**Bellcore**

ⓐ Bell Communications Research

# TCM NETWORK ADMINISTRATION

User Manual

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Copyright Page
Release 8.5

BR 252-573-304
Issue 17, December 1996

Prepared for Bellcore by the User Documentation Design and Development Group.

For further information, please contact:

Bellcore CSC

To obtain copies of this document, Regional Company/BCC personnel should contact their company's document coordinator; Bellcore personnel should call (908) 699-5802.

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Contents
Release 8.5

# TCM Network Administration

# Contents

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

iii

**CONFIDENTIAL — RESTRICTED ACCESS**

**TCM Network Administration**
**Contents**
**Release 8.5**

**BR 252-573-304**
**Issue 17, December 1996**

CONFIDENTIAL — RESTRICTED ACCESS

**BR 252-573-304**
**Issue 17, December 1996**

**TCM Network Administration**
**List of Figures**
**Release 8.5**

# List of Figures

**CONFIDENTIAL — RESTRICTED ACCESS**

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
General
Release 8.5

# 1. General

> **NOTE —** For CSAS documents, any reference to
> "ZRxxxx" should be changed to "VMxxxx". Also, any
> reference to "RMxxxx" should be changed to "MMxxxx".

## 1.1 Document References

This document is one of a series of user manuals that describe the Bellcore CSAS
Communication Module (TCM). These documents are listed below.

| Number | Title |
|---|---|
| 252-573-260 | TCM Online Message Directory |
| 252-573-301 | TCM Overview |
| 252-573-302 | TCM Route Administration (RA) |
| 252-573-303 | TCM Message Administration (MA) |
| 252-573-304 | TCM Network Administration (NA) |
| 252-573-305 | TCM Translation Administration (TA) |
| 252-573-382 | TCM Cron User Manual |
| 252-551-703 | CSAS Interface Data Catalog |
| 252-551-791 | Planning Transition Guide for a SOP to CSAS Interface |
| 252-541-230 | TQS User Manual |

## 1.2 Introduction to Network Administration

The Network Administration (NA) component provides tools enabling the user to monitor
and change the network of communication channels that connect to the TCM. The user
may:

- Create, update (manually or automatically), and delete path information in the SEC
  (System Entity Code) database (VMMPSCDD)

- Monitor the volume of messages handled by TCM

- Manipulate error exception list records in the ADMIN (Administrative Applications)
  database (VMMPAADP).

- Trigger the "automatic link verification" (i.e., physical link verify) and message
  dequeue process.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

1-1

The following figure is an overview of the NA process.
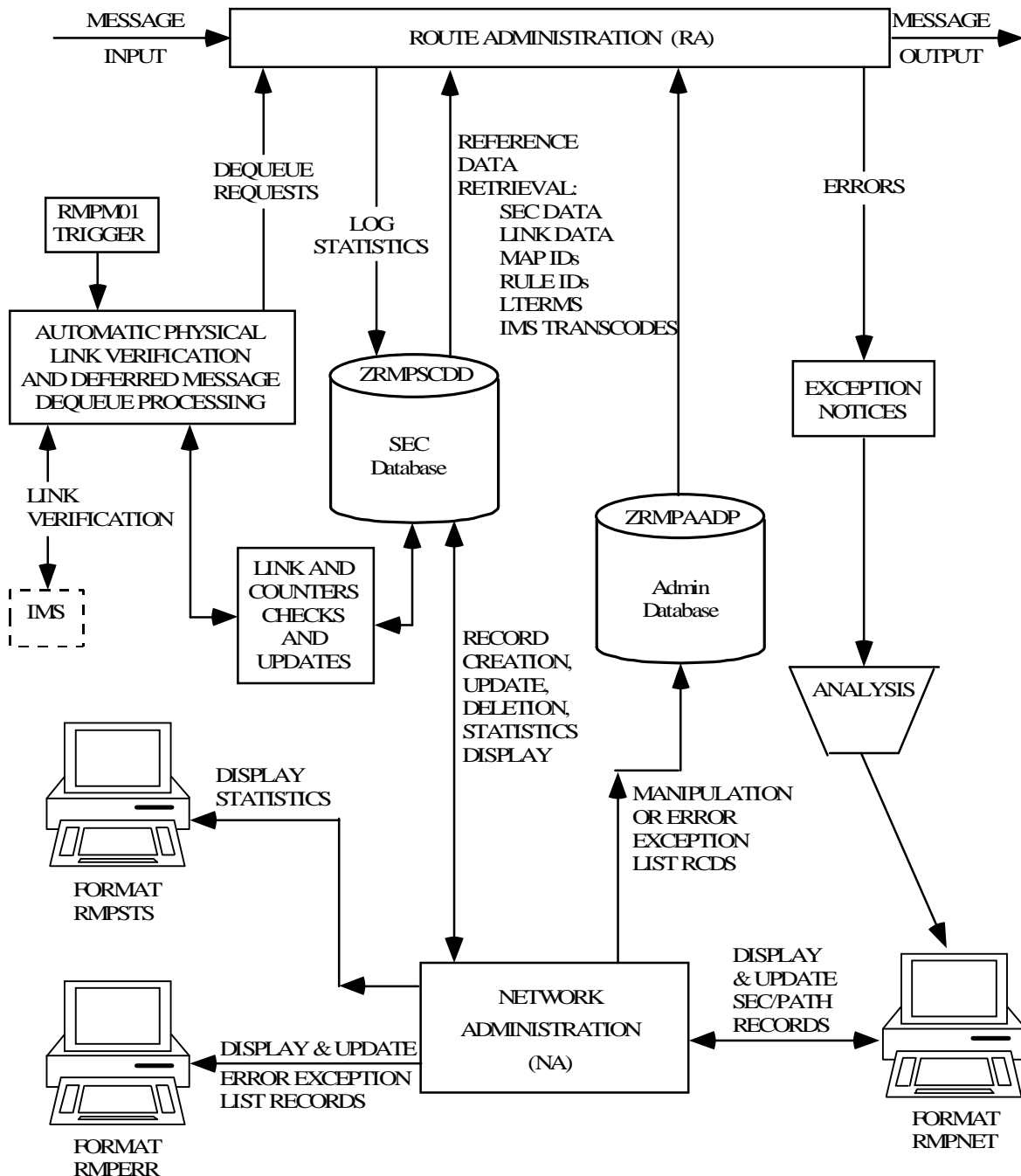
**Figure 1-1.** Network Administration Overview

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

1-2

## 1.3    Security

The Network Administration (NA) component uses the S1 Security System.  This provides a single online display that allows an Administrator to create and update security for all participating NA components.

Security is provided at the logical level, with LTERMS being grouped by the Administrator.  A GROUP is the basic unit to which security is assigned.  Each individual LTERM has the privileges assigned to its respective GROUP.  Privileges are assigned to a GROUP through GRIDS.  GRIDS are two dimensional arrays (e.g., USER ID by function key and command word) whose intersection values define security privileges.  Copies of GRIDS are added to GROUPS and updated by the Administrator.

All terminals used to access an individual component system should be enabled to log in to that component system.  The ability to log in as an Administrator should be reserved for the TCM System Administrator.  Consult your group Security Administrator for further information concerning the S1 Security System.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

**1-4**

## 2.    NA Processing (Manual)

The initial creation and some of the subsequent maintenance of the SEC records and associated path segments within those records is a manual process that is performed via Format MMPNET.

## 2.1    Initial Record Creation

The creation of records in the SEC database is a prerequisite to the activation of TCM in the CSAS System. The data in these records provide information that is essential to RA in performing its task of routing messages between applications.

Data collection must precede the actual task of using Format MMPNET to create records. The data collection consists of three main steps:

1. *SEC Identification*
   A record must be created for every system with which the TCM will communicate. The key to each record will be the SEC (system entity code) of each of those systems. The Network Administrator must identify each of these systems and obtain the codes that have been assigned to each of them. The structure of the SEC code is defined in Bellcore COMMON LANGUAGE® Standard 255. The assignment and maintenance of these codes are BCC responsibilities. *The NA process does not validate the SEC.*

2. *Path Identification*
   A path segment within each SEC record must be created for each category of message that will be sent to or received from that system. The key to each of these path segments is the PATHID and SCENARIO TYPE.

   PATHIDs are mnemonic codes that identify the category of messages that are being transmitted between two application systems.

> **NOTE —** The HELP key (PF11/23) feature of formats MMPNET, MMPSTS or MMPERR provides a description of PATHID that includes the latest set of supported PATHID codes that have been defined for the various interfaces to and from TCM in the CSAS project line. The description also includes the mapping between those codes and various IMS TRANCODEs, TPAM FORMAT IN (input MFD) names, and TPAM FORMAT OUT (output MFD) names.

CONFIDENTIAL — RESTRICTED ACCESS

TCM Network Administration
NA Processing (Manual)
Release 8.5

BR 252-573-304
Issue 17, December 1996

SCENARIO TYPE is a TCM code that indicates the direction the message is being sent and the type of systems involved (TCM/non-TCM). The specific codes are:

| CODE | DEFINITION OF CODE |
|------|--------------------|
| S | TCM (sending) to TCM |
| R | TCM (receiving) to TCM |
| I | Intra-TCM |
| A | TCM to non-TCM |
| Z | non-TCM to TCM |
| N | TCM (sending) to non-TCM (no database safestore) |
| D | application (bypass sending TCM) to TCM |

It must be understood that a combination of PATHID and SCENARIO TYPE must appear in the header portion of every message processed by TCM. This combination is automatically placed in the header by TSYS (the transmitting system, which is the system that originates the message). The Network Administrator must pre-determine which combinations of PATHID and SCENARIO TYPE to expect in these messages and create path segments for them.

> **NOTE —** In the case of a TCM-to-TCM scenario, the sending TCM changes the SCENARIO TYPE code in the message header from "S" to "R".

3. *Path Data Identification*
The many items of data that must be placed in the SEC and path portions of the record are listed in the section of this document that describes Format MMPNET. However, two of these items require special mention:

— *IMS TRANCODE*
TCM cannot just give a message to IMS for delivery to a CSAS System or non-CSAS System application. It must specify the exact transaction within that application that is to receive it. The exact transaction is identified by the specification of an IMS TRANCODE (IMS transaction code).

> **NOTE —** The HELP key (PF11/23) feature of Formats MMPNET, MMPSTS, or MMPERR provides a description of PATHIDs including mapping and IMS TRANCODE information.

— *INPUT MFD and OUTPUT MFD*
TPAM (the TCM Parser and Mapper) cannot directly interpret the data in a message from a CSAS System application (Scenario type "S", "A" or "N" or from a remote sending application that resides in the same IMS control region and bypasses its supporting TCM (scenario type "D") without the aid of an input MFD (Message Format Descriptor). This is because these messages are not in the Flexible Computer Interface Format (FCIF). Instead, they are in either the Mapped

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

2-2

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
NA Processing (Manual)
Release 8.5

Data Area (MDA) or Fixed Fielded (DSECT) format. Likewise, TPAM cannot directly place a message into the internal format (MDA or DSECT) of a CSAS System application (Scenario type "R", "Z" or "D") without the aid of an output MFD.

The Network Administrator will note that the MFD entered into a given path segment must be consistent with both PATHID and SCENARIO TYPE in that segment.

The PATHID specifies the CSAS System application that is sending or receiving the message. The MFD must be correct for that CSAS System application (Scenario type "R", "Z" or "D") or the remote sending application (Scenario type "D").

The SCENARIO TYPE specifies whether the message is being sent or received. An input MFD can only be specified in path records over which messages are to be sent to either a non-TCM or another TCM (Scenario type "A", "S" or "N") or messages are received from a remote sending application that bypasses its supporting TCM (Scenario type "D"). An output MFD can only be specified in path records over which messages have been received for delivery to a CSAS System application (SCENARIO TYPEs "R", "Z" or "D").

> **NOTE —** The HELP key (PF11/23) feature of Formats MMPNET, MMPSTS or MMPERR provides a description of PATHIDs that includes the mapping between them and the latest set of MFDs.

Defining LTERMs to which Exception Notices are to be routed is also performed at the Path level of Format MMPNET. The user should define (at the bottom of the screen) PRIMARY and SECONDARY LTERMS (printers) for the output of exception notices for errors encountered locally, and the REMOTE NOTIFICATION LTERM for the printout of exceptions detected at a remote (receiving) TCM application in a TCM-to-TCM scenario.

## 2.2    Subsequent Record Maintenance

It is expected that the Network Administrator will receive three kinds of input in the daily maintenance of the TCM databases:

- *Exception Notices*
  TCM produces exception notices whenever RA (routing administration) encounters an error while processing a message. An error that points to a missing path, for example, will be given to the Network Administrator for corrective action.

- *Verbal Requests*
  Requests may be received for any number of things, such as turning up or turning

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

2-3

down a given path to a given SEC, adding a RULE ID to the path, or revising an IMS TRANCODE.

- *Statistics Analysis*
  The Network Administrator can monitor the status of the TCM processes via the statistics that RA enters into the SEC database each time it processes a message. These statistics show the current status of the TLOG and SENDQ databases, the total volume of messages processed for the current day (today, up to this moment in time), and the total volume of messages processed the previous day for which TCM processed messages (yesterday). Based on these statistics, the Network Administrator may, for example, wish to turn MAY-I indicators up or down on certain paths to increase or decrease volume during certain times of the day.

  These statistics can be displayed at any time on Format MMPSTS. It is recommended that the statistics be printed each day as TCM automatically resets the path statistics on processing the first message of the day for that path.

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
NA Processing (Automatic)
Release 8.5

# 3. NA Processing (Automatic)

The three automatic processes that update the SEC database are discussed in the following subsections.

- Physical Link Verification and Dequeue of Deferred Messages

- Resetting of Statistical Counters

- Logical Flag Manipulation

## 3.1 Physical Link Verification and Dequeue of Deferred Messages

### 3.1.1 Physical Links

The physical communication channel (link) over which a message is transmitted is identified in the path segment of a SEC record in the LINK NAME field. Three link types are valid: MSC (Multiple System Coupling), a special link called ISC (Inter System Communications), and LU6.2 (APPC).

There are two indicators of a link's status. The CAN-I indicator specifies whether a link is *physically* available. The MAY-I indicator specifies whether it is currently acceptable for TCM to use the link. For example, a link's CAN-I indicator may indicate "Y", the link is available, but the MAY-I indicator may be set to "N" because the host at one end of the link is about to go down for maintenance.

### 3.1.2 Deferred Messages

During the processing of a message being sent from TCM, the RA process checks the CAN-I and MAY-I indicators in the SEC database to determine if the communication path over which the message is to be sent is turned up or down. If either of these indicators is turned down, RA defers the message. (The process of deferring a message under this condition is called a "link deferral.") This causes the message to be stored in the SENDQ database. It also causes the statistics field (in the SEC database) that contains the number of messages in SENDQ to be incremented by one. The MMPSTS screen field corresponding to this statistic is DEFERRED.

A message will also be deferred if there are any previous "link deferred" messages stored in SENDQ for this path.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

3-1

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
NA Processing (Automatic)
Release 8.5

BR 252-573-304
Issue 17, December 1996

### 3.1.3    Link Verification and Dequeue Process

At regular intervals during the day a BMP run, VMMPM01, can trigger the automatic link verification and deferred message dequeue process (VMMPNP).

> **NOTE —** The link verification process uses the IMS DISPLAY command to determine whether MSC, LU6.2, and ISC links are active. Therefore, it is imperative that VMMPNP have IMS security to issue the DISPLAY command. If VMMPNP does not have the proper security, all CAN-I flags will be changed to "N", regardless of the actual status of any link, and all messages will be deferred indefinitely. In order to grant DISPLAY authority to VMMPNP, two control cards must be included in the IMS Security Maintenance Utility Run. In the following display, "ƀ" stands for a blank space and the control card information begins in column one.
>
>     )(ƀ CTRANSƀ VMMPNP
>     ƀ TCOMMANDƀ DISPLAY

This link verification and dequeue process operates in several steps, as follows:

1. The CAN-I status of each physical link (MSC, LU6.2, or ISC LTERM) is compared with the actual status of that link or LTERM in the Information Management System (IMS). If the actual status is different, the CAN-I status is updated to agree with IMS. In addition, if the queue count for a link is above the maximum set in the TTS table (TCM User Control), the CAN-I will be set to N.

2. The MAY-I (in both SEC and path segments) and CAN-I links in each SEC record are checked. If the indicators are turned up (set to "Y"), the statistics field that contains the number of messages in SENDQ is checked. If this is greater than zero, a request is sent to RA to begin re-processing messages that were deferred for this "defer path (RSYS-PATHID-LINKNAME)." The request also includes the maximum number of messages that should be dequeued at this time. The maximum number is called the DEQUEUE COUNT. Both the dequeue count and the statistics counter for DEFERRED messages are found in the path segment of the SEC record.

3. The RA component retrieves messages from the SENDQ database and processes them. For each message that is processed, RA updates the appropriate statistics fields in the SEC database, including decrementing the field that contains the number of messages in SENDQ. The RA component will process a number of messages less than or equal to the dequeue count. The dequeue activity is the smaller of the number of deferred messages for a particular interface path or the dequeue count for that path.

4. The process is repeated until all SEC records and all paths within those records have been checked and dequeued up to their specified DEQUEUE COUNT.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

3-2

## 3.2     Resetting of Statistical Counters

It is important to network administration to be able to monitor the status of the TCM processes at all times. This is done by having those processes update the SEC database with statistics that show how many messages reside in TCM at each moment during the day along with statistics that show total message volumes processed for both today and yesterday. These statistics are automatically updated each time a message is processed.

The NA component provides BMP run VMMPM07, which resets the "CURRENT MSG STATUS" display statistics to reflect the message volumes in the SENDQ and TLOG databases. For complete information on this process, please refer to BR 252-573-507, the Statistics Resynchronization Process, the runbook that covers VMMPM07.

## 3.3     Logical Flag Manipulation

The BMP run VMMPM01 can trigger transaction VMMPNM, the Logical Flag Manipulation Process, which sets TCM's MAY-I flags to either "Y" or "N" at the user's discretion. Before exiting, VMMPNM activates VMMPNP, the link verification and dequeue process.

Typically, during peak traffic hours, certain MAY-I flags (Format MMPNET) are turned off (values set to "N"), preventing messages from being sent via the corresponding links. These links may be turned back up (MAY-I values changed to "Y") when traffic is lighter. In this way, TCM can defer some or all of its own messages, either to give certain messages priority, or to yield resources to other applications that share the communications links. Changing the flags, of course, does not actually change the link itself, but will control the operation of the link verification and dequeue process, VMMPNP, which should be run at regular intervals. Users wishing to vary messaging activity on a regular basis should consider use of VMMPNM.

VMMPNM is used to set the MAY-I flags automatically. For example, during the regular working hours, say 8 AM until 5 PM, TCM normally processes a large volume of messages. But some of these messages may not be needed by the receiving application at the time they are generated; perhaps the receiving application only processes them once a day, at 11 PM. System resources would be most efficiently used if such messages were deferred until hours of peak activity had passed, and "urgent" messages had been delivered. If "non-urgent" messages can, by some combination of SEC, PATHID and Scenario Type, be distinguished from urgent messages, then VMMPNM can automatically cause TCM to store the non-urgent messages in the SENDQ database until a user-specified time. When VMMPNM is again (automatically) invoked, and has set the MAY-I flags back to "Y", it will activate VMMPNP, the link verification and dequeue process, just before it exits.

The logical flag manipulation process may be triggered in either of two ways:

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

3-3

- Via the Cron screen, Format MMPCRN, which will insert records into the Cron database

- Via control cards in the trigger BMP (VMMPM01)

Both methods (MMPCRN and control cards) can be used to trigger the logical flag manipulation process in local or remote TCMs. In either case, the user must supply information that specifies the:

- Target system (the TCM that will receive the command)

- SEC (on the target system) that will be affected

- PATHID (on the target system) that will be affected

- SCENARIO TYPE (on the target system) that will be affected

- Trancode of the of the logical flag manipulation process.

The destination (target system) is specified by the trancode and the link name. If the command is to be transmitted to a TCM that resides in another control region of the same host or a different host, then a link name must be supplied. This link name specifies the control region that will execute the trancode when received. If no link name is present the trancode will be delivered to a TCM within the same control region as the sending TCM. Whether the receiving TCM is local or not, it is the name of the trancode itself that specifies the name of the application that hosts the TCM that will receive the trancode. All of the following trancodes represent the logical flag manipulation process, known to the present user as VMMPNM, as it is named in each of the corresponding applications. Select the appropriate trancode for the application that is to accept it from the following list:

|         |         |
|---------|---------|
| TIRKS   | VMMPNM  |
| NSDB    | VJMPNM  |
| CSAS    | VMMPNM  |
| PICS    | VPMPNM  |
| WFA/DO  | VGMPNM  |
| WFA/C   | VOMPNM  |
| WFA/DI  | YXMPNM  |
| 3DS     | VZMPNM  |

The methods of transmitting the command to initiate the logical flag manipulation process to another TCM are described in the following subsections. In these descriptions, the logical flag manipulation process is referred to as "xxMPNM". The "xx" is to be replaced by the appropriate value obtained from the foregoing list.

> **WARNING —** It is **imperative** that any users planning to execute logical flag manipulation on a TCM other than "their own" obtain, **in advance**, the permission and complete cooperation of the Administrators of the receiving TCM.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

3-4

### 3.3.1    Logical Flag Manipulation via Format MMPCRN

Enter the data in the following list in the TRANSACTION AND DATA TO BE
SCHEDULED field at the bottom of the screen. (For complete information on Format
MMPCRN, please refer to BR 252-573-382, the TCM Cron User Manual.) Enter the name
of the transaction, xxMPNM, in the IMS TRAN CODE field near the top of the screen.

| INFORMATION | POSITION | VALUE |
|---|---|---|
| Transaction code | 1-8 | xxMPNM |
| SEC name | 9-16 | alphanumeric |
| Spacer | 17 | blank |
| PATHID | 18-25 | alphanumeric |
| Spacer | 26 | blank |
| Scenario Type | 27 | alphabetic |
| Spacer | 28 | blank |
| SEC to (MAY-I) | 29 | "Y", "N", or blank |
| Spacer | 30 | blank |
| SEC from (MAY-I) | 31 | "Y", "N", or blank |
| Spacer | 32 | blank |
| PATH status (MAY-I) | 33 | "Y", "N", or blank |

**Figure 3-1.** Format MMPCRN Data

Figure 3-2 shows Format MMPCRN completed with information that will enable TCM to
send messages to a non-TCM system (scenario type "A") known by the SEC
"LOCALSEC" via the PATHID "LOCALNMA". All MAY-I flags are set to "Y". This
command is not being sent from one TCM to another, but merely from MMPCRN to "its
own" VMMPNM. Thus, the MSC name is left blank, and the usual name of the logical flag
manipulation transaction, VMMPNM, is supplied. In the figure, "b̷ " stands for a blank
space.

```
           * CSAS-TCM: CRON COMMUNICATION (MMPCRN) *
 COMMAND:                              /FOR
           SCHEDULING INFORMATION        96.225  08/12/96
 IMS TRAN CODE: VMMPNM       USER KEY:                    19:16:11

      (CCYYMMDD)          (HHMM)
 START DATE: 19960901    START TIME:0830
  END DATE: 19960930     END TIME:


      (HHMM)             (NN)
 INTERVAL TIME:        DAY OF MONTH:       MSCNAME:

 WEEK DAY(S):  ALL y   SUN   MON   TUE   WED   THU   FRI   SAT




        TRANSACTION AND DATA TO BE SCHEDULED
       (REQUIRED FOR ADD OR UPDATE. 200 BYTE MAX)
 xxmpnm/b/blocalsecbloc/lnmababyb/yb/  /  /


 1/13-FIND  4/16-ADD  5/17-UPDATE  8/20-REFRESH  10/22-DELETE  11/23-HELP
```

**Figure 3-2.** Scheduling a Local Logical Flag Manipulation Transaction

CONFIDENTIAL — RESTRICTED ACCESS

**BR 252-573-304**                                                      **TCM Network Administration**
**Issue 17, December 1996**                                             **NA Processing (Automatic)**
                                                                        **Release 8.5**

In the next example, the instruction will be sent from one TCM to another TCM in the *same* IMS control region. The following figure shows Format MMPCRN completed with information that will prevent TCM from sending messages to a TCM (scenario type "S") known by the SEC "THIRDSEC" via the PATHID "OPDTONMA". All MAY-I flags are set to "N". Because the message will be delivered within the control region in which it originated, the MSC link is left blank, and the exact identity of the receiving application is determined solely by the value of "xx" as detailed above. In the figure, "ɓ" stands for a blank space.

```
                    * CSAS-TCM: CRON COMMUNICATION (MMPCRN) *
COMMAND:                           /FOR
              SCHEDULING INFORMATION      96.225  08/12/96
IMS TRAN CODE: xxMPNM      USER KEY:                 19:16:11

    (CCYYMMDD)          (HHMM)
START DATE: 19960901   START TIME:0830
 END DATE: 19960330    END TIME:

    (HHMM)              (NN)
INTERVAL TIME:      DAY OF MONTH:       MSCNAME:

WEEK DAY(S): ALL y   SUN   MON   TUE   WED   THU   FRI   SAT



    TRANSACTION AND DATA TO BE SCHEDULED
    (REQUIRED FOR ADD OR UPDATE. 200 BYTE MAX)
xxmpnmɓɓthirdsecɓopdtonmabsbnɓnɓn/  /



1/13-FIND  4/16-ADD  5/17-UPDATE  8/20-REFRESH  10/22-DELETE  11/23-HELP
```

**Figure 3-3.** Scheduling a Remote Logical Flag Manipulation Transaction

The "xx" in both the following and preceding examples must be replaced by the character strings previously specified.

The following logical flag manipulation transaction will be received by a TCM in a *different* IMS control region than the sending TCM. The name of the TCM host application will be determined by the user-supplied value of "xx". The following figure shows Format MMPCRN completed with information that will prevent TCM from sending messages to a TCM (scenario type "S") known by the SEC "THIRDSEC" via the PATHID "OPDTONMA". All MAY-I flags are set to "N". The message will be sent via an MSC link known as "MSC1615". In the figure, "ɓ" stands for a blank space.

```
                * CSAS-TCM: CRON COMMUNICATION (MMPCRN) *
   COMMAND:                        /FOR
              SCHEDULING INFORMATION       96.225  08/12/96
   IMS TRAN CODE: xxMPNM       USER KEY:                19:16:11

       (CCYYMMDD)        (HHMM)
   START DATE: 19960901    START TIME:0830
    END DATE: 19960930    END TIME:

        (HHMM)          (NN)
    INTERVAL TIME:        DAY OF MONTH:        MSCNAME: msc1615

    WEEK DAY(S): ALL y   SUN   MON   TUE   WED   THU   FRI   SAT




        TRANSACTION AND DATA TO BE SCHEDULED
        (REQUIRED FOR ADD OR UPDATE. 200 BYTE MAX)
   xxmpnmbbthirdsecbopdtonmabsbnbnbn  /   /



    1/13-FIND  4/16-ADD  5/17-UPDATE  8/20-REFRESH  10/22-DELETE  11/23-HELP
```

**Figure 3-4.** Scheduling a Remote Logical Flag Manipulation Transaction

The "xx" in the preceding example must be replaced by the character strings previously specified. Because the user has supplied an MSC name, this logical flag manipulation transaction will be received by a TCM that resides in a different IMS control region (and perhaps a different host computer as well) than the sending TCM.

### 3.3.2    Logical Flag Manipulation via Control Cards

Control cards may be used to trigger this logical flag manipulation process whether or not it is to be executed in the same IMS copy as the Cron. However, the control cards required are slightly different depending upon which situation exists. In either situation, if the MAY-I fields are left blank, their default setting is "Y".

3.3.2.1     Control Card Manipulation of Local Flags

This list of control card values should be used when the SEC or path the user wishes to manipulate is in the *same IMS control region* as the user's TCM. Whether or not this TCM

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

3-8

is the same as the "user's own" TCM is immaterial. The receiving application will be
determined by the value of "xx".

| INFORMATION | POSITION | FORMAT/VALUE |
|---|---|---|
| transaction code | 1-8 | xxMPNM |
| starting time | 9-12 | hhmm |
| ending time | 13-16 | hhmm |
| interval time | 17-20 | hhmm |
| SEC name | 21-28 | alphanumeric |
| spacer | 29 | blank |
| PATHID | 30-37 | alphanumeric |
| spacer | 38 | blank |
| Scenario Type | 39 | alphabetic |
| spacer | 40 | blank |
| SEC to (MAY-I) | 41 | "Y", "N", or blank |
| spacer | 42 | blank |
| SEC from (MAY-I) | 43 | "Y", "N", or blank |
| spacer | 44 | blank |
| PATH status (MAY-I) | 45 | "Y", "N", or blank |

Following is an example of a control card that will schedule the transaction locally (in the
same IMS copy as the TCM). This control card will cause TCM to start sending messages
at 6 PM to a non-TCM (scenario type "A") known by the SEC "THIRDSEC" via the
PATHID "OPDTONMA". All MAY-I flags are set to "Y"; the SEC MAY-I flags by
default (control card has blanks), and the PATH MAY-I by the control card specifying "Y"
in position 45. In the figure, "ƀ" stands for a blank space.

xxMPNMƀ ƀ 1800ƀ ƀ ƀ ƀ ƀ ƀ ƀ THIRDSECƀ OPDTONMAƀ Aƀ ƀ ƀ ƀ ƀ Y

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

3-9

3.3.2.2      Control Card Manipulation Of Remote Flags

If the control card is to trigger the process in a different IMS control region, regardless of host, the following values must be used.

| INFORMATION | POSITION | FORMAT/VALUE |
|---|---|---|
| transaction code | 1-8 | xxMPNM |
| starting time | 9-12 | hhmm |
| ending time | 13-16 | hhmm |
| interval time | 17-20 | hhmm |
| "literal" | 21-28 | MSCNAME= |
| MSC name | 29-36 | alphanumeric |
| SEC name | 37-44 | alphanumeric |
| spacer | 45 | blank |
| PATHID | 46-53 | alphanumeric |
| spacer | 54 | blank |
| Scenario Type | 55 | alphabetic |
| spacer | 56 | blank |
| SEC to (MAY-I) | 57 | "Y", "N", or blank |
| spacer | 58 | blank |
| SEC from (MAY-I) | 59 | "Y", "N", or blank |
| spacer | 60 | blank |
| PATH status (MAY-I) | 61 | "Y", "N", or blank |

Following is an example of a control card that will schedule the transaction in a different control region. This control card will cause TCM to start sending messages at 9 PM to a TCM (scenario type "S") known by the SEC "THIRDSEC" via the PATHID "OPDTONMA". All MAY-I flags are set to "Y"; the SEC MAY-I flags by default (control card has blanks), and the PATH MAY-I by the control card specifying "Y" in position 45. This instruction will be sent over the MSC link known as "MSC1615".  In the figure, "ƀ " stands for a blank space.

xxMPNMƀ ƀ 2100ƀ ƀ ƀ ƀ ƀ ƀ ƀ MSCNAME=MSC1615ƀ THIRDSEC ƀ OPDTONMAƀ Sƀ ƀ ƀ ƀ ƀ Y

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

3-10

# 4. TCM Messages Stuck In Held Status

## 4.1 General

The purpose of TCM's Hold processing is to sequence messages delivered to the receiving system so that "associated" messages are delivered in the order sent from the sending system. Held messages are to be processed sequentially, such that until a prior "associated" message is positively acknowledged to TCM, no subsequent associated message is released to the receiving system. Messages are considered "associated" when the values of certain name=value pairs in the TCM Route Control (ROUTCTL) section of the message are identical. These fields are Remote SEC (TSYS for Hold processing in the receiving system or RSYS for Hold processing in the sending system), Scenario Type (SCTYPE), Activity Number (ACNO), and optionally PATHID.

In order to process messages sequentially, a secondary index (VMMPTLP1) exists for the TLOG database (VMMPTLDD). The secondary index is keyed by ACNO, Message Timestamp and SEC. TCM's Route Administration (RA) checks this secondary index when it processes a data message to see if a record exists in TLOG with the same ACNO. If one or more records exist, then RA will determine if the current message is associated to them by checking their TSYS or RSYS, SCTYPE and optionally PATHID. If the data message is "associated" to any existing TLOG record, then the message is placed into TLOG in Held status. During acknowledgment processing, RA will check the secondary index to see if an associated Held message exists to be released.

Sometimes TCM transactions are parallel scheduled into multiple IMS regions. Parallel scheduling means that the RA process can be executing in more than one message region at the same time. When many messages are being processed in TCM for the same ACNO with Hold processing, data base activity is occurring at the same time for the same set of data base records.

In order to avoid IMS deadlock situations in the RA transactions, data base records are allowed to be read from the secondary index without "reliability", so that contention is not an issue to IMS. This means that during parallel scheduling, IMS allows a transaction in one region to see uncommitted data in another region. This results in a "Held Message Problem". This problem occurs when a message and acknowledgment that are "associated" are processing simultaneously in different message regions. A data message has already been processed by TCM and delivered to a local application or remote system. A second, associated data message begins processing in one region and sees the TLOG record (of the first data message) waiting to be acknowledged, through the secondary index. The second data message is, therefore, placed into *Held* status. However, before the second data message finishes and commits the Held message into TLOG, the acknowledgment of the first data message processes in its entirety in a second region, deleting the TLOG record that caused the second data message to be marked as Held. Since the Held message from the first region is not yet in TLOG, the acknowledgment in the second region will never see

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

4-1

and release it. Once the first region commits the Held message to TLOG, it will remain there indefinitely since no earlier pending acknowledgment message will exist to release it. Any additional messages received by TCM, associated with the same ACNO, will also remain in Held status behind the first Held message.

## 4.2    Releasing Stuck Held Messages

The Held Message Release transaction, VMMPHLD, releases only stuck Held messages. It reads a TLOG secondary index (VMMPTLP3) finding only Held messages where the earliest associated message is in Held status, and it releases this earliest message. The positive acknowledgment of the first message will begin a processing chain of events that will release all of the associated Held messages. The VMMPHLD transaction is beneficial because it releases Held messages in a timely fashion through automatic scheduling via the TCM Cron, and it releases only stuck Held messages, not messages Held by errors or Pending Acknowledgment messages.

Execution of the VMMPHLD transaction requires no input message text. It may be executed by entering the transaction names, VMMPHLD, followed by a space, from a clear screen during an IMS session. For example:

<div align="center">VMMPHLDⷬ</div>

By default, the transaction will only release stuck Held messages whose timestamps are less than seven (7) days old. This transaction is intended to clear stuck Held messages frequently by scheduling the transaction via the TCM Cron (e.g., every 10-30 minutes). Therefore, the default processing will not address messages greater than seven days old. Should there be a need to alter the time frame for which messages are eligible for selection, then the keyword DATE= may be supplied as message text. The keyword DATE=ALL will cause the transaction to release all stuck Held messages, regardless of the message timestamp. For example:

<div align="center">VMMPHLDⷬ DATE=ALLⷬ</div>

The keyword DATE=yyddd will release any stuck Held message with a timestamp equal to or greater than the Julian date specified by yyddd. The following will release any stuck Held message with a timestamp equal or greater than February 1, 1991.

<div align="center">VMMPHLDⷬ DATE=91032ⷬ</div>

The default processing should be acceptable under normal circumstances. It may be desirable to use the DATE=ALL keyword once, if for some reason, the VMMPHLD transaction had not been scheduled via the TCM Cron for some period of time.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

4-2

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPNET Description
Release 8.5

# 5.    Format MMPNET Description

## 5.1    General

Format MMPNET is accessed either by typing "/FOR MMPNET" on a blank screen and pressing the ENTER key, or via the MMPNET key on Format MMPSTS, or via the MMPNET key on format MMPERR.

The screen layout is shown below.

```
* CSAS-TCM: NETWORK ADMINISTRATION (MMPNET) *  /FOR      PAGE   1
 SEC:       PATHID:      SCENARIO TYPE:  96.256 DATE 09/12/96
                              TIME 17:47:02
********** SEC  INFORMATION **********
 SEC TYPE:  APPL HEADER:  RELEASE LEVEL:
LINK STATUS   (TO) MAY-I:    (FROM) MAY-I:
 PROCESSING LEVEL  RESEND:       HOLD:
 DESCRP:
 STATISTICS:
         ********* PATH  INFORMATION *********
                 (MYSEC)
  MESSAGE CLASS:        RULE ID:
    LINK TYPE:        LINK NAME:
LINK STATUS MAY-I:     LINK STATUS CAN-I:
  DEQUEUE COUNT:        INPUT MFD:
    TRANCODE:        OUTPUT MFD:
 TCM ERROR LDEST:      APP ERROR LDEST:
             DEF OFFSET:  -
  *** LTERMS FOR EXCEPTION NOTICES ***
  PRIMARY:       SECONDARY:      REMOTE NOTIFICATION:

1/13 FIND  2/14 NEXT PATH  3/15 MMPPLEX  4/16 ADD  5/17 UPDATE 6/18 NEXT SEC
7/19 MMPERR  8/20 REFRESH   9/21 MMPSTS  10/22 DELETE      11/23 HELP
```

**Figure 5-1.** Format MMPNET

| FIND | FWD | MMP-PLEX | ADD | UPDT | NEXT | MMPERR | RFSH | MMPSTS | DEL | HELP | PRNT |
|------|-----|----------|-----|------|------|--------|------|--------|-----|------|------|
| PF1 | PF2 | PF3 | PF4 | PF5 | PF6 | PF7 | PF8 | PF9 | PF10 | PF11 | PF12 |
| PF13 | PF14 | PF15 | PF16 | PF17 | PF18 | PF19 | PF20 | PF21 | PF22 | PF23 | |

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

5-1

CONFIDENTIAL — RESTRICTED ACCESS

TCM Network Administration
Format MMPNET Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

The upper part of the screen contains information about the operating system with which the CSAS System (via TCM) must communicate. That system may or may not communicate via TCM. The other system is identified by its SEC (System Entity Code) which is referred to as a "remote SEC."

The lower part of the screen contains information about a single logical interface path to and/or from that SEC and the LTERMs designated to receive Exception Notices.

There are no command words used with this format.

## 5.2     Function Keys

### 5.2.1     FIND Function Key (PF1/13)

- SEC
  This is the system entity code of the system with which the CSAS System (via TCM) will communicate. That system may or may not communicate via TCM. The entry of this search criteria will cause the retrieval of the SEC record and the display of only the SEC portion of that record in the upper part of the screen. If no value is provided in the SEC field, then the first SEC in the SEC database (VMMPSCDD) will be displayed. (VMMPSCDD is an HDAM database, which provides quickest access to any named record. Because of the way in which HDAM databases are organized, the first record encountered may be literally any record in the database. HDAM databases are written in no user-oriented order. The HDAM technique itself tracks the location of each individual record.) The NEXT key can then be used to find and display succeeding SEC records in the database one at a time.

- SEC, PATHID, and SCENARIO TYPE
  These three entries will cause the retrieval of the SEC record, the display of the SEC portion of that record in the upper part of the screen, and the display of one of the paths in that record in the lower part of the screen. The particular path displayed is determined by the given PATHID and SCENARIO TYPE. The FORWARD key can then be used to find and display succeeding paths in that same record one at a time, or the NEXT key can be used to find and display the next SEC record in the database. The FIND key also produces and displays a simple sketch on line 11 of the screen that indicates the relationship of "MYSEC" to the SEC in the record, and also indicates the direction of message transmission on the path. The patterns that this sketch can assume are:

  - SECx------------->SECy (MYSEC)
    This sketch shows the communication path running from SECx to "MYSEC". Note that "MYSEC" is identified both by its actual system entity code (SECy) and the literal (MYSEC).

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

5-2

- SECx  <-------------SECy (MYSEC)
  This sketch shows the communication path running from "MYSEC" to SECx.
  Note that "MYSEC" is identified both by its actual system entity code (SECy) and
  the literal (MYSEC).

- SECa>-INTRA SEC--<SECa (MYSEC)
  This sketch shows the communication path lying entirely within "MYSEC". Note
  that the actual system entity code of "MYSEC" is displayed.

> **NOTE —** The TCM process that creates these sketches
> obtains the correct system entity code for "MYSEC" from
> the TTS Table called TCM USER CONTROL.

### 5.2.2    FORWARD Function Key (PF2/14)

A SEC record must be retrieved and displayed by the FIND key prior to the operation of
the FORWARD key. If the FIND key action does not retrieve and display a given path, the
operation of the FORWARD key will retrieve and display the first path in the record.
Succeeding operations of the FORWARD key will find and display succeeding paths in
that same record one at a time. Once the last record is reached, FORWARD generates a
warning message.

### 5.2.3    MMPPLEX Function Key (PF3/15)

This key is used to switch the user from this MMPNET screen to the MMPPLEX screen.
This switch is to find any Control Region names which are having problems delivering
messages over MSC/ISC/LU6.2 links.  The SEC, PATHID and SCENARIO TYPE must
be populated in order to display this information.  The MMPPLEX screen is ignored by
TCM unless the SYSPLEX field on the TTS Table: TCM USER CONTROL is a 'Y'.

### 5.2.4    ADD Function Key (PF4/16)

This key is used to create a record in the SEC database. The record that is created may
contain only a SEC segment, or may contain both the SEC segment and the first path
segment.

The ADD key can also add path segments to an existing SEC record in the database.

The required fields for creating a SEC segment in the record are:

- SEC
  Not validated; however, the standard established for defining valid SECs is described
  by the online HELP feature.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

5-3

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Format MMPNET Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

- SEC TYPE
  Validated: must be T (TCM), N (non-TCM), S (SOAC) or P (PAWS).

- PROCESSING LEVEL    RESEND:    HOLD:
  Validated: must be S or P

Optional input fields include:

- APL HEADER
  Send SOAC Application Header Section (C3) with data. (Used only for SOAC - CSAS systems.)

- DEF OFFSET

  — Validated: must be in HH:MM format. Valid entries are 23 - 00 for HH and 00 - 59 for MM. This will add the Deferred Time amount for messages over a specific path, thereby, delaying their delivery. (This should be used for the WFA/NSDB interface).

  — Default for an ADD or UPDATE is 00-00.

- DESCRP
  Not validated: a 40-character free-format field.

- RELEASE LEVEL
  The release level is not validated. It is required for SEC TYPE = T.

- (TO) MAY-I and (FROM) MAY-I
  Validated: must be N (no) or Y (yes). Defaults to Y, if no entry is provided.

- STATISTICS
  Validated: can be "Y", "N" or blank. A blank entry will default to "Y". "Y" or Blank will keep all statistics for this SEC.  "N" turns off all statistics counters for this SEC except for the current message deferred count, however, no statistics may be viewed. If the flag is changed from a "N" to a "Y", then the only correct statistics count on the MMPSTS screen is the current deferred count. It is necessary to execute the BMP run VMMPM07 to resync all the current message statistics. However, this run will not resent the total message volume statistics.

The required fields for creating a path segment within the record are:

- PATHID
  Not validated

- SCENARIO TYPE
  Validated: must be S, R, A, Z, I, N or D. If I must also be message class 2 or class 5.

**CONFIDENTIAL — RESTRICTED ACCESS**

BR 252-573-304     TCM Network Administration
Issue 17, December 1996     Format MMPNET Description
    Release 8.5

- MESSAGE CLASS
  Validated: must be 1, 2, 3, 4 or 5.

| CLASS | MEANING |
|:-----:|---------|
| 1 | application-to-application message. |
| 2 | application-to-TCM FCIF acknowledgment. |
| 3 | application-to-application DSECT or MDA grouped message. |
| 4 | application-to-application message where only the "ROUTCTL" is message switched. |
| 5 | application-to-TCM DSECT acknowledgment. |

- INPUT MFD or OUTPUT MFD
  These fields are required for all message classes. In the case of *some class 2 message paths*, TCM-supplied default values are acceptable.

  For all message classes, these fields are validated in two ways. First, the entry must be consistent with the given SCENARIO TYPE.

| SCENARIO TYPE | REQUIRED ENTRY |
|:-------------:|----------------|
| S | TPAM FORMAT IN (INPUT MFD) |
| R | TPAM FORMAT OUT (OUTPUT MFD) |
| A | TPAM FORMAT IN (INPUT MFD) |
| Z | TPAM FORMAT OUT (OUTPUT MFD) |
| I | TPAM FORMAT not permitted |
| N | TPAM FORMAT IN (INPUT MFD) |
| D | TPAM FORMAT IN (INPUT MFD) AND TPAM FORMAT OUT (OUTPUT MFD) |

  Second, the Message Format Descriptor (MFD) must exist.

- (IMS) TRANCODE
  This field is required for all message classes except Class 2,
  SCTYPE = I messages.
  It is required for class 2 message paths if *one* of the following is true:

  — The originating (TCM or non-TCM) system wishes to receive an acknowledgment message in FCIF as specified by the presence of the fields EPATHID and/or PPATHID in the class 1 message header.

  — The originating (TCM) system wishes to receive an acknowledgment message (in FCIF) from its TCM when TCM receives an acknowledgment message from a receiving non-TCM system. This is based on the presence of the field EPATHID and/or PPATHID in the class 1 message header.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

**5-5**

— The originating system wishes to receive exception notices for errors encountered at the receiving TCM based upon the presence of the field EPATHID (generated when the Remote Notification LTERM is specified in the path segment for the class 1 message "S" scenario path) in the Class 1 message header.

TRANCODE validation is determined by LINK TYPE. A blank LINK TYPE refers to the local TCM. (The TRANCODE is then validated against the local IMS.) A non-blank LINK TYPE implies a remote application, so validation is limited to checking for a non-blank TRANCODE.

Optional input fields include:

- LINK TYPE
  Validated: must be M (for MSC), I (for ISC), L (for LU6.2), or blank. Note that an entry of I will be accepted by TCM even if the system is not equipped with the TCIS software. In such cases, TCM will determine that the link is *currently* unavailable, and will simply defer transmission indefinitely.

- LINK NAME
  Validated: must exist and be known to the local IMS system that contains this TCM. In addition, no entry is permitted unless LINK TYPE = M, L, or I (non-blank).

- RULE ID
  Validated: must exist and be known to the local IMS system that contains this TCM.

- LINK STATUS MAY-I (Indicator)
  Validated: must be N (no) or Y (yes). If no entry is provided, defaults to "Y" for "S", "A", "Z", "R", "N" and "D" scenario message paths. Must be blank for "I" scenario message paths.

- LINK STATUS CAN-I (Indicator)
  No entry permitted.   If a LINK NAME and LINK TYPE are removed from the MMPNET screen, the CAN-I flag is set to "Y".  If a LINK NAME and LINK TYPE are added, the TCM AIB Services determines if the link is started or stopped.

  If the link is started, the link will be added to the SEC database, and the message "add successful" is displayed.

  If the link is stopped, the UPDATE (PF5/17)/ADD (PF4/16) of the MMPNET screen changes the CAN-I flag to "N".

- DEQUEUE COUNT
  Not validated.

**CONFIDENTIAL — RESTRICTED ACCESS**

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPNET Description
Release 8.5

— Defaults to 50 for "S", "Z", "R", "N" and "D" Scenario types for all class messages.

— Defaults to zero (is not applicable) for class 2 or 5, with SCTYPE "I".

- TCM ERROR LDEST
  Applicable only to Class 1, 3 and 4 messages of "A", "Z", "R" and "D" scenarios. Not permitted for Class 2 and 5 message paths. To handle both TCM and Application error message acknowledgments. Used in SOAC interfaces to populate the LDEST= parameter in the acknowledgment message.

- APPLICATION ERROR LDEST
  Applicable only to Class 1, 3 and 4 messages of "A", "Z", "R" and "D" scenarios. Not permitted for Class 2 and 5 message paths. Used in SOAC interfaces to populate the LDEST= parameter in the acknowledgment message.

- PRIMARY, SECONDARY, and REMOTE NOTIFICATION (LTERMs)
  Validated: must exist and be known to the local IMS system that contains the TCM. In addition, a SECONDARY LTERM cannot be added without adding a PRIMARY LTERM. The REMOTE NOTIFICATION LTERM is valid only for class 1 and 3 "S" scenario message paths. If no PRIMARY ERROR LTERM is specified, errors are routed to the TSA LTERM (specified in the TCM USER CONTROL TABLE within TTS). All three must be blank for class 2 message paths. All local LTERM error printing can be suppressed by typing "NONE" in the PRIMARY LTERM field. This feature is for limited testing situations.

### 5.2.5    UPDATE Function Key (PF5/17)

This key is used to change data in existing records in the SEC database. Data can be changed in both the SEC segment and the path segment, either individually or together. All changes must pass the same validations that are listed under the ADD key.

All fields can be changed except LINK STATUS CAN-I and the three fields that define the SEC and path segments (SEC, PATHID, and SCENARIO TYPE).

> **WARNING —** When updating the DEF OFFSET field value to a lesser amount, if there are deferred messages for this path, it may cause sequencing errors when there are new incoming messages for the same Activity Number (ACNO), which are deferred for a lesser amount of time than messages already in the database.

A SEC record must be retrieved and displayed by the FIND key prior to the operation of the NEXT key. The NEXT key is then used to find and display succeeding SEC records in

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

5-7

CONFIDENTIAL — RESTRICTED ACCESS

TCM Network Administration
Format MMPNET Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

the database one at a time. In each case, only the SEC portion of the record is displayed in the upper part of the screen.

### 5.2.6    MMPERR Function Key (PF7/19)

This key is used to jump/find the user from the MMPNET screen to the MMPERR screen and display the error exception list record stored in the ADMIN database (VMMPAADP). The SEC, PATHID and SCENARIO TYPE fields are used as the access keys.

### 5.2.7    REFRESH Function Key (PF8/20)

This key is used to return a blank MMPNET format to the CRT screen.

### 5.2.8    MMPSTS Function Key (PF9/21)

This key is used to switch the user from the MMPNET screen to the MMPSTS screen and to find and display on that screen the statistics that are stored in whatever SEC or path segment was being displayed, if any. If neither a SEC nor path segment was being displayed, MMPSTS will display the statistics for the first SEC in the SEC database (VMMPSCDD). If STATISTICS is "N", then the screen will be displayed, but all fields are blank. The M07 batch run will still work for these statistics, and the M07 Report will show the actual numbers for the current status statistics.

### 5.2.9    DELETE Function Key (PF10/22)

This key is used to request, and then confirm deletion of:

- An individual path segment and any error exception list record that may exist for that path.

- A SEC segment, all associated path segments, and all the error exception list records that may exist for those paths.

If a path segment is displayed on the MMPNET screen, the DELETE key will remove only that path (segment) from the database. It will not remove the SEC segment that is displayed in the upper part of the screen.

If a SEC segment is displayed without any of its associated path segments, the DELETE key will remove the entire record from the database (both SEC and path segments).

A FIND key action, or a FIND key plus NEXT key action, or a FIND key plus FORWARD key action, must precede the DELETE key action.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

5-8

**WARNING —** The DELETE key must be pressed twice before the record is deleted. When the key is pressed the first time, a message warning the user that a deletion is pending will be displayed. This is a safety feature that allows the user the opportunity to escape from an accidental pressing of the DELETE key. To cancel the pending deletion, the user may press any PF key *other* than DELETE, PF10/22, or PRINT, PF12/24. If the user desires to complete the deletion, the DELETE key must be pressed a second time.

### 5.2.10    HELP Function Key (PF11/23)

This key provides "help" by displaying definitions and other explanatory text for any designated field on the screen including the screen title. This key also provides "help" by displaying descriptions and appropriate actions for the TCM-generated error, warning, or informational message that is displayed at the system message line (available on CSAS screens only).

The field for which help is desired is identified by the cursor. If the field is unprotected, the tab key is used to position the cursor in the field for which help is desired. If the field is protected, the cursor positioning keys are used to move the cursor to the first position within the field name.

If the cursor is positioned on a screen field, then pressing the HELP key will switch the user to a special TCM FIELD INFORMATION screen on which the definition and other information is displayed. The user can return to the MMPNET screen by pressing the PA2 (NEXT MESSAGE) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

Similarly, if the cursor is positioned in the MMPNET screen title, then pressing the HELP key will return a list of valid function keys for that screen.

If the cursor is positioned in the TCM error, warning, or informational message, then pressing the HELP key switches the user to the CSAS Formatted Message Help screen (for MHELPF) on which the directions and appropriate actions for the condition are displayed. The user can return to the MMPNET screen by pressing the PF7 (LAST SCREEN) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

5-9

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Format MMPNET Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

### 5.2.11    PRINT Function Key (PF12)

This key generates a local printed copy of whatever information is currently being displayed on the CRT screen. The displayed data is directed to the printer associated with the requesting CRT.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

5-10

# 6. Format MMPERR Description

## 6.1 General

Format MMPERR is accessed either by typing "/FOR MMPERR" on a blank screen and pressing the ENTER key, or via the MMPERR key on format MMPNET.

The screen layout is shown below.

```
* CSAS-TCM: NETWORK EXCEPTION LIST (MMPERR) * /FOR        PAGE   1
SEC:        PATHID:        SCENARIO TYPE:   89.219 DATE 08/07/89
                              TIME 09:22:15
  _ TREAT ALL ERRORS AS WARNINGS      _ TREAT ALL WARNINGS AS ERRORS
  NOTE: THE ABOVE 2 FLAGS WILL FORCE THE OVERRIDE OF THE TABLE BELOW
  ACT  ERROR    ACT  ERROR    ACT  ERROR    ACT  ERROR    ACT  ERROR
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------
  - -------   - -------   - -------   - -------   - -------


  1/13 FIND       4/16 ADD       5/17 UPDATE      7/19 MMPNET
  8/20 REFRESH     10/22 DELETE      11/23 HELP
```
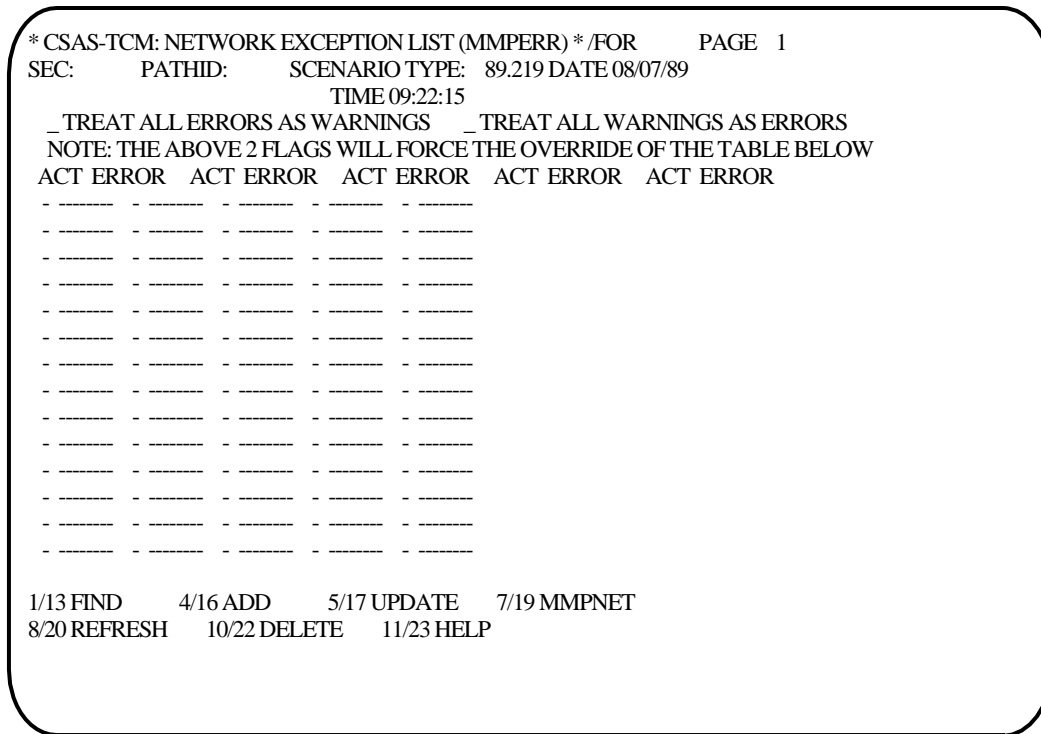
**Figure 6-1.** Format MMPERR

| FIND | | | ADD | UPD | | MMPNET | RFSH | | DELT | HELP | PRNT |
|------|--|--|-----|-----|--|--------|------|--|------|------|------|
| PF1 | | | PF4 | PF5 | | PF7 | PF8 | | PF10 | PF11 | PF12 |
| PF13 | | | PF16 | PF17 | | PF19 | PF20 | | PF22 | PF23 | |

The screen contains a group of application error codes that have been identified by the user to require processing by TCM other than the processing requested by the application using TCM.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

**6-1**

CONFIDENTIAL — RESTRICTED ACCESS

TCM Network Administration
Format MMPERR Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

There are no command words used with this format.

## 6.2    Function Keys

### 6.2.1    FIND Function Key (PF1/13)

This key is used to retrieve and display the error exception list record from the ADMIN database (VMMPAADP) using the SEC, PATHID, and SCENARIO TYPE fields as the keys.

### 6.2.2    ADD Function Key (PF4/16)

This key is used to create an error exception list record in the ADMIN database.

The required fields for creating an error exception list record are:

- SEC, PATHID, SCENARIO TYPE
  Validated: must exist in the SEC database as a path.

- SCENARIO TYPE
  Validated: must be "R", "Z" or "D".

Optional input fields include:

- TREAT ALL ERRORS AS WARNINGS *flag*
  This field is used by RA (Route Administration) to indicate whether or not all application error acknowledgments (ACKS) should be treated as warning ACKS.
  Validated: must be "N" (no) or "Y" (yes). Defaults to "N" if no entry is provided.

- TREAT ALL WARNINGS AS ERRORS *flag*
  This field is used by RA to indicate whether or not all warning ACKS should be treated as application error ACKS.
  Validated: must be "N" (no) or "Y" (yes). Defaults to "N" if no entry is provided.

- ACT *flag*
  This field is used by RA to indicate whether or not the associated ERROR code is used in the error exception list process.
  Validated: must be "N" (no) or "Y" (yes). Defaults to "N" if no entry is provided and the ERROR field is populated.

- ERROR *code*
  This field contains an application error code.
  Validated: must not start with the characters "TCM".

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

6-2

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPERR Description
Release 8.5

> **NOTE —** The fields ACT and ERROR are paired together, with the ACT field to the left of its associated ERROR field.

### 6.2.3     UPDATE Function key (PF5/17)

This key is used to change existing error exception list records in the ADMIN database. All changes must pass the same validations that are listed under the ADD key.

All fields can be changed except the SEC, PATHID and SCENARIO TYPE.

### 6.2.4     MMPNET Function key (PF7/19)

This key is used to jump/find the user from the MMPERR screen to the MMPNET screen and display the path segment stored in the SEC database (VMMPSCDD) using the SEC, PATHID and SCENARIO TYPE fields as the keys.

### 6.2.5     REFRESH Function Key (PF8/20)

This key is used to return a blank MMPERR format to the screen.

### 6.2.6     DELETE Function Key (PF10/22)

This key is used to request, and then confirm, the deletion of an error exception list record from the ADMIN database.

A FIND (PF1/13) key must precede the DELETE (PF10/22) key action.

> **WARNING —** The DELETE (PF10/22) key must be pressed twice before the error exception list record is deleted. When the key is pressed the first time, a message warning the user that a deletion is pending is displayed. This is a safety feature that allows the user the opportunity to escape from an accidental pressing of the DELETE key. To Cancel the pending deletion, the user may press any PF key *other* than DELETE (PF10/22) or PRINT (PF12/24). If the user desires to complete the deletion, the DELETE key must be pressed a second time.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

6-3

### 6.2.7    HELP Function Key (PF11/23)

This key provides "help" by displaying definitions and other explanatory text for any designated field on the screen including the screen title. This key also provides "help" by displaying descriptions and appropriate actions for the TCM-generated error, warning, or informational message that is displayed at the system message line (available on CSAS screens only).

The field for which help is desired is identified by the cursor. If the field is unprotected, the tab key is used to position the cursor in the field for which help is desired. If the field is protected, the cursor positioning keys are used to move the cursor to the first position within the field name.

If the cursor is positioned on a screen field, then pressing the HELP key will switch the user to a special TCM FIELD INFORMATION screen on which the definition and other information is displayed. The user can return to the MMPERR screen by pressing the PA2 (NEXT MESSAGE) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

Similarly, if the cursor is positioned in the MMPERR screen title, then pressing the HELP key will return a list of valid function keys for that screen.

If the cursor is positioned in the TCM error, warning, or informational message, then pressing the HELP key switches the user to the CSAS Formatted Message Help screen (for MHELPF) on which the directions and appropriate actions for the condition are displayed. The user can return to the MMPERR screen by pressing the PF7 (LAST SCREEN) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

### 6.2.8    PRINT Function Key (PF12)

This key generates a local printed copy of whatever information is currently being displayed on the CRT screen. The displayed data is directed to the printer associated with the requesting CRT.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

6-4

**CONFIDENTIAL — RESTRICTED ACCESS**

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPSTS Description
Release 8.5

# 7. Format MMPSTS Description

## 7.1    General

The MMPSTS screen may be accessed either by entering "/FOR MMPSTS" on a blank screen, or by pressing the MMPSTS key on the MMPNET screen.

The screen layout is shown below. Please note that there are three distinct collections of statistics displayed on this screen, as described following screen image.

```
* CSAS-TCM: NETWORK MSG VOLUMES (MMPSTS) *  /FOR          PAGE   1
SEC:        PATHID:        SCENARIO TYPE:   85.185 DATE 07/04/85
               CURRENT MESSAGE STATUS          TIME 15:22:46
DEFERRED:          TCM  :          TRNSLTN:
HELD  :          PARSE:         APPLCTN:
PEND ACK:          MAP  :          RETURND:
TOTAL MESSAGE VOLUMES    YESTERDAY       TODAY
         INPUT:
       DELIVERED:
        DEFERRED:
          HELD:
     ACKNOWLEDGED:
    RESENT TO MYSEC:
    RESENT BY MYSEC:
      TCM ERRORS:
     PARSER ERRORS:
     MAPPER ERRORS:
   TRANSLATION ERRORS:
   APPLICATION ERRORS:
  APPLICATION WARNINGS:
```

**Figure 7-1.** Format MMPSTS

| FIND | | | | | | | RFSH | MMPNET | | HELP | PRNT |
|------|---|---|---|---|---|---|------|--------|---|------|------|
| PF1 | | | | | | | PF8 | PF9 | | PF11 | PF12 |
| PF13 | | | | | | | PF20 | PF21 | | PF23 | |

The upper part of the screen contains statistics that tell the Network Administrator how many messages are **currently** stored in the TCM databases (TLOG and/or SENDQ) for this particular communication path. Totals are provided for each possible status category under which the messages may be stored.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

**7-1**

The lower part of the screen contains statistics that tell the Network Administrator the total number of messages that were processed during the entire day. Cumulative totals are shown for both today and yesterday.

There are no command words used with this screen.

## 7.2     Statistics

### 7.2.1     Current Message Status Statistics

- *DEFERRED*
  DATA CONTENT: up to 15N
  Count of currently deferred messages. The count of the number of messages currently in SENDQ. Messages are deferred because the link status indicator - **MAY-I** or **CAN-I** - is set to "N" for the designated path which is to carry the message. Such messages are assigned status D.

- *HELD*
  Data Content: up to 15N
  Count of currently held messages. Held messages are placed on TLOG according to the following criteria:

    1. HOLD FLAG = YES

    2. If scenario type is Z or R then the message is held if TLOG already contains a message with the same activity number as the one under consideration.

    3. If scenario type is A or S then the message is held if TLOG already contains a message with the same activity number and target SEC (RSYS) as the one under consideration.

  Held messages are placed in TLOG with status H.

- *PEND ACK*
  Data Content: up to 15N
  Current count of messages pending acknowledgment. The count of the number of messages currently awaiting acknowledgment from their targetted applications. Such messages are placed in TLOG with status K.

- *TCM*
  Data Content: up to 15N
  Current count of messages with TCM errors. The count of the current number of messages with header errors or other errors detected during TCM processing. Such messages are placed in TLOG with status E.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

7-2

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPSTS Description
Release 8.5

- *PARSE*

  Data Content: up to 15N

  Current count of messages with parsing errors. The count of the current number of messages with errors detected while parsing the input messages. Such messages are placed in TLOG with status P.

- *MAP*

  Data Content: up to 15N

  Current count of messages with mapping errors. The count of the current number of messages with errors detected while mapping the input into output format. Such messages are placed in TLOG and assigned status M or G.

- *TRNSLTN*

  Data Content: up to 15N

  Current count of messages with translation errors. The count of the current number of messages with errors detected while translating the input into output format. Such messages are placed in TLOG and assigned status T.

- *APPLCTN*

  Data Content: up to 15N

  Current count of messages with application errors. The count of the current number of messages which have been acknowledged by the targetted application as being in error (acknowledgment type 005). Such messages are placed in TLOG with status A.

- *RETURND*

  Data Content: up to 15N

  Current count of messages returned to sender. The count of the current number of messages which have been returned to the sender - that is, this CSAS System. Such messages are placed in TLOG and assigned status R (Returned).

## 7.2.2  TOTAL MESSAGE VOLUME STATISTICS

- *INPUT*

  Data Content: up to 15N

  Total number of messages received by TCM. The count of the number of messages which have been received by TCM from transmitting applications. Cumulative totals are shown separately for all messages received both yesterday and today.

- *DELIVERED*

  Data Content: up to 15N

  Total number of messages transmitted by TCM. The count of the number of messages transmitted to targeted applications by TCM. Cumulative totals are shown separately for all messages transmitted both yesterday and today.

- *DEFERRED*

  Data Content: up to 15 N.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

7-3

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Format MMPSTS Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

Total number of messages deferred by TCM. The count of the number of messages deferred by placement in SENDQ by TCM. Deferred messages have status equal to D. Separate cumulative totals shown for both yesterday and today.

- *HELD*
  Data Content: up to 15N
  Total number of messages held by TCM. The count of the number of messages held by TCM. Cumulative totals are shown separately for both yesterday and today. Messages are held if they meet the following criteria:

  1. HOLD FLAG = YES

  2. If scenario type is Z or R then the message is held if TLOG already contains a message with the same activity number as the one under consideration.

  3. If scenario type is A or S then the message is held if TLOG already contains a message with the same activity number and target SEC (RSYS) as the one under consideration.

  Held messages are placed in TLOG with status H.

- *ACKNOWLEDGED*
  Data Content: up to 15N
  Total number of messages acknowledged by TCM. The count of the number of messages for which positive acknowledgments (TYPE 000) were received by TCM. Separate cumulative totals are shown for both yesterday and today.

- *RESENT TO MYSEC*
  Data Content: up to 15N
  Total number of messages resent to MYSEC. The count of the number of messages received by TCM in which the resend flag field contained Y (yes). Separate cumulative totals are shown for both yesterday and today.

- *RESENT TO MYSEC*
  Data Content: up to 15N
  Total number of messages resent by MYSEC. The count of the number of messages resent (re-transmitted) by MYSEC, that is, resent by Message Administration after being corrected. Separate cumulative totals are shown for both yesterday and today.

- *TCM ERRORS*
  Data Content: up to 15N
  Total number of messages with TCM errors. The count of the number of messages for which header or other processing errors were detected by TCM. Separate cumulative totals are shown for both yesterday and today.

- *PARSER ERRORS*
  Data Content: up to 15N
  Total number of messages with parsing errors. The count of the number of messages

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

7-4

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPSTS Description
Release 8.5

for which parsing errors were detected by TCM. Separate cumulative totals are shown for both yesterday and today.

- *MAPPER ERRORS*
  Data Content: up to 15N
  Total number of messages with mapping errors. The count of the number of messages for which mapping errors were detected by TCM. Separate cumulative totals are shown for both yesterday and today.

- *TRANSLATION ERRORS*
  Data Content: up to 15N
  Total number of messages with translation errors. The count of the number of messages for which translation errors were detected by TCM. Separate cumulative totals are shown for both yesterday and today.

- *APPLICATION ERRORS*
  Data Content: up to 15N
  Total number of messages with application errors. The count of the number of messages for which a negative acknowledgment (type 005) was received from the application which processed the message. Separate cumulative totals are shown for both yesterday and today.

- *APPLICATION WARNINGS*
  Data Content: up to 15 N.
  Total number of messages with application warnings. The count of the number of messages for which a warning acknowledgment (type 006) was received from the application which processed the message. Separate cumulative totals are shown for both yesterday and today.

- *RETURNED TO MYSEC*
  Data Content: up to 15 N.
  Total number of messages returned to sender to MYSEC. The count of the number of messages returned to sender which were received by MYSEC. Resent messages are stored on TLOG with status R. Separate cumulative totals are shown for both yesterday and today.

- *RETURNED TO MYSEC*
  Data Content: up to 15 N.
  Total number of messages returned to sender by MYSEC. The count of the number of messages returned to sender from MYSEC. Separate cumulative totals are shown for both yesterday and today.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

7-5

CONFIDENTIAL — RESTRICTED ACCESS

**TCM Network Administration**
**Format MMPSTS Description**
**Release 8.5**

**BR 252-573-304**
**Issue 17, December 1996**

## 7.3     Function Keys

### 7.3.1     FIND Function Key (PF1/13)

This key is used to retrieve and display the statistics fields from the SEC (sum of all paths) record or the individual path segments in the SEC database (VMMPSCDD). The search criteria consists of the SEC, PATHID, and SCENARIO TYPE. The SEC identifies the record in the database; the PATHID and SCENARIO TYPE identify the path segment within that record. If no value is provided in the SEC field, the statistics for the first SEC in the SEC database (VMMPSCDD) will be displayed. If the SEC value is provided, but those for PATHID and SCENARIO TYPE are not, then the statistics displayed will be the sum of the statistics for all of the paths associated with the given SEC.

### 7.3.2     MMPNET Function Key (PF9/21)

This key is used to switch the user from the MMPSTS screen to the MMPNET screen and to find and display on that screen the SEC or path segment to which the statistics apply.

If the user displays a new SEC or path on the MMPNET screen, the MMPSTS key on that screen will bring back the MMPSTS screen and cause the statistics for that new SEC or path to be found and displayed.

### 7.3.3     REFRESH Function Key (PF8/20)

This key is used to return a blank MMPSTS format to the CRT screen.

### 7.3.4     PRINT Function Key (PF12)

This key obtains a local printed copy of whatever information is currently being displayed on the CRT screen. The displayed data is directed to the printer associated with the requesting CRT.

### 7.3.5     HELP Function Key (PF11/23)

This key provides "help" by displaying definitions and other explanatory text for any designated field on the screen including the screen title. This key also provides "help" by displaying descriptions and appropriate actions for the TCM-generated error, warning, or informational message that is displayed at the system message line (available on CSAS screens only).

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

7-6

**CONFIDENTIAL — RESTRICTED ACCESS**

| | |
|---|---|
| BR 252-573-304 | TCM Network Administration |
| Issue 17, December 1996 | Format MMPSTS Description |
| | Release 8.5 |

The field for which help is desired is identified by the cursor. If the field is unprotected, the tab key is used to position the cursor in the field for which help is desired. If the field is protected, the cursor positioning keys are used to move the cursor to the first position within the field name.

If the cursor is positioned on a screen field, then pressing the HELP key will switch the user to a special TCM FIELD INFORMATION screen on which the definition and other information is displayed. The user can return to the MMPSTS screen by pressing the PA2 (NEXT MESSAGE) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

Similarly, if the cursor is positioned in the MMPSTS screen title, then pressing the HELP key will return a list of valid function keys for that screen.

If the cursor is positioned in the TCM error, warning, or informational message, then pressing the HELP key switches the user to the CSAS Formatted Message Help screen (for MHELPF) on which the directions and appropriate actions for the condition are displayed. The user can return to the MMPSTS screen by pressing the PF7 (LAST SCREEN) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

**7-7**

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

7-8

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Format MMPPLEX Description
Release 8.5

# 8. Format MMPPLEX Description

## 8.1 General

The MMPPLEX screen may be accessed by entering "/FOR MMPPLEX" on a blank screen.

The screen layout is shown below.

```
* CSAS-TCM: SYSPLEX ADMINISTRATION (MMPPLEX) *        /FOR
SEC:       PATHID:       SCENARIO TYPE:


  SYSTEM 1 :
  SYSTEM 2 :
  SYSTEM 3 :
  SYSTEM 4 :
  SYSTEM 5 :
  SYSTEM 6 :
  SYSTEM 7 :
  SYSTEM 8 :
  SYSTEM 9 :
  SYSTEM 10:




  1/13 FIND   3/15 MMPNET   5/17 UPDATE   8/20 REFRESH   11/23 HELP
```
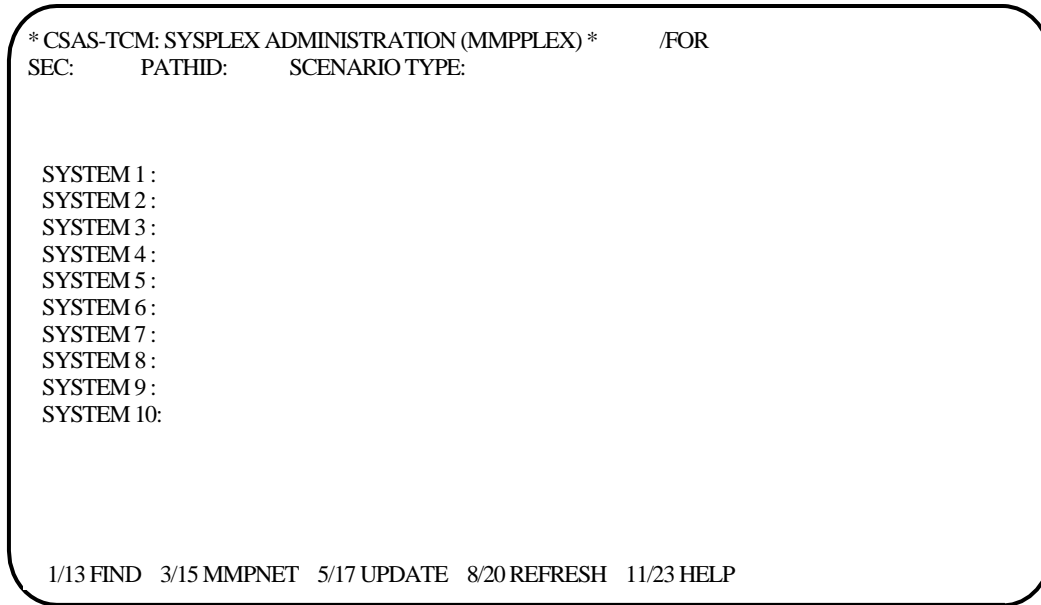
**Figure 8-1.** Format MMPPLEX

| FIND | | Switch to MMPNET | | UPDATE | | | RFSH | | | HELP | |
|------|--|------------------|--|--------|--|--|------|--|--|------|--|
| PF1 | | PF3 | | PF5 | | | PF8 | | | PF11 | |
| PF13 | | PF15 | | PF17 | | | PF20 | | | PF23 | |

This MMPPLEX Screen enables users to see the current status of a path with a link problem. The SEC is of the external system receiving data. The path is defined on the MMPNET screen. The fields shown on this screen are control region names which are having link problems for the PATHID referenced on the format.

There are no command words used with this format.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

8-1

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Format MMPPLEX Description
Release 8.5

BR 252-573-304
Issue 17, December 1996

## 8.2      Function Keys

### 8.2.1      FIND Function Key (PF1/13)

This key is used to retrieve and display the SYSPLEX Control Region Names for the SEC (System Entity Code of outside application) record and PATH segments in the SEC database (VMMPSCDD). The search criteria consists of the SEC, PATH (Path out of the local TCM), and SCENARIO TYPE (Definition of receiving system as a TCM supported system (S), or a Non-TCM supported system (A or N).

### 8.2.2      SWITCH (MMPNET) Function Key (PF3/15)

This key is used to SWITCH to format MMPNET, using SEC, PATHID and SCENARIO TYPE fields that are populated.

### 8.2.3      UPDATE Function Key (PF5/17)

This key is used to UPDATE the control region name list. A FIND prior to UPDATE is required.

### 8.2.4      REFRESH Function Key (PF8/20)

This key is used to return a blank MMPPLEX format to the CRT screen.

### 8.2.5      HELP Function Key (PF11/23)

This key provides "help" by displaying definitions and other explanatory text for any designated field on the screen including the screen title. This key also provides "help" by displaying descriptions and appropriate actions for the TCM-generated error, warning, or informational message that is displayed at the system message line (available on TIRKS screens only).

The field for which help is desired is identified by the cursor. If the field is unprotected, the tab key is used to position the cursor in the field for which help is desired. If the field is protected, the cursