

- The connection of the path is not set up. The operating company personnel did not specify a setup connection.
- The maximum number of permitted hits or data errors for the path test exceeds the threshold.
- A card on the path is not equipped.
- A specified card on the path is OOS.

In each of these examples, the system cancels the test.

A system maintenance action of higher priority that requires hardware components in the test path can cancel the test in progress. The path test resumes automatically when the higher priority process completes. The test continues to run for the amount of time that remains from the point of cancellation. Refer to table 8-2 for ENET path test commands.

Table 8-2
ENET path test commands

Command	Description
ALTPATH	Alters the path definition section of the path test record.
ALTTEST	Alters the test options section of a path test record.
CLEAR	Erases information from a path test record.
CPYBUFF	Copies the originating and terminating points of a path from the saved buffer into the named test record.
CPYPATH	Copies the path test record of a defined test to a new test record.
DEFINE	Defines the parameters for the operation of the path test.

—continued—

Table 8-2
ENET path test commands (continued)

Command	Description
DISPBUF	Displays the current contents of one of the following buffers: • path save buffer • integ buffer • BERT buffer
INFO	Displays path definition, test option, and result information. These displays are for a single test record, all defined tests, or for all tests in a specified state.
POST	Accesses the path test post record level for a test record.
RESET	Returns a completed test back to the pending state.
SNAPSHT	Captures data from the integrity or BERT buffer and writes the data into the path test level path saved buffer.
START	Initiates the testing sequence.
STATUS	Queries test state information.
STOP	Stops a test that is in progress.
—end—	

Diagnostic tests

This section describes diagnostic tests for the DSNE and ENET.

Double shelf network equipment

For all networks other than the NT0X48AJ network, two types of OOS diagnostics occur. The CC software completely controls one type of OOS diagnostic. This diagnostic performs a basic test of the network. You can begin the diagnostic with the TST command from the NET level of the MAP display. You can use this diagnostic when you test a network that is OOS. The second diagnostic is a firmware-driven self-diagnostic. The diagnostic provides a full test of the crosspoint cards and connection memories. Use this test only for the XPTS section of the NET level of the MAP display. This test can require one hour to complete. The duration of the test depends on the network type and office configuration.

Four basic types of link diagnostics occur. The diagnostic varies according to PM type, and if the link is a combined message and speech link or speech only link. The following is a list of the four types of link diagnostics.

On message links, the CC sends the message. The PM loops the message to the CC.

On the speech links of TMs, digital carrier modules (DCM), and line modules (LM), the system sets up a looparound connection in the network. The system requests a channel in the PM to transmit a specified integrity value. The PM looks for this integrity value to loop back through the network. The channel that you test on the link depends on the entry of the PM. The system cannot seize C-side channels of specified service circuits and trunks. The MAP display response indicates if you ran this test on a speech link. The PM must be InSv to run these link diagnostics, but the network link can be InSv or OOS.

On speech links to an LTC or LTC variants, the system sets up a looparound in the PM. The network sends a test code through the PM looparound and checks for reception of this same test code. The network uses channel 16 for this diagnostic because the network uses this channel only for interprocessor message links in CCIS6 offices. On this channel, trunk entries or trunk states will not normally block the diagnostic. This test does not completely use the whole channel supervision message (CSM) path.

The LTC has a more complete link diagnostic to use the whole CSM path. The diagnostic is like the integrity looparound diagnostic for the TM, but tests all channels on the link. This test requires that the link pair be set ManB to run. This diagnostic will run automatically when you perform a link diagnostic and the link pair is OOS. The diagnostic runs instead of the test code looparound.

Integrity analysis package

The integrity analysis section of the NET level of the MAP display is a tool you can use to diagnose network faults. NET INTEG is an optional software package. The NET INTEG feature identifies paths where faults occur when the system establishes a call between two PMs.

The integrity logs can show correlation to each other according to the state of an office, the integrity failure mode and location. The general manual mode of analysis is to review all integrity logs for a set period of time. The purpose of this review is to look for a pattern in the network paths and PMs involved. When you find a pattern, identify and change the correct network or PM cards involved. The test runs more traffic, and checks to see that the problem with the paths improved.

Network error counters

You can use different error counters that the network firmware supports to analyze network problems. In general, these counters display error conditions and display 0 during normal, error-free operation.

Network firmware link sensitivity monitor

Implement the non-menu NET level command CHKLNK to manipulate this function. As the system scans PM ports or as message transactions occur, the firmware checks that the system follows normal digital signal DS30 link protocols. If the system violates the protocol, the firmware takes special action.

FILTER, is a non-menu command that is part of the NET INTEG level. Filter alters the integrity or parity error threshold level (or both) in the specified XPM. When this command reduces the threshold value, the problem identification sensitivity increases. This increase makes the need for problem repair activity greater.

Enhanced network

This section describes the following diagnostic tests:

- in-service
- out-of-service
- matrix
- REx tests

In-service tests

In-service tests are a group of tests that do not effect the normal messaging of the DMS-Bus, the ENET, and peripherals. In-service tests are not destructive software. In-service tests verify the basic sanity of the system cards. The following information describes in-service tests.

Address hold register test

This test generates a bus error and checks the address hold register to see if the address is latched.

Data cache memory test

This test uses the data logic and access circuits.

Low memory check

This test is required to check the amount of memory left in the software load.

Memory access unit test

This test is required to check the memory access protection, data cache access, and bus timing.

Memory controller test

This test determines the controllers ability to detect 2-bit errors and correct single-bit errors.

Memory protection access test

This test makes sure that the different access protections can be enabled or disabled.

Read identification programmable read only memory test

This test compares the identification programmable read-only memory (ROM) on the cards with table ENCDINV (enhanced network card inventory).

Read-only memory checksum test

This test calculates a checksum over ROM and compares the checksum with the value defined earlier.

Remote terminal interface card in test

This test checks if the remote terminal interface (RTIF) card is present.

Remote terminal interface read status test

This test indicates the subsystem clock status, CPU clock status, and RTIF status. The register checks if any error flags are present.

Remote terminal interface self-test

This self-test checks the different components of the RTIF card, like the microcontroller.

9X36 sanity test

This test checks the sanity of the clock and message card.

9X36 clock test

This test writes a phase offset value to the phase control register. The test also checks if the card can track or sync to the phase control register.

Out-of-service tests

These out-of-service tests include all of the in-service tests in addition to some destructive tests. Out-of-service tests detect faults or secure the sanity of the ENET before the ENET is RTS. The following describes out-of-service tests.

Fault indication register test

This test checks if the system can detect and latch interrupts for more diagnostics.

Interrupt mask test

This test verifies that the system can mask and unmask all the interrupts.

Interrupt handler test

This test checks if the system can recognize each interrupt. The test also determines if the system can implement the corresponding interrupt service routine.

Matrix test

The matrix test verifies the condition of the crosspoint cards. The matrix test consists of the following three tests:

- horizontal bus test
- vertical bus test
- matrix test

Horizontal bus test

This test verifies the link between a set of crosspoint cards on the same horizontal bus. This test verifies the correct operation of the horizontal bus interface circuitry and the horizontal bus components of the backplane. This test also makes sure the system correctly transmits and receives the data on the horizontal bus.

Vertical bus test

This test checks the link between a set of crosspoint cards on the same horizontal bus. This test verifies the correct operation of the vertical bus interface circuitry and the vertical bus connectors. This test also ensures that the system correctly inserts data into and extracts data from the vertical bus.

Matrix test

This test verifies the action between all of the crosspoints of a single plane. This test is a complete diagnostic. There are two types of matrix tests: an in-service test and an out-of-service test. You can specify an in-service test on crosspoint cards that are InSv. You must run an out-of-service test on either ManB or SysB cards.

REX test

The REX test is an audit driven test that you can implement at the MAP display manually. The system can also implement the test by a time programmed in advance. You can also disable the test completely. If you

manually implement this test, then the condition of the ENET is not important. If the ENET is ManB, then the system REX test will not test that node.

The system implements this test after the DMS-Core component and the DMS-Bus component complete the REx tests. The system must implement this test before the XPM starts to test. The system performs the REX test for each plane. The system tests only one plane each day. If the plane correctly completes the test, the system tests the other plane the next day. If the plane does not complete the test, the system repeats the test on the same plane. The REx test consists of two tests: a node out-of-service and a matrix test.

Node out-of-service test

The node out-of-service test causes the ENET shelf to go SysB, unless the ENET shelf is already SysB. This test performs a node reset test for each message switch (MS) line on that node. This test verifies that each ENET shelf C-side link can synchronize with the MS.

Matrix test

This REx *matrix test* is the same as the matrix test but there is also a test that verifies the pseudo-random data checker. This additional test verifies that the pseudo-random data checker and generator on each bus interface are working. The system inserts the pseudo-random data errors into the data stream, and checks the other bus interfaces on the bus to verify that the interfaces observed the errors. Perform this test as an additional test within the vertical and horizontal bus tests.

Product specific test tools

This section describes test tools for the DSNE and ENET.

Double shelf network equipment tools

This section describes the product specific test tools for the DSNE.

Integrity check traffic simulator (ICTS)

The integrity check traffic simulator test tool is available in feature package Switch Path Diagnostics (NTX885AB). The integrity check traffic simulator assists in speech path maintenance. The simulator identifies paths that have defects caused by hardware components. The integrity check traffic simulator uses call processing resources. To simulate traffic, the simulator sets up connections on call paths between networks and the PMs associated with them. After the system reports integrity failures, the PMs involved in the connections continuously check integrity on the same plane. Because the system increments integrity counters at each check, large integrity counts identify the paths that have faults.

Integrity check traffic simulator tests use call processing resources and can compete with call processing for network paths. To avoid this competition, run this test only when traffic is low. Integrity check traffic simulator is a manual test. All the commands available with integrity check traffic simulator are non-menu commands. To access these commands enter the ICTS command at any level of the CI, MAPCI, or MAP display.

Operation

The system sets up integrity check traffic simulator connections only on links that you specify. If the specified links meet the integrity check traffic simulator requirements, the system marks the links as available for integrity check traffic simulator connections. The integrity check traffic simulator scans the set of configured links until the simulator finds two available channels. Then the integrity check traffic simulator establishes network to PM connections, and the PMs as the pathends begin to check integrity. When an integrity failure occurs, the PM reports the failure sends a message to the CC and then the PM switches network planes. The CC verifies that the connection belongs to the integrity check traffic simulator. The CC increases the integrity count against the PM and the network hardware that reported the failure. Finally, the CC generates log NET100 or NET102.

The integrity check traffic simulator makes sure that the integrity counts against hardware that has faults are accurate. To make sure the counts are accurate, the integrity check traffic simulator forces the PMs to continuously check integrity on the network plane where the integrity failure occurred. If the quantity of integrity failures exceeds the integrity threshold, the integrity check traffic simulator turns off integrity checking. Then the simulator clears the integrity check traffic simulator connection, and generates an ICTS101 log. The fault path and NET INTEG buffers record the paths with detected failures for additional testing.

More than one user can access the integrity check traffic simulator at one time. The first user to access the integrity check traffic simulator is the main user. The main user has control of the commands that control the tests. Users can access the integrity check traffic simulator later (while the program is in use). The system assigns these users observer status. These users can monitor, but not control, the integrity check traffic simulator.

You can use the integrity check traffic simulator separately. Use of the simulator with the network integrity analysis feature (NET INTEG) and the network path (NET PATH) test tool is the recommended method.

Links with other features

The integrity check traffic simulator identifies call paths that have defects caused by marginal hardware components that are not important. The NET INTEG feature correlates the integrity counts that identify these paths. The

path fault buffer and NET INTEG buffer LOG BUF register the integrity counts. The NET PATH test tool uses the data from these buffers to recreate the paths and isolate the components that cause the fault. After the component is replaced, the NET PATH test tool can recreate and test the path. This verifies that the fault clears.

Effect of restarts on integrity check traffic simulator

All restarts deactivate the integrity check traffic simulator and free all integrity check traffic simulator connections.

Safeguards for the use of integrity check traffic simulator

You can use the integrity check traffic simulator in offices which are InSv or not InSv. Integrity check traffic simulator connections can interfere with live traffic in InSv offices. Established safeguards for the use of this tool are present. The integrity check traffic simulator audit monitors and enforces these safeguards.

The ICTS audit

The integrity check traffic simulator audit runs as long as the integrity check traffic simulator maintains connections. The audit cycles through the connections, clears the integrity counts and frees connections where the safety limits are exceeded. The audit keeps a record of the start and stop time of the cycle. The record also contains the quantity of connections cleared, the reasons for clearing the connections, and the quantity of connections refreshed.

The safeguards enforced by the integrity check traffic simulator audit are as follows:

- integrity thresholds
- line channel limits
- traffic limits

Integrity thresholds

The integrity check traffic simulator audit clears all integrity counts during each cycle. The integrity threshold is the quantity of integrity failures allowed on a connection during an audit cycle. Operating company personnel determines the threshold value. The threshold value has a range of 5 to 50 failures. The default threshold value for InSv offices is 15 failures. The default threshold value for offices not InSv is 50 failures.

Line channel limits

The line channel limits vary according to the office type. These limits are the maximum percentages of call processing resources that the system can use for integrity check traffic simulator connections. These limits apply to

network links associated with lines and operating company personnel must strictly apply these limits. This process prevents the integrity check traffic simulator from interfering with call processing. For InSv offices the maximum percentage of line channels that the integrity check traffic simulator can use is 25%. For offices that are not InSv, the maximum percentage of line channels that the integrity check traffic simulator can use is 75%. When the percentage of line channels used in integrity check traffic simulator connections exceeds the limits, the integrity check traffic simulator audit clears connections. When the percentage of line channels exceeds these limits, the system cannot set up integrity check traffic simulator connections.

Traffic limits

Traffic limits are the quantity of connections that the system sets up or attempts on a link. These limits vary according to the office type. For InSv offices the maximum quantity of connections the system attempts for each link is seven. For offices that are not InSv, the maximum quantity of connections the system attempts for each link is 21. If you change the office type from InSv to not InSv or from not InSv to InSv, a warning occurs. This warning indicates the change in line channel and traffic limits. If you change the office type a *yes* or *no* prompt occurs. This prompt requires operating company personnel to verify the office type before the test continues.

As with line channel limits, the integrity check traffic simulator audit clears connections that are present when the number of attempted connections exceeds the traffic limits. The system cannot set up integrity check traffic simulator connections if this occurs.

Junctors associated with all PM types

The associated junctors remain below the following limits to avoid blockage (the PM types are not important):

- for InSv offices
  - — maximum channels on a link used by the integrity check traffic simulator is 7
- for offices that are not InSv
  - — maximum channels on a link used by the integrity check traffic simulator is 21

To establish integrity check traffic simulator connections, do the following:

- configure the links
- specify the options

- setup the connections

Configure the links

The system sets up integrity check traffic simulator connections on end-to-end paths between networks, or between one network and a PM. The connection depends on the configuration of the links.

The possible configurations are

- inter configures links between two networks and the PMs directly connected to the networks
- intra configures links between a network and a PM. Intra causes the system to loop the connection back to the network

Specify the options

To specify options for integrity check traffic simulator connections, use the IOPTION command. The defaults to this command define a set of options for the use of the integrity check traffic simulator in InSv offices. These options take effect when you access the integrity check traffic simulator tool.

These options determine the environment in which the integrity check traffic simulator runs:

- office type
- pattern for channel selection
- MS or CMC clock
- integrity threshold
- refresh the connections
- clear the connections
- generate ICTS logs

How to set up ICTS Connections

When you have configured the links, and have specified the conditions, use the command ISETUP to set up ICTS connections.

To specify the quantity of attempts at connections each link can support, use the parameter CONNS.

Determine the office type

The line channel limits, traffic limits, and the integrity thresholds depend on the office type: InSv or not InSv. Establish and verify the office type before you set up integrity check traffic simulator connections.

Specify a pattern for channel selection

The integrity check traffic simulator selects channels for use in integrity check traffic simulator connections. The simulator selects channels according to a pattern specified by operating company personnel. The following patterns are available

- bottomup
  - — starts at zero and looks for low numbered channels
- topdown
  - — starts at 31 and looks for high numbered channels
- increment
  - — starts at the last channel found and looks over all the remaining channels

Identify the MS or CMC clock

The system clocks the networks involved in integrity check traffic simulator connections from the MS or CMC. To identify the MS or CMC, enter zero for MS or CMC 0 and enter one for MS or CMC 1. Choose the parameter CLOCK of the IOPTION command. If you do not specify either option, the parameter CLOCK defaults to BOTH. The default BOTH causes the networks to switch clocks when you enter the IREFRESH or ISETUP command.

Establish the integrity threshold

To allow the audit to monitor the integrity threshold, use the parameters ITHRESHOLD ENABLE ON with the IOPTION command. The integrity threshold varies according to the office type.

Refresh integrity check traffic simulator connections

The system makes sure that integrity counts against hardware that has faults are accurate. To do this, the system automatically refreshes integrity check traffic simulator connections each time an integrity failure occurs. When the system refreshes integrity check traffic simulator connections, the system forces PMs to continue to check integrity on the original plane.

How to clear integrity check traffic simulator connections

The operating company personnel can clear connections. In an InSv office the operating company personnel must clear connections daily to free the line channels for call processing. The operating company personnel can choose to clear the integrity check traffic simulator connections at a specified time. If they do not specify a time to clear connections, the audit clears all connections at 7:00 am daily. In offices that are not InSv, the system can retain connections indefinitely.

How to generate integrity check traffic simulator logs

The integrity check traffic simulator audit generates ICTS logs that contain summaries of the status of all integrity check traffic simulator connections. The summaries include the quantity of integrity check traffic simulator connections whose integrity the system refreshed. The summaries also include the quantity of integrity check traffic simulator connections that the system freed because of traffic.

Refer to table 8-3 for descriptions of integrity check traffic simulator commands.

Table 8-3
ICTS commands

Tool	Application	Commands	Reference
ICTS	Accesses the ICTS subsystem and activates ICTS.	ICLEAR. Stops integrity checking by the PM and clears all ICTS connections. These connections include the history of the previous connection setup.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.
		ICONFIG. Identifies user specified links as available to set up ICTS connections.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.
		IOPTION. Establishes the conditions for running ICTS and displays the configuration that resulted from from each parameter used.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.

—continued—

Table 8-3
ICTS commands (continued)

Tool	Application	Commands	Reference
		IQUERY. Queries and displays the following. • The quantity of connections established by the command ISETUP. • The quantity of channels tested on links and junctors. • The count of integrity failures on ICTS connections. • The components in the paths involved in ICTS connections. • The counters for the ICTS audit.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.
ICTS (continued)	Accesses the ICTS subsystem and activates ICTS.	IREFRESH. Refreshes ICTS connections and forces integrity checking to continue on the original plane. You can use this command when you verify that a fault cleared after you change a hardware component.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822.
		ISETUP. Sets up connections on links configured for ICTS.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822

—continued—

Table 8-3
ICTS commands (continued)

Tool	Application	Commands	Reference
		ITRNSL. Translates a channel on a network link to a PM circuit, channel, and a calling link identification.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		QUIT. Exits the ICTS subsystem.	
		—end—	

Network fabric

The network fabric test feature provides the ability to schedule network call path tests. These tests identify network integrity problems before live traffic encounters them. The network fabric feature is available in feature package Switch Path Diagnostics (NTX885AB) and requires the integrity check traffic simulator software. Network fabric is a scheduled test that uses the call paths when there is no live traffic. The test does not require manual interruption.

The test uses all the link and junctor ports in the network each night. The test can take a maximum of three nights to test all link and junctor channels. When the test uses all links and junctor channels, the test starts again. The network fabric and integrity check traffic simulator cannot run at the same time. You can suspend network fabric and resume the test after the integrity check traffic simulator completes. Commands are available that suspend and resume the test and to start and stop the manual test.

The following do not support the network fabric tool:

- the remote cluster controller (RCC)
- the remote line concentrating module (RLCM)
- the outside plant module (OPM)

Do not use the network fabric test tool during diagnostic testing of these remotes. If the network fabric test tool operates while diagnostics run on these remotes, diagnostic test failures that are not covered can occur.

How the network fabric test works

When you use the integrity check traffic simulator software, the network fabric test tool sets up a connection on each junctor in the office. The tool distributes endpoints for each connection to each link in the office. For each connection, the network fabric test tool follows these procedures.

- establishes integrity and parity checking on one plane
- maintains a count of the quantity of integrity failures detected on each connection
- reports each failure to the network integrity analysis feature that relates the integrity failures according to the hardware in the connection
- after 10 min, switches integrity and parity checking to the other plane and monitors for failures
- after an additional 10 min, analyzes the results of the tests, and records the errored path in the path fault buffer. If a port appears in more than one errored path, each later path involving the same port writes over the previous entry
- selects new links and channels as endpoints for the connections and repeats the above sequence

Scheduled tests run for hours each night. The tests resume at the point where the test stopped the previous night. You must run the network fabric test tool during periods of low traffic. The network fabric test tool is a scheduled test that you can control manually.

If the test detects more than ten failures on a connection, the network fabric test tool stops integrity checking on that connection. The network fabric test tool generates ICTS105 and ICTS106 logs. Both logs record the test status, the percentage of networks tested, and the test results. The system produces Log ICTS105 each morning which lists the paths that had integrity failures during the previous night. The system produces Log ICTS106 when a network fabric test completes.

The following office parameters associate directly with the network fabric test tool:

- NETFAB_SCHEDULE_ENABLE in table OFCVAR (office variable), starts or disables this test.
- NETFAB_SCHEDULE_TIME in table OFCVAR provides the selection of the start time.

Interaction with network integrity analysis feature

The network fabric test sets up connections which use integrity and parity to measure network performance. When this feature detects failures, the

feature reports them to the network integrity analysis program for correlation.

Interaction with network path test tool

This tool stores errored paths identified by network fabric tests in the path fault buffer. The tool also stores errors identified by manual integrity check traffic simulator tests in the path fault buffer.

Refer to table 8-4 for descriptions of network fabric commands.

Table 8-4
Net fab commands

Tool	Application	Commands	Reference
NETFAB	Accesses the netfab directory.	STATUS. Displays the status of the test and a summary of results.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		SUSPEND. Suspends scheduled NETFAB tests.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		RESUME. Resumes scheduled NETFAB tests.	Refer to *DMS-100 Family Commands Reference Manual*,297-1001-822
		START. Manually implements the NETFAB tests.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		STOP. Stops a NETFAB test manually implemented.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		QUIT. Leaves the NETFAB increment.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822

Network integrity analysis package

The network integrity (net integ) analysis program identifies paths between connected PMs where errors occur. The net integ program exchanges PCM samples for calls in progress and CSM samples for signal integrity to identify errors on speech links. Errors can occur in the hardware or software. The program determines errors in the hardware by monitoring the parity bits and integrity bytes. A network path with few mismatches of

parity bits and integrity bytes is a sane connection with integrity and parity unless otherwise specified.

The net integ program analyzes integrity when counts for the port of a link or junctor reach the threshold count. When counts for the port of a link or junctor reach the threshold, the system automatically tests the port and makes the port SysB if the port fails. The net integ status program stores information on paths that have faults in fault counters and integrity buffers. You can display the information in the counters and buffers by the NET log system. You can also display the information on the MAP display.

A connection in a network is a link of two network ports. A link joins a network port to a PM port. A link that joins a connection to another link is a path.

Note: The NET INTEG status display and menu is present if software package Maintenance Assistance (NTX053AA) is also present.

Net integ enhances the information contained in the network integrity failure logs NET101 and NET102. The following features of the net integ program enhance the information in these reports:

- A 100 message circular buffer that saves specified information from the network integrity log reports.
- The system pegs failure counts associated with network cards as a result of integrity failures.
- The ANALYZE feature which indicates how many times each serial port interface and each crosspoint card have contributed to a path that has faults.
- The ability to chart paths that have faults and that occur between two specific network modules.
- A method to determine the PM from the net port and channel.
- A chart for each PM involved in a path that has faults and that indicates the number of hits on each port.

The NET INTEG level can provide operating company personnel with instant access to the network integrity logs. The system sends the logs to a sent to a printing device. This device provides a printout of the integrity failures.

Integrity failures

The system uses integrity to verify the sanity of the speech path between two PMs. An integrity fault can be either a parity failure or an integrity mismatch.

The network logs that report integrity information are NET Logs 101 and 102. The system generates logs

- NET101 when
  - — an integrity failure occurs
  - — the system does not maintain the network path
- NET102 when
  - — an integrity failure occurs
  - — the system maintains the network path

The following can cause integrity failures

- hardware
- CC software
- PM software
- manual office activity

Refer to table 8-5 for descriptions of net integ commands.

Table 8-5
NET INTEG commands

Tool	Application	Commands	Reference
NETINTEG	Accesses the net integ directory.	ANALYZE. Analyzes the information in the fault counters and integrity (parity) buffer. Generates a list of codes that have faults.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		BUFFSEL. Allows operating company personnel to select specific logs for storage in the logbuff.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
NETINTEG (continued)	Accesses the net integ directory	CLEAR. Clears all counters on the posted plane and pair.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		COUNTS. Specifies analysis of the total number of fault counts for the network cards.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822

—continued—

Table 8-5
NET INTEG commands (continued)

Tool	Application	Commands	Reference
		DISP. Shows and clears the integrity failures and fault counters in the buffer.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		FILTER. Allows operating company personnel to query the integrity (parity) throttling, or set the parity throttling on a specified PM basis.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		MODE. Specifies one of three modes to peg network failures.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		POST. Posts a network plane and pair.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		PM. Displays the counts of faults for the PM ports that connect to NM ports.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		RETH. Is the same as the UPTH command except that the RETH command resets all thresholds to a count of 250.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		RSTI. Resets the displays without clearing out the fault counters and integrity buffer.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
NETINTEG (continued)	Accesses the net integ directory	SETLOG. Enables or disables the output of network integrity log messages to a printer.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		TIMER. Allows operating company personnel to control when counters are cleared.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822

—continued—

Table 8-5
NET INTEG commands (continued)

Tool	Application	Commands	Reference
		TRLNK. Translates a network pair, link and channel to a PM and TID.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		TRNSL. Identifies the location of the card by frame and row. TRNSL identifies the location of a specified card.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		UPTH. Changes the thresholds for the counters on which the DISP COUNTS command relies.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
—end—			

Network path

The net path test tool identifies components that have faults and that cause integrity failures. This tool confirms that suspected components have faults before you replace the components, and verifies if you correct the problem when you replace the components. The network path test tool is available in feature package NTX885AB. The net path feature supports network types NT5X13AA and NT8X11AD.

Network type NT5X13AA requires network firmware release 8 or greater. Because of hardware restrictions, you cannot implement the net path feature on network type NT0X48AJ.

How the net path test tool works

To perform a net path tests, the system inserts a test pattern at a point along a speech path. The system extracts that test pattern at another point further along the same path. An extracted pattern that differs from the insert pattern, indicates a hardware path segment under test that has faults. To isolate the component, run a series of net path tests with different insertion and removal points. Replace the component that has faults. Perform additional tests. Use the original insertion and removal points to verify that you corrected the faults.

Note 1: Operating company personnel select the insertion and removal points are selected by operating company personnel.

Note 2: Net path tests run without supervision.

The system automatically schedules tests on the required resources in the order in which you submit the tests. Tests run only when all required resources become available. The status display area of the net path level continuously updates and echoes test results, while the test is in progress. You can query and display the results of one or all submitted tests at any time.

Net path tests run on any PM directly connected to a network, except a LM. The system creates a record that contains input and output data and test control information for each path tested. There are 20 records available. You can submit 20 records all for testing at the same time. But, if you submit more than one test on a record, the tests form a queue and run in order. When net path tests complete, the system releases the resources. The test results remain in the system until operating company personnel clear the results.

To change the information in a record, post the record. Only the first user to post a record can change the data or terminate a test that runs on that record. This process prevents revision of the record by more than one user at a time. Another user can view the posted record. The second user cannot take control of the record until the original user clears the display.

Some maintenance actions can cause net path tests to abort. The following is a list of those maintenance actions:

- network change of state
- out-of-service test on a network
- network crosspoint test
- network link test and a return to service
- network junctor test and a return to service

Note: The system suspends system initiated link and junctor tests while net path tests run.

Interaction with other features

Net path tests run on paths that have faults by

- the network integrity analysis feature
- the integrity check traffic simulator feature
- the bit error rate performance testing feature

Network integrity analysis feature

The network integrity analysis feature handles speech path maintenance. If a fault is not continuous and occurs only one time during testing, this feature cannot locate the source of the fault. To isolate the cause of the fault, the

system accesses the network integrity buffer and the net path tool recreates and tests the path. To access the network integrity buffer, enter the BUFPATH INTEG command at the net path level of the MAP display.

Integrity check traffic simulator feature

This feature sets up large quantities of connections and simulates traffic to identify call paths that have faults. The net path tool stores data on paths that have faults in the path fault buffer for testing. To access the path fault buffer, enter the BUFPATH PATH command at the net path level of the MAP display.

Bit error rate performance testing feature

This feature tests the complete transmission path through the network. When this feature detects errors, the bit error rate performance testing feature displays the tested end-to-end path. The feature also stores the path data in an output file. To locate the component that causes errors, the net path tool accesses the data and recreates the path for additional testing.

Network tests available with network path

The tests that you can perform on the network are as follows:

- auto
- hold
- ICTS (ICTS hand over)
- loop (network interface)
- net (network)
- scheduled

Auto

The auto test combines features of the net and loop tests. The auto test does not require operating company personnel to manually apply these tests to isolate faults. The system generates two network logs in conjunction with the auto test: NET104 and NET105. NET104 gives information on cards and links that have faults. NET105 indicates when a test passes or is aborted. The duration of the auto test is 1 to 60 min.

Hold

The hold test reserves connections on a defined path for a maximum of 960 min. You can use this test to make a path not available for call processing. The duration of the hold test is 1 to 960 min.

ICTS

The ICTS hand over test obtains a connection on a specified path and includes the path in ICTS testing. After the net path test tool detects a card

that has faults and the card is replaced, you can perform the ICTS test. The ICTS test does not require insertion and removal points or other test data.

Loop

The loop test applies only to XPMs. Integrity and parity monitor the complete path during a call or ICTS test. The path includes the links out of the PM directly connected to the network. The loop test tests these links. The loop test sets up a looparound connection through the PM link interface card associated with the network. The duration of the loop test is 1 to 180 min.

Net

The network test runs on paths in a network. You can test all or any of the hardware components in a network connection. The components that you can test depend on the insertion and removal points that you use.

Scheduled

The scheduled test runs at a specified time. The scheduled test takes paths from the input buffer, and performs path tests on problem paths automatically. The system sets up path tests based on the severity and frequency of the problems. Multiple scheduled tests run at the same time while test resources are available. The system prints the test results in logs and generates a status report each morning. The system places all failed paths in a fault buffer. Operating company personnel can retrieve the paths that have faults from this buffer and perform manual tests on selected paths. The test duration of the scheduled test depends on the source and type of the defect or defects.

Data required for net path tests

The system requires path and test data to define net path tests.

Path data

The system takes path data from the INTEG or path fault buffers. The system enters the path components at the MAP position. The DMS system administers automatically the difficult rules which govern the integrity of a path. When the system enters path data at the MAP display, the DMS system is in a path data input state. Specify the minimum information for the path (only the components of interest). To complete the path, the DMS system selects components from available resources.

Test data

Test data tests consists of the insertion and removal points for the test code, and the duration of the tests. The insertion and removal points are the points in a network where the system can insert or remove the test code. The system enters the test data in the DMS system, if the system is in the test

data input state. The test code is a pattern used to test paths that have faults. The test code card monitors the pattern. The net path tool checks the pattern at 10-s intervals.

The net path tool can test a complete path or a single path component, according to the chosen points. The point of removal must follow the point of insertion in the call path. The limit of the path or path segment that the tool tests does not affect this rule.

The DMS system automatically determines the correct insertion and removal points for each path. The choice of insertion and removal points depends on the following:

- type of networks involved in the path
- network side
- junctors (serial or parallel) that connect the networks

Note: Refer to Chapter 10 procedure 10-5 for steps on how to perform a net path test.

Refer to table 8-6 for descriptions of net path commands.

Table 8-6
Net path commands

Tool	Application	Commands	Reference
NETPATH	Accesses the net path directory.	ALTPATH. Alters a section of the path definition.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		ALTTEST. Alters the test data for a posted record.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		ALTTYPE. Alters the test type.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		BUFPATH. Allows you to obtain a path from the integrity buffer or the NET PATH fault buffer.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822

—continued—

Table 8-6
Net path commands (continued)

Tool	Application	Commands	Reference
		CARDLST. Displays the locations of all cards between the user-defined insertion and removal point for the AUTO test.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		CLEAR. Frees a test record.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		CPYPATH. Copies the path data from a current record to the posted record.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		DEFPATH. Specifies the first path information for a recently posted test record.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		DEFTEST. Defines the test data for the record.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
NETPATH (continued)	Accesses the net path directory.	DISP. Displays a posted record or group of records.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		INFO. Displays a diagram of the cards involved in the tested path.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		NEXT. Posts the next element in the post set.	
		POST. Creates a new test record, and provides the commands to define and submit a test. Specifies a test record or set of records that will appear.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822

—continued—

Table 8-6
Net path commands (continued)

Tool	Application	Commands	Reference
		RESET. Returns a posted test to a previous state.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		START. Starts a test that is recently defined or reset.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		STOP. Aborts the posted test.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
		VERPATH. Verifies that the path data entered is correct.	Refer to *DMS-100 Family Commands Reference Manual*, 297-1001-822
—end—			

Enhanced network tools

This section describes the product–specific test tools for the ENET.

Enhanced integrity check traffic simulator

The enhanced integrity check traffic simulator is a tool that you can use to test the integrity of network connections in an office. To perform this test, set up a potentially large number of connections that the peripherals monitor for integrity.

The test monitors integrity faults on different architectural components of an ENET. Examples of architectural components are: the complete frame, each plane, each shelf, and different operating levels provided by the crosspoint cards. Levels are thresholds. If the thresholds are exceeded, the affected card changes to an ISTb state.

The enhanced integrity check traffic simulator provides a command interpreter (CI) increase to configure, set up, and clear connections. Based on selection requirements, the CI uses two channels on a link to set up a network connection. This process enables integrity monitoring. If the number of integrity failures exceed the threshold within a fixed time period, the connection is taken down, and the network path test tool tests the path.

Note: The enhanced integrity check traffic simulator and the integrity check traffic simulator are the *same* tools used in different environments. Refer to the DSNE tools section of this chapter (page 8-21) for a detailed explanation of the integrity check traffic simulator.

Enhanced integrity check traffic simulator instead of integrity check traffic simulator tool

At any time, both the DSNE and ENET hardware and software can be present in a switch at the same time. The ENET version has a different name—enhanced integrity check traffic simulator. Only minor differences occur in the command syntax for each switch. For example, DSNE uses junctors and ENET uses a shelf or card. Changes do not affect the user interface of the exiting integrity check traffic simulator tool. Logs that the enhanced integrity check traffic simulator produced are ECTS logs. These logs are not ICTS logs. Refer to table 8-7 for enhanced integrity check traffic simulator commands.

Table 8-7
Enhanced integrity check traffic simulator commands

Command	Description
ICLEAR	Takes down all network integrity check traffic connections and stops integrity scanning.
ICONFIG	Configures the network links required to set up connections.
IOPTION	Allows you to change enhanced network integrity check traffic options.
IQUERY	Queries the number of connections established, the number of integrity failures, and the actual links used for the enhanced integrity check traffic simulator.
IREFRESH	Rebuilds the enhanced integrity check traffic simulator integrity checking to the original plane.
ISETUP	Establishes the network connections previously configured with the ICONFIG command.
ITRNSL	Translates an ENET shelf, card, link, and channel into a PM, circuit, channel, and terminal identifier (TID).

About network bit error rate tests

The ENET BERT level of the MAP display allows operating company personnel to perform network BERTs. The BERT tests only the ENET performance. The system does all insertion and removal of data in the ENET and does not include other components, for example, peripherals. The DS30 Interface Paddle Board (NT9X41) and Quad DS512 Fiber Interface Paddle Board (NT9X40) cards allow the system to generate and compare test data on the respective receive and transmit ports. The test data can be constant data or pseudo-random data. The system inserts pseudo-random data at a *from* port and checks the data at a *to* port. Any discrepancies between the inserted and extracted data cause a bit error counter to increase. You can use a network BERT to measure the performance of the hardware components which form the ENET switching matrix.

A network BERT performs this function. To perform this function, the network BERT establishes two-way block connections at the same time. The network BERT establishes these connections over ENET speech paths. The network BERT also measures the bit error rates over these connections.

A block connection consists of a block of 511 PCM channels. The channels originate and terminate at the interface ports of an ENET link interface paddle board. An example of a block connection is a speech path over all the channels of a DS512 fiber. Another example is a speech path over one DS30 cable. A DS30 cable consists of 16 DS30 links joined to a connector.

When the measured error rate of a test path exceeds the acceptable threshold, the system records transmission errors, or hits. The test definition specifies this threshold. One of eight BERT buffers can store these hits. The buffers correspond to the available test records. The system uses hit information to determine a performance rate for the ENET.

Note: The definition of a BERT on a single PCM channel is not a supported test option. The amount of time required to run this test with an acceptable target error rate is not acceptable.

The connections established during a BERT depends on the options you chose when you implemented the test and the user definition of the test record. The software supports BERTs. You rarely use BERTs on a single entity smaller than a crosspoint card.

You can add one or more of the following entities to the user definition section of a BERT record:

- a network node (one plane of a shelf)
- a single 16K X 16K channel crosspoint (NT9X35BA) card

- a port on a crosspoint card
- a two-way connection through the ENET

If you start the test with the USER parameter, the added entities are considered for inclusion in the BERT connection map.

Connection mapping

When you define and submit a test, the system determines a *connection map* for the test. The system pairs ports that are in a correct state.

The standards that allow the system to determine which ports are correct are based on the following:

- the hardware selected for the test
- if the test uses InSv or OOS mode to run
- the configuration of the ENET

When the system determines the connection map, the paired ports connect. These paired ports form two-way connections.

In-service and out-of-service BERTs

When you submit a BERT that you defined, you can choose to run the test in InSv or OOS mode.

Table 8-8 shows the standards used to determine which ports are correct. Table 8-8 shows these standards for all BERT definitions when you implement BERT in either mode.

Table 8-8
How to implement BERTs with InSv and OOS conditions

BERT definition	In-service testing	Out-of-service testing
BERT. BERT is the default definition.	Any unequipped ports on InSv crosspoints in the specified plane are correct for this BERT.	Any ports in a shelf where the crosspoints are all ManB or OFFL are correct for this test.
SHELF. Use this to add any shelf to the user definition for a BERT.	All unequipped ports on InSv cards in the specified shelf are correct for the BERT.	All ports on ManB cards will be correct, provided all crosspoints on the shelf are either ManB or OFFL.
Note: The ENET BERT facility does not support InSv testing on ports that connect to a PM.		
—continued—		

Table 8-8
How to implement BERTs with InSv and OOS conditions (continued)

BERT definition	In-service testing	Out-of-service testing
CARD. Use this to add any card to the user definition for a BERT.	Any unequipped ports on the specified crosspoint are correct, provided the card is InSv.	All ports on the specified crosspoint are correct, if all crosspoints in the shelf are ManB or OFFL.
CONN. Use this to add a two-way connection to the user definition for a BERT.	The specified ports are correct, if all elements of the connection are InSv and the ports are unequipped.	The specified ports are correct, if the ports are both on ManB crosspoints in a shelf where the crosspoints are all ManB or OFFL.
PORT. Use this to add a single port to the user definition for a BERT.	The specified port is correct if it is not equipped and the crosspoint of the port is InSv.	The specified port is correct, if the port is in a shelf where the crosspoints are all ManB or OFFL.
Note: The ENET BERT facility does not support InSv testing on ports that connect to a PM.		
—end—		

The two types of BERT tests are: a partial test and a complete test. The partial test tests unequipped ports on all equipped paddle boards. This test does not affect service. You can implement this test if the crosspoints are InSv. You can also use this test as a background test in an audit. Use the complete test to test all ports on all equipped paddle boards. This test affects service. You cannot implement this test if any if the crosspoints that you test are InSv.

Block test connections

This section describes the configuration of a single block connection test.

Hardware contained in the ENET interface paddle boards generates data. The system inserts data onto the test path. Point A in figure 8-4 represents this process.

The network switches this data according to the connections established in the test definition. Then the system loops the data around at the far end of the connection. The dotted line segment in figure 8–4 represents this process.

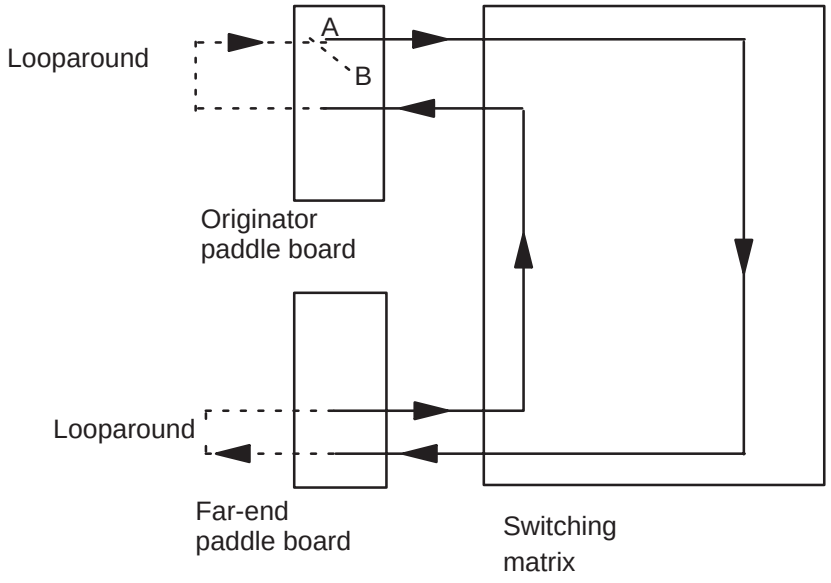
The test data travelled a two-way connection. The system loops the data around at the originator paddle board. Software on the originating paddle

board removes and analyzes the data. Point B in figure 8-4 represents this process.

The system can perform the looparound at the paddle board in two ways:

- internal loop
  - — the far-end paddle board loops the data back onto the test path internally
- external loop
  - — for DS512 paddle boards only, you can attach a fiber cable to the board to provide external looparound

Figure 8-4
Generic view of a 511 channel block connection test



Note: You do not require external test equipment to perform a network BERT.

The path of a two-way block connection involves the following hardware elements of the ENET:

- Link interface paddle boards
  - — the originator paddle board of the connection contains hardware and software. The system needs this software to generate, insert, remove, and analyze the data used by the BERT.

— both the originator and far-end paddle boards in the connection perform data loopback. This action establishes a two-way connection through the switching matrix.

- Crosspoint cards

  — the system switches the block connection over the crosspoint cards in the ENET switching matrix. The crosspoint cards in the ENET switching matrix form the vertical and horizontal buses.

Fault isolation

The network BERT facility can indicate if suspect hardware is present on a connection path. The facility is not required to isolate faults on each hardware component of the ENET switching matrix. These components form the path.

The system can import connections written to a BERT buffer in response to test hits. The system imports these connections at the path test level in order to perform fault isolation. The system performs fault isolation on the hardware components associated with the one-way paths that form the connection.

BERT log reports

The following log reports associate with the ENET BERT level:

- ENET600 —the system generates ENET600 when a BERT starts
- ENET601—the system generates ENET601 when a BERT finishes

Refer to table 8-9 for descriptions of ENET BERT commands.

Table 8-9
ENET BERT commands

Command	Description
POST	Displays information of the specified BERT number and makes this the current BERT.
DISPLAY	Displays the information for the specified test number.
DEFINE	Defines the parameters for a BERT.
START	Initiates a test on the specified path.

Enhanced network fabric test tool

This tool enables you to perform scheduled tests of the DMS Supernode system call paths through the switching matrix. These tests identify ENET integrity problems before live traffic encounters them. The enhanced network fabric test requires the enhanced integrity check traffic simulator software. The test operates as follows:

- Scheduled testing occurs each night. The tests check all channels on InSv links and cards. The test can take several nights to test all cards, according to the size of the office.
- Manual start and stop, or resume and suspend commands, are available.
- The test reports each error path over the set threshold to the ENET integrity fault handler.
- The ENET remains InSv during the tests.
- An office parameter, NETFAB_SCHEDULE_ENABLE in table OFCVAR, enables or disables this test.
- An office parameter, NETFAB_SCHEDULE_TIME in table OFCVAR, provides the selection of the start time.
- Each day the system generates an ECTS log report. The report indicates the results of the tests from the previous night.
- You cannot run enhanced network fabric and enhanced integrity check traffic simulator at the same time. You can suspend the enhanced network fabric test when the enhanced integrity check traffic simulator is run. After the enhanced integrity check traffic simulator completes, you can resume the enhanced network fabric test.
- You can manually implement and terminate the enhanced network fabric test.

Refer to table 8-10 for descriptions of ENET fabric test commands.

Table 8-10
ENET fabric commands

Command	Description
QUIT	Leaves the ENET fabric increment.
RESUME	Resumes scheduled ENET fabric testing.
START	Manually implements ENET fabric testing.

—continued—

Table 8-10
ENET fabric commands (continued)

Command	Description
STATUS	Displays the status of the test and a summary of results.
STOP	Stops a ENET fabric test that you implemented manually.
SUSPEND	Suspends scheduled ENET fabric testing.
—end—	

The network fabric test tool is not supported on any variations of the following:

- the remote cluster controller (RCC)
- the remote line concentrating module (RLCM)
- the outside plant module (OPM)

Do not use the network fabric test tool during diagnostic testing of these remotes. Incorrect diagnostic test failures can occur, if the network fabric test tool is in progress while diagnostics run on these remotes.

Problem solving chart

This chapter provides a list of indications and possible causes of problems that affect service. These problems are for the enhanced network (ENET) and the double shelf network equipment (DSNE). Table 9-1 provides a list of ENET and DSNE alarm conditions and possible causes.

Table 9-1
ENET and DSNE alarm clearing

Alarm condition	Possible cause	Action
Critical	A minimum of one card pair is out of service (OOS) in an ENET shelf.	Refer to *Alarm and Performance Monitoring Procedures*.
	Both planes of an ENET shelf are OOS	Refer to *Alarm and Performance Monitoring Procedures*.
	The number of network module (NM) pairs indicated are OOS.	Refer to *Alarm and Performance Monitoring Procedures*.
Major	A minimum of one ENET node is in a central side (C-side) busy state. A blocked messaging path to the DMS-bus component causes a C-side busy ENET node to be OOS.	Refer to *Alarm and Performance Monitoring Procedures*.
	The system removed a minimum of one crosspoint card from service.	Refer to *Alarm and Performance Monitoring Procedures*.

—continued—

Table 9-1
ENET and DSNE alarm clearing (continued)

Alarm condition	Possible cause	Action
Major (continued)	The system removed a minimum of one ENET node from service.	Refer to *Alarm and Performance Monitoring Procedures*.
Minor	A C-side link from an ENET node to a message switch (MS) is OOS.	Refer to *Alarm and Performance Monitoring Procedures*.
	You cannot open the image file. Table PMLOADS contains incorrect entries or the file has faults.	Refer to *Alarm and Performance Monitoring Procedures*.
	Manual action on a minimum of one ENET component.	Refer to *Alarm and Performance Monitoring Procedures*.
	A minimum of one ENET node is manually busy (ManB).	Refer to *Alarm and Performance Monitoring Procedures*.
	A minimum of one peripheral side (P-side) link between the ENET and a peripheral module (PM) is OOS.	Refer to *Alarm and Performance Monitoring Procedures*.
	A routine exercise (REx) test runs on the plane of the ENET. The number that follows REx indicates the plane.	Refer to *Alarm and Performance Monitoring Procedures*.
	The specified number of NMs is in the ManB or C-side busy state.	Refer to *Alarm and Performance Monitoring Procedures*.

—continued—

Table 9-1
ENET and DSNE alarm clearing (continued)

Alarm condition	Possible cause	Action
Minor (continued)	The alarm indicates the number of network junctors in one of the four following states: • SysB • ManB • C-side busy • P-side busy	Refer to *Alarm and Performance Monitoring Procedures*.
	The indicated number of NMs have links that are in one of the following states: • SysB • C-side busy • ManB	Refer to *Alarm and Performance Monitoring Procedures*.
	The indicated number of NMs are in the in-service trouble (ISTb) state. The system sets the NM to the ISTb state when the link, junctor or crosspoint reaches the threshold for integrity or parity failure.	Refer to *Alarm and Performance Monitoring Procedures*.
	The indicated number of NM pairs are OOS.	Refer to *Alarm and Performance Monitoring Procedures*.
	The indicated number of NMs are SysB.	Refer to *Alarm and Performance Monitoring Procedures*.
In-service trouble	A crosspoint card in the ENET has problems and remains in service (InSv).	Refer to *Alarm and Performance Monitoring Procedures*.

—continued—

Table 9-1
ENET and DSNE alarm clearing (continued)

Alarm condition	Possible cause	Action
In-service trouble (continued)	A P-side link component of the ENET has problems, but remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*.
	A minimum of one system card in an ENET node has problems, but remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*.
	A component in the ENET has problems, but remains InSv.	Refer to *Alarm and Performance Monitoring Procedures*.
No alarm	A scheduled REX test is manually disabled.	Refer to *Alarm and Performance Monitoring Procedures*.
—end—		

Advanced problem solving procedures

Advanced trouble locating procedures

Use advanced trouble locating procedures when the normal problem solving procedures do not clear faults. A later Batch Change Supplement (BCS) release provides advanced trouble locating procedures.

How to turn on the network

This section provides the steps that you follow when you turn on the double shelf network equipment (DSNE), and the enhanced network (ENET).

Two-shelf network equipment

Refer to procedure 10–1 to power up the DSNE.

Procedure 10-1
How to power up the DSNE network

Step	Action
1	Enter the network level at the MAP display. **>NET**
2	Set the switch on the power converter to the up (ON) position and push the reset switch. This procedure powers up the network plane.
3 3 (continued)	At the MAP display, return the network plane that you power up to service. **>RTS <plane> <network>** For example **>RTS 0 4** (where network 4 plane 0 returns to service).
	—continued—

Procedure 10-1
How to power up the DSNE network (continued)

Step	Action
4	Return to service (RTS) any links that you manually busied in the power down process. **>LINKS <pair>** **>RTS <plane> <links>** (The network is back in service [InSv]).
5	Continue this process until all of the network planes are back InSv.
	—end—

Enhanced network

Refer to procedure 10-2 to power up the ENET.

Procedure 10-2
How to power up the ENET

Step	Action
1	Make sure that all four power converter cards that you power up sit correctly in the slots. The four power converters consist of: • two +5V 80A Power Converter cards (NT9X30) • two –5V 20A Power Converter cards (NT9X31)
2	To turn ON the four power converters, press upward on each power switch. The switch automatically returns to the center position. As you turn ON each card, the light-emitting diode (LED) of the converter turns off.
3	After you power up the shelf, you can load the shelf again and RTS the shelf.
	—continued—

Procedure 10-2
How to power up the ENET (continued)

Step	Action
4	Access the System level of the MAP display from the network (NET) level.
5	Busy the ENET shelf.
6	Load the software into the shelf. Only use the parameter file name if you require a specified ENET load. If you do not use the parameter file only when required, the system loads the default file identified in tables PMLOADS and ENINV (enhanced network node inventory).
7	Test and RTS the shelf. If all tests pass, the shelf is InSv. If a test fails, refer to the test response and logs to determine why the test failed.
8	Allow calls to be routed to the other shelf.
	—end—

How to power down the network

This section provides the steps to follow when you power down the DSNE and the ENET.

Double shelf network equipment

Refer to procedure 10-3 to power down the DSNE.

Procedure 10-3
How to power down the DSNE network

Step	Action
1	Enter the network level at the MAP display. **>NET**
2	Busy the correct plane of each network. **>BSY <plane> <network>** for example **>BSY 0 4 (where network 4 plane 0 is being busied)**
3	Set the switch on the power converters to the OFF position. (The network plane is powered down).
4	Continue this process until you power down all of the correct network planes.

Enhanced network

Refer to procedure 10-4 to power down the ENET.

Procedure 10-4
How to power down the ENET network

Step	Action
1	Access the System level of a MAP display from the NET level.
2	Allow calls in progress to complete. Request that the system route later calls to the other shelf. Wait 30 min to allow calls in progress to complete.
3	Busy the shelf.
4	Offline (OFFL) the shelf.
	—continued—

Procedure 10-4
How to power down the ENET network (continued)

Step	Action
5	Turn OFF the following power converter cards on the shelf: • two +5V 80A NT9X30 cards • two –5V 20A NT9X31 cards To turn OFF the power converter cards, press downward on each power switch. This switch automatically returns to a center position. As each card turns off, the LED labeled *Converter Off* lights up.
6	The shelf is turned off.
	—end—

DSNE net path testing

Procedure 10-5 contains the sequence for net path testing in the DSNE.

Procedure 10-5
DSNE net path testing

Step	Action
1	Post a new record with the POST NEW command. The system posts a record, and the state changes to path data input.
2	Enter the path data. Use the DEFPATH command to define a path at the MAP display. You can also use the BUFPATH INTEG OR BUFPATH PATH command to recreate a path from a buffer. The ALTPATH command modifies the path data. The CPYPATH command replaces path data with data from another record.
3	Enter the VERPATH command to check the path data for errors or other problems that can stop the test. If the command detects errors, perform the actions described in the responses to the VERPATH command. Perform these actions until the command verifies the path, and the state changes to test data input.
4	Enter new test data or modify default data with the DEFTEST or ALTTEST commands.
Note: Enter the INFO command for help to select insertion and removal points for net or loop tests.	
	—continued—

Procedure 10-5
DSNE net path testing (continued)

Step	Action
5	Enter the START command to submit the test. The test runs when resources become available. If the command detects errors, perform the action described in the responses to the START command. Submit the test again.
6	To run another test, repeat steps 1 to 5.
7	To monitor the progress of any test, enter the DISP command. When you post the record that contains the submitted, the status of that test appears.
8	To stop a test, enter the STOP command. The test aborts in 10 s. The state of the test changes to aborted.
9	To clear a test and free a record, enter the CLEAR command. The record must be in the correct state as described in the responses to the CLEAR command.
10	To busy out a path for a long period, define and submit a minimum of two tests with identical paths. Use the CPYPATH command.
Note: Enter the INFO command for help to select insertion and removal points for net or loop tests.	
—end—	

Common procedures

There are no common procedures.

Appendix A: Status fields of ENET functional blocks

Appendix A describes the values of the status field of the major operating blocks for the enhanced network (ENET). This appendix also lists ENET alarms codes.

System status field

Table 11-1 describes the possible values for the System status field. In this example, System refers to the processing complexes of the nodes in a plane.

Table 11-1
System status field values

Field value	Meaning
•	OK. All ENET nodes in the plane are in service (InSv).
—	Unequipped. ENET nodes in the plane are not equipped.
ISTb	In-service trouble. A fault is present in the system portion of a minimum of one ENET node, but the affected hardware remains InSv.
RexTst	A routine exercise (REx) test is in progress on a node.
CSLink	A fault is present on the central side (C-side) link on a node.
Fault	An ENET system is out of service (OOS). The affected node is OOS.

Matrix status field

Table 11-2 describes the possible values of the Matrix status field. This field monitors the switching matrix for each plane. The switching matrix consists of all crosspoint cards and the associated link interface paddle boards.

Table 11-2
Matrix status field values

Field value	Meaning
•	OK. The crosspoint matrix on the indicated plane is InSv without faults.
—	Unequipped. The crosspoint matrix on the indicate plane is not equipped.
ISTb	In-service trouble. A fault is present on a component of the crosspoint matrix, but the affected hardware remains InSv.
RexTst	A REx test is in progress on the crosspoint matrix.
Fault	A minimum of one element in the matrix is OOS. This condition does not affect service. You can route traffic through the corresponding matrix card on the other plane.

Blocked status indicator

Crosspoint cards and their associated link interface paddle boards compose the ENET switching matrix. The BLOCKED indicator is on the right of the ENET shelf status field. The BLOCKED indicator will identify an out-of-service (OOS) ENET component (node, card, paddleboard, or link) in one plane, and as an OOS ENET component in the opposite plane. In this state, the switching matrix is broken and network blockage occurs.

A warning at the MAP terminal will identify when an HMI command could cause network blockage. For example:

>card 10
CARD:

>bsy 1 link 9
WARNING: This action will cause NETWORK BLOCKAGE. Please confirm (”YES”, ”Y”, ”NO”, or ”N”):

If the craftsperson decides to ignore this warning and proceed, the matrix will be broken and certain calls will not be setup successfully.

Note that if the same ENET component is OOS in both planes, in addition to network blockage, peripheral isolation may cause calls to drop. A critical alarm will appear under the Net header of the MAP display alarm banner to indicate the double fault on the ENET component.

Deload status indicator

The letter D appears when you set a minimum of one crosspoint in an ENET plane to an deload status. The D appears between the System and Matrix status fields for the affected plane.

Shelf status field

Table 11-3 describes possible values for the Shelf status fields.

Table 11-3
Shelf status field values

Field value	Meaning
•	OK. All components in the node are InSv.
—	Unequipped. The node is not equipped.
|	ISTb. A fault is present on the node, but the node remains InSv.
L	Peripheral side (P-side) link ISTb. A fault is present on one of the P-side links from the node, but the affected hardware remains InSv.
F	Fault. A fault is present on a crosspoint, link, or paddle board in the node. The affected hardware is OOS.
O	Offline. The node is offline (OFFL).
S	System busy (SysB). The system removed the node from service.
C	Central side (C-side) busy. The node is OOS because both links from the node to the DMS-bus component are OOS.
M	Manual busy (ManB). A manual action removed the node from service.
T	Test in progress. A diagnostic test is in progress on the node.

Table 11-4 lists the alarms that can appear under the NET header.

Table 11-4
ENET alarm codes

Alarm code	Severity	Explanation
CBSY	major	An ENET node is C-side busy.
CDPR	critical	An ENET crosspoint card slot is OOS in both planes.
CSLK	minor	A C-side link is OOS.
ISTB	no alarm	An ENET component has problems, but the component remains InSv.
MBCD	minor	A non-system card is ManB.
MBSY	minor	An ENET node is ManB.
PSLK	minor	A P-side link is OOS.
REX	minor	An ENET REx test is in progress.
REXOFF	no alarm	This code indicates a disabled scheduled REx test.
SBCD	major	A non-system card is SysB.
SBSY	major	An ENET node is SysB.
SHLV	critical	An ENET shelf is OOS.
.	no alarm	Faults are not present on any network components.

Appendix B: System level status fields

Appendix B describes the meaning of different fields for the System level of the enhanced network (ENET).

Status overview version

Table 12-1 describes the values that can appear in plane n (where n is 0 or 1) status field of the system level.

Table 12-1
Plane n status field values

Field value	Meaning
•	OK. The node is in service (InSv) without faults.
—	Unequipped. The node is not equipped.
O	Offline. The node is offline (OFFL).
I	In-service trouble (ISTb). A fault is present in the node, but the node remains InSv.
S	System busy (SysB). The system removed the node from service.
C	Central side (C-side) busy. The node is out of service (OOS) because both links to the DMS-bus component are OOS.
M	Manual busy (ManB). A manual action caused the removal of the node from service.
T	Test in progress. Diagnostic tests are in progress on the node.

Field values listed in table 12-1 can appear to the right of the plane n status field. The messages are for each node in the ENET. Messages that explain

different maintenance actions also can appear on the right side of the plane n status field. Table 12-2 lists and defines these messages.

Table 12-2
System level maintenance action messages

Field value	Meaning
Loading: nnnn	Software loads into memory on the node. The number displayed (nnnn) indicates the number of bits loaded.
System RTS	A system-initiated return-to-service attempt is in progress.
Manual RTS	A manually-initiated return-to-service attempt is in progress.
In-service test	An in-service test is in progress.
OOSN test	An out-of-service test, which is not destructive, occurs on the node. This test does not affect the software load.
OOSD test	A destructive out-of-service test occurs on the node. This test destroys the software load.
Mtce-open links	The system opens the messaging links between the message switch (MS) and the ENET shelf. This message appears before diagnostics start on an OOS node.
Mtce-close links	The system closes the messaging links between the MS and the ENET shelf. This message appears when diagnostics complete an OOS node.
Message test	A test runs on the messaging path between the MS and the node.
Fiber link test	A test runs on a fiber link between the MS and the node.
Reset test	A test runs on the ability of the node to reset.
Cold restart	A cold restart of the indicated node is in progress.
Reload restart	A reload restart of the indicated node is in progress.
CSLink n closed	The link from the node to MS number n is OOS.

Memory use version

Table 12-3 explains memory use information.

Table 12-3
Shelf memory use information

Field value	Meaning
Loadname	The name of the default load file in table ENINV (enhanced network node inventory).
Time	The system obtained the time when the information displayed. The format of the time is hours (h), minutes (min), and seconds (s).
DS used	The amount of data store used, expressed in kilobytes, and the percentage of total available memory.
DS avail	The amount of available data store that remains, expressed in kilobytes.
DS total	The total amount of memory allocated for data store, expressed in kilobytes.
PS used	The amount of program store used, expressed in kilobytes, and the percentage of total available memory.
PS avail	The amount of available program store that remains, in kilobytes.
PS total	The amount of memory allocated for program store, in kilobytes.

Central processing unit use version

Table 12-4 explains central processing unit (CPU) use information.

Table 12-4
Shelf CPU use information

Field value	Meaning
Loadname	The name of the default load file.
Traps:	
# / min	The number of software traps that occur each minute.
Total	The total number of software traps since the last restart.
% CPU occupancy:	
Call Pro	The percentage of node CPU time that call processing uses.
Total	The percentage of node CPU time that all processes use.

Appendix C: Shelf level status fields

Appendix C describes the meaning of different fields for the Shelf level of the enhanced network (ENET).

Status overview version

Table 13-1 lists possible values for the slot status fields of the shelf level display. Note that the slot status fields for each crosspoint card represents the following two cards:

- the crosspoint at the front of the slot
- the paddle board for the link interface at the rear of the shelf

Table 13-1
Slot status field values

Field value	Meaning
•	OK. The cards in the slot are in service (InSv).
—	Unequipped. The slot is not equipped.
I	In-service trouble (ISTb). The system detected a fault on one of the cards in the slot. The affected card remains InSv.
L	Link-service trouble. The system detected a fault on one of the links on the paddle board in the slot. The affected link remains InSv.
F	Fault. A fault is present on one of the links in the slot or the paddle board.
O	Offline. The cards in the slot are offline (OFFL) as a result of manual action.

—continued—

Table 13-1
Slot status field values (continued)

Field value	Meaning
S	System busy (SysB). The system removed the front card in the slot from service.
C	Central side (C-side) busy. The processing complex is out of service (OOS).
M	Manual busy (ManB). You manually removed the cards in the slot from service.
T	Test in progress. A test is now in progress on the cards in the slot.

—end—

Appendix D: Card level status fields

Appendix D describes the meaning of different fields for the Card level of the enhanced network (ENET). The following table lists the possible states that can apply to the card sublevel.

Table 14-1
Slot status field values

Field value	Meaning
•	OK. The card is in service (InSv).
—	Unequipped. The card is not equipped.
O	Offline. The card is offline (OFFL) as a result of manual action.
I	In-service trouble (ISTb). A fault is present on the card. The card remains InSv.
S	System busy (SysB). The system removed the card from service.
C	Central side (C-side) busy. The card is out of service (OOS) because the C-side links to the DMS-bus component are OOS.
M	Manual busy (ManB). You manually removed the card from service.
T	Test in progress. A maintenance action is now in progress on the card.

The following table contains the values that indicate the status of the links that connect the ENET shelf to the message switches.

Table 14-2
C-side port states

Field value	Meaning
OPEN	The port is open for all messaging. A port only can be open if the shelf is InSv.
MTCOPEN	The port is open for maintenance messaging. The shelf can be InSv or OOS.
CLOSED	The port is closed to all messaging. The shelf can be InSv or OOS.

The following table lists possible values for the power converter card status field.

Table 14-3
Power converter states

Field value	Meaning
IDPROM OK	The system can identify the power converter card. The system also can determine if the version of the card is correct.
IDPROM FLT	The system cannot read the identification programmable read-only memory (ROM) because the ROM has faults. The other option is that the system read the identification programmable ROM. The system determined that the version of the card is not the same version entered in software tables for the slot.
NOT INSERVICE	The system cannot read the identification programmable ROM because the ENET shelf is OOS.

The Front status field identifies the card that occupies the selected slot as a crosspoint card. This field also indicates the status of the crosspoint card in each plane. The following table describes the values that can appear in the front status field.

Table 14-4
Front status field values

Field value	Meaning
•	OK. The crosspoint card is InSv.
—	Unequipped. The crosspoint card is not equipped.
O	Offline. The crosspoint card is OFFL as a result of manual action.
I	In-service trouble (ISTb). A fault is present on the crosspoint card. The crosspoint card remains InSv.
S	System busy (SysB). The system removed the crosspoint card from service.
C	Central side (C-side) busy. The crosspoint card is OOS because the system cards on the shelf are OOS.
M	Manual busy (ManB). You manually removed the crosspoint card from service.
T	Test in progress. A maintenance action is in progress on the crosspoint card.

The Back field identifies the paddle board that occupies the selected card slot as an interface paddle board. This field also indicates the status of the paddle board in each plane. The following table describes the values that can appear in this field.

Table 14-5
Back status field values

Field value	Meaning
•	OK. The interface paddle board is InSv.
—	Unequipped. The interface paddle board is not equipped.
O	Offline. The interface paddle board is OFFL as a result of manual action.

—continued—

Table 14-5
Back status field values (continued)

Field value	Meaning
I	In-service trouble (ISTb). A fault is present on the interface paddle board, but the interface paddle board remains InSv.
S	System busy (SysB). The system removed the interface paddle board from service.
C	Central side (C-side) busy. The interface paddle board is OOS because the crosspoint card that occupies the slot is OOS.
M	Manual busy (ManB). You manually removed the interface paddle board from service.
T	Test in progress. A maintenance action is in progress the interface paddle board.
	—end—

The Links field identifies the type of links on the paddle board as DS512 or DS30. This field also indicates the status of each link number for each plane. The following table describes the values that can appear in the field.

Table 14-6
Link status field values

Field value	Meaning
•	OK. The link is InSv.
—	Unequipped. The link is not equipped.
O	Offline. The link is OFFL as a result of manual action.
I	In-service trouble (ISTb). A fault is present on the link. The link remains InSv.
F	Fault. A DS30 equivalent link is OOS on the DS512 link.
	—continued—

Table 14-6
Link status field values (continued)

Field value	Meaning
L	A DS30 equivalent link is in the ISTb state. A fault is present on the DS30 equivalent link, but the link remains InSv.
P	Peripheral side (P-side) busy. The peripheral connected to the link is OOS.
S	System busy (SysB). The system removed the link from service.
C	Central side (C-side) busy.
M	Manual busy (ManB). You manually removed the link removed from service.
T	Test in progress. A maintenance action is in progress on the link.

—end—

Appendix E: Matrix, integrity, path test and BERT information

Appendix E describes the meaning of different fields for the Matrix, Integrity, path test, and bit error rate test (BERT) levels of the enhanced Network (ENET).

Table 15-1 lists the possible field values for the matrix element status fields of the MAP display.

Table 15-1
Matrix element states

Field value	Meaning
•	OK. The matrix element is in service (InSv).
—	Unequipped. The matrix element is unequipped (Uneq).
O	Offline. The matrix element is offline (OFFL).
I	In-service trouble (ISTb). A fault is present on the matrix element, but the matrix remains InSv.
L	Peripheral side (P-side) link ISTb. A P-side link connected to the matrix element has a fault, but remains InSv.
F	Link out of service (OOS). A P-side link connected to the matrix element is OOS, system busy (SysB), or manual busy (ManB).
S	System busy (SysB). The system removed the matrix element from service.
C	Central side (C-side) busy. The matrix element is in a C-side busy state. This state indicates that a system card in the node that contains the matrix element is OOS.

—continued—

Table 15-1
Matrix element states

Field value	Meaning
M	Manual busy (ManB). You manually removed the matrix element from service.
T	Test in progress. Maintenance action occurs on the matrix element.
	—end—

Table 15-2 describes the values that can appear under the shelf status header of the analyze display. The analyze display is a menu command available at the INTEG level.

Table 15-2
Analyze status field values

Field value	Meaning
•	OK. The slot does not have integrity faults reported against the slot.
+	Slot has between 0 and the threshold value integrity faults.
*	Slot has more than the threshold value integrity faults.
–	Unequipped. The slot is Uneq.

Table 15-3 lists and defines the test states for the path test level of the MAP display.

Table 15-3
Path test level test states

Field value	Meaning
PENding	Tests in this state are defined and ready to start.
SUSpended	Submitted tests are suspended for one of the following reasons: • resources required by the test are not available at the time of submission. • higher priority maintenance action overrides the test.
RUNning	Submitted tests in this state now run.
FINished	Submitted tests in this state are complete.
ABorTed	The system or manual action aborted the tests in this state.

BERT level status fields

The status fields of the MAP display for the BERT level provide information about the now posted BERT. Table 15-4 lists and defines these fields.

Table 15-4
Bert level status fields

Field value	Meaning
Observed error rate	The bit error rate measured by the test. If equal to the optimum error rate, the test did not detect errors.
Elapsed time	This field indicates the amount of time that the posted test runs. The time is expressed in hours and minutes.
Percent complete	This field indicates the amount of time that the test runs. The time is expressed as a percentage of the total time specified in the test definition. Updates of the completion rate occur at 1-min intervals.
Optimum error rate	The optimum bit error rate for the test. This figure represents the highest bit error rate that the test can verify, given the amount of data already sent. The system updates the field as the test runs.

Appendix F: DSN display codes

Appendix F contains display and alarm codes for the double shelf network equipment (DSNE).

Table 16-1 lists and describes the status codes used to show the status of the network.

Table 16-1
Link status field values

Field value	Meaning	
. (dot)	all	No faults. The network, link, junctor, or crosspoint is OK.
–	LInk, Jctr, Xpt	Unequipped.
C	Net	Central side (C-side) busy, where the network module (NM) is busy as a result of call processing conditions.
	Link	The link is busy as a result of call processing conditions.
	Jctr	The junctor is busy as a result of call processing conditions.
	Xpt	The crosspoint card is busy as a result of call processing conditions.
I	Net	The in-service trouble (ISTb) flag is set for the NM.
J	Net	A minimum of one junctor in the NM is out-of-service (OOS).

—continued—

Table 16-1
Link status field values

Field value	Meaning	
L	Net	A minimum of one link in the NM is OOS.
M	all	Manual busy (ManB).
O	Net, Jctr	Offline (OFFL).
P	Link	Peripheral side (P-side) busy, where the link is busy as a result of conditions in the peripheral module (PM) that are assigned to the link.
	Jctr	The other end of the junctor is OOS.
	Xpt	The crosspoint card is busy because all the links and junctors connected to the crosspoint card are busy.
S	Net, Link, Jctr	System busy (SysB).
T	Net, Xpt	The system tests a network or crosspoint.
—end—		

Table 16-2 lists the alarms codes for the NET subsystem.

Table 16-2
Alarm codes

Status	Alarm	Description
. (dot)	blank	Faults are not present in any of the units maintained by the NET subsystem.
nn.IsTb	blank	NMs have ISTb.
Note: The nn is 0–31 to represent the quantity of NMs.		
—continued—		

Table 16-2
Alarm codes (continued)

Status	Alarm	Description
JctOfl	blank	NMs have junctors that are offline.
nn.Jctr	blank	NMs have OOS junctors.
nn.Link	blank	NMs have OOS links.
nn.Bsy	blank	NMs are ManB or C-side busy.
NetOfl	blank	The NM is OFFL.
nn.Pair	*C*	A quantity of network pairs in both planes are OOS.
nn.SysB	M	NMs are SysB.
nn.Xpts	blank	NMs have OOS crosspoint cards.
Note: The nn is 0–31 to represent the quantity of NMs.		
—end—		

List of terms

batch change supplement (BCS)

A DMS-100 Family software release.

BCS

batch change supplement

BERT

bit error rate test

bit error rate test (BERT)

A test that used to measure the transmission quality of a loop. The BERT transmits a known bit pattern over a line and compares the reflected signal against the first pattern.

call condense block (CCB)

A data block associated with a call from beginning through completion. The CCB contains enough information to describe a basic call. The system can extend the CCB for calls that require more data.

CC

central control

CCB

call condense block

CCC

central control complex

CCIS6

Common Channel Interoffice Signaling No. 6

central control (CC)

A part of the NT40 processor that consists of the data processing functions with the associated data store (DS) and program store (PS).

central control complex (CCC)

The part of the DMS-100 Family switch that contains all the central control (CC) functions. The functions include the central message controller (CMC), CPU, program store (PS), and data store (DS).

central message controller (CMC)

A hardware device, located in the central control complex frame, that provides an interface between the CPU, network module controllers, and input/output controllers.

central processing unit (CPU)

The hardware unit of a computing system that contains the circuits that control and perform the execution of instructions.

central side (C-side)

The side of a node that faces away from the peripheral modules (PM) and toward the central control (CC). Also known as control side. *See also* peripheral side.

channel supervision message (CSM)

A message received and transmitted continuously over each connected voice channel of a peripheral module (PM). The CSM contains a connection data byte. The connection data byte includes the channel supervision bit (CSB), and an integrity byte, that issues call path integrity.

CI

command interpreter

CM

computing module

CMC

central message controller

command interpreter (CI)

A component in the support operating system that functions as the main interface between machine and user. The main functions of the CI include the following:

- read lines entered by a terminal user
- break each line into known units
- analyze the units
- recognize command-item numbers on the input lines

- activate these commands

Common Channel Interoffice Signaling No. 6 (CCIS6)

A common channel signaling (CCS) system that uses analog trunks for the North American customers. CCIS6 uses fixed-length signaling messages.

computing module (CM)

The processor and memory of the dual-plane combined core (DPCC) used by DMS SuperNode. Each CM consists of a pair of CPUs with associated memory. The CPUs operate in a synchronous matched mode on two separate planes. Only one plane is active and the plane maintains control of the system while the other plane is on standby.

CPU

central processing unit

C-side

central side

CSM

channel supervision message

DCM

digital carrier module

digital carrier module (DCM)

A peripheral module (PM), located in a digital carrier equipment frame, that provides speech and signaling interfaces between a DS30 network port and digital trunks. A DCM contains a maximum of five line cards.

Digital Multiplex System (DMS)

A central office switching system in which all external signals are converted to digital data and are stored in assigned time slots. The DMS assigns the original time slots again to perform the switching.

digital trunk controller (DTC)

A peripheral module that connects DS30 links from the network with digital trunk circuits.

DMS

Digital Multiplex System

DMS-Bus

The messaging control component of the DMS SuperNode processor. The DMS-Bus components are a pair of message switches (MS).

DMS-Core

The call management and system control section of the DMS SuperNode processor. The DMS-Core section consists of a computing module (CM) and a system load module (SLM).

double shelf network equipment (DSNE) frame

A frame that packages one network plane on a single shelf and permits two complete networks for each plane in a single bay.

DS30

- A 10-bit 32-channel 2.048-Mb/s speech-signaling and message-signaling link as used in the DMS-100 Family switches
- The protocol by which DS30 links communicate

DS512 fiber link

The fiber optic transmission link implemented in the DMS SuperNode processor. The DS512 connects the computing module (CM) to the message switch. One DS512 fiber link is the equivalent of 16 DS30 links.

DSNE

double shelf network equipment

DTC

digital trunk controller

ENET

Enhanced Network

Enhanced Network (ENET)

A channel-matrixed time switch that provides pulse code modulated voice and data connections between peripheral modules (PM). ENET also provides message paths to the DMS-Bus components.

in-service test

A test that sends a null B word on a DS-1 link from a Subscriber Carrier Module-100 Rural (SMR) to a remote concentrator terminal (RCT). If the RCT fails to send a reply, a timeout occurs and indicates a link that has faults.

in-service trouble (ISTb)

A status imposed on a unit that has trouble indications but can continue to process calls.

InSv

in service

ISTb

in-service trouble

JNET

Junctored Network

Junctored Network (JNET)

A time-division multiplexed system that allows for switching of 1920 channels for each network pair (completely duplicated). The use of external junctors, internal junctors, and a digital network interconnecting (DNI) frame establish additional channels. You can route channels directly, or use alternate routing, through the use of junctors, a DNI frame, and software control. Capacity for a DMS-100 switch is 32 network pairs or 61 440 channels (1920 channels × 32 network pairs).

LED

light-emitting diode

light-emitting diode (LED)

A solid-state device which emits light when the device has appropriate voltage applied to the device. The LEDs function in the DMS-100 switch components as front panel indicators. The LEDs are normally off when equipment status is normal.

line module (LM)

A peripheral module that provides speech and signaling interfaces for a maximum of 640 subscriber lines. The LM consists of line drawers, a line module controller, and a frame supervisory panel.

line trunk controller (LTC)

A peripheral module (PM) that is a collection of the line group controller (LGC) and the digital trunk controller (DTC). The LTC provides all the services offered by the LGC and DTC. The LTC supports line concentrating module (LCM) and AB trunks.

LM

line module

LTC

line trunk controller

magnetic tape drive (MTD)

In a DMS switch, a device used to record DMS-100 Family data. You can mount an MTD on a magnetic tape center (MTC) frame or an input/output equipment (IOE). Also known as tape drive.

maintenance and administration position

See MAP.

maintenance level

See MTC.

MAP

Maintenance and administration position. A group of components that provides a user interface between operating company personnel and the DMS-100 Family switches. The interface consists of a visual display unit (VDU) and keyboard, a voice communications module, test facilities, and special furniture.

MAPCI

MAP command interpreter

message switch (MS)

A high-capacity communications facility that functions as the messaging hub of the dual plane combined core (DPCC) of a DMS SuperNode processor. The MS controls messaging between the DMS-Buses. The MS concentrates and distributes messages and allows other DMS-STP components to communicate directly with each other.

MS

message switch

MTC (maintenance level)

A MAP level used to access several areas of the DMS-100 switch. Areas include central control (CC), peripheral modules (PM), the lines maintenance subsystem (LNS), and other areas.

MTD

magnetic tape drive

nailed-up connection (NUC)

A permanently assigned network connection that forms part of the speech path between equipped peripheral modules (PM).

NETC

network combined

network combined (NETC) frame

A single-bay network frame that contains two network modules.

network module controller (NMC)

A group of circuit cards that communicates with the central message controller. The NMC is in the network module. The NMC directs messages to the peripheral modules or interprets connection instructions to the crosspoint switches. The NMC organizes the flow of internal messages.

network module (NM)

The basic building block of the DMS-100 Family switches. The NM accepts incoming calls. The NM uses connection instructions from the central control complex (CCC) to connect the incoming calls to the appropriate outgoing channels. Network module controllers control the activities in the NM.

NM

network module

NMC

network module controller

NUC

nailed-up connection

OFFL

offline

offline (OFFL)

- Equipment or devices not under direct control of the CPU.
- An equipment state in which the input/output (I/O) system recognizes a node. Connection information is defined, but the node is not available for normal I/O and system maintenance activity. In this state, the nonresident commissioning package accesses the node and does not affect the rest of the system.

- Terminal equipment not connected to a transmission line.

OM

operational measurements

OOS

out of service

operational measurements (OM)

The hardware and software resources 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 the transfer of the data to the displays and records. The OM data is for maintenance, traffic, accounting, and provisioning decisions.

OPM

Outside Plant Module

out of service (OOS)

An equipment state in which manual action (by operating company personnel) or automatic action (by the system) removes equipment from service.

Outside Plant Module (OPM)

A stand-alone weatherproofed enclosure. The enclosure can connect two to six DS-1 links from a line group controller (LGC) at a host office. The enclosure also can connect a maximum of 640 local connected subscriber lines. An OPM consists of the following:

- one line concentrating module (LCM)
- a remote maintenance module (RMM)
- a host interface equipment (HIE) shelf
- a power supply
- environmental control equipment
- a cable cross-connection for a maximum of 1280 pairs

PCM

pulse code modulation

peripheral module (PM)

A generic term that refers to all hardware modules in the DMS-100 Family switches. These modules provide interfaces with external line, trunk, or service facilities. A PM contains peripheral processors (PP), which perform local routines, and relieve the load on the CPU.

peripheral side (P-side)

The side of a node that faces away from the central control and toward the peripheral modules. *See also* central side.

PM

peripheral module

P-side

peripheral side

pulse code modulation (PCM)

- The process used to convert an analog (voice waveform) signal to a digital code.
- A form of modulation that samples the signal that modulates, quantifies, encodes and sends the signal as a bit stream.
- Coded and quantified periodic samples of the signal represent an analog waveform. Each element of information consists of a binary number that represents the value of the sample.

RAM

random access memory

random access memory (RAM)

A static read/write memory system that stores information in discrete individually-addressable locations so that access time is separate from location.

RCC

remote cluster controller

read-only memory (ROM)

A solid state storage integrated circuit programmed at the time of manufacture. You cannot reprogram the integrated circuit.

remote cluster controller (RCC)

A two-shelf peripheral module (PM) that provides a master controller for all units at the Remote Switching Center (RSC). The host line trunk controller (LTC) controls the RCC.

Remote Line Concentrating Module (RLCM)

An equipment frame that provides an interface between two to six DS-1 links (from the line group controller [LGC] at the host office). The RLCM provides a maximum of 640 subscriber lines (connected at the local level).

An RLCM has the following:

- one line concentrating module (LCM)
- remote maintenance module (RMM)
- host interface equipment (HIE) shelf

remote terminal interface (RTIF)

See reset terminal interface.

reset terminal interface (RTIF)

In DMS SuperNode, a terminal used to reboot and monitor the status of the system. The RTIF can be a local terminal or a remote terminal connected through a modem. Also known as remote terminal interface.

return to service (RTS)

An action that allows an out-of-service unit or piece of equipment to process calls.

REx

Routine Exercise

RLCM

Remote Line Concentrating Module

ROM

read-only memory

routine exercise (REx) test

An automatic test performed at normal intervals on DMS equipment by internal software.

RTIF

- remote terminal interface. Preferred term is reset terminal interface.
- reset terminal interface

RTS

return to service

SLM

system load module

SONET

Synchronous Optical Network

Synchronous Optical Network (SONET)

A standard for optical transport that defines optical carrier levels and the electrically equivalent synchronous transport signals of the carrier. The SONET standard allows for the following:

- a multivendor environment
- arranges of the network to transport new services
- synchronous networking
- enhanced operation, administration, and maintenance (OAM).

system load module (SLM)

A mass storage system in a DMS SuperNode processor that stores office images. From the SLM, new loads or stored images can boot into the computing module.

terminal ID (TID)

In DMS software, the TID identifies any item on which a call can originate or terminate.

TID

terminal ID

TM

trunk module

trunk module (TM)

A peripheral module (PM), in a trunk module equipment (TME) frame, that provides speech and signaling interfaces between a DS30 network port and analog trunks.

user interface

The series of commands and responses used by operating company personnel to communicate with the DMS-100 Family switches. The MAP terminal and other input/output (I/O) devices allow the communication to occur. Known earlier as man-machine interface.

XMS-based peripheral module (XPM)

The generic name for XMS peripheral modules that use the Motorola 68000 microprocessor. An XPM has two processors in a hot standby configuration: a signaling processor and a master processor.

XPM

XMS-based peripheral module

Northern Telecom Publications Customer Feedback Form

This form provides you with a means of communicating comments and concerns about Northern Telecom publications (NTP). Please return your comments to the address shown on the reverse and include your name and address. For urgent documentation-related issues, use the Documentation Hotlines: 1-877-662-5669, Option 4 + 1 (U.S. only) or 905-452-4588 (Canada/International). To fax comments and supporting information, use the Documentation Hotline fax numbers: 919-481-5854 (U.S. only) or 905-452-5423 (Canada/International).

Please identify this NTP's medium: *Paper*____ *CD*____

Number: 297-1001-591 04.03 *Date:* March 1999 *BCS/Release:* BASE10

Use this space for your comments, concerns, or problems encountered
For specific problems, please identify the appropriate page and volume numbers.

If you would like a reply, please provide:

Your name: _____

Address: _____

_____

City, State/ Province: _____ *ZIP/ Postal code:* _____

Phone no.: _____ *Ext.:* _____

If you care to send us a letter, please do so. We always appreciate your comments.

Please fold along dotted lines and tape closed.

northern telecom

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 1024 DURHAM, NC

POSTAGE WILL BE PAID BY ADDRESSEE

Northern Telecom Inc.
Product Documentation
Department 3423 / 200 PPK
P. O. Box 13010
Research Triangle Park, NC 27709

DMS-100 Family
Networks
Maintenance Guide

Product Documentation—Dept 3423
Northern Telecom
P.O. Box 13010
RTP, NC 27709–3010
1–877-662-5669, Option 4 + 1

Publication number: 297-1001-591
Product release: BASE10
Document release: Standard 04.03
Date: March 1999
Printed in the United States of America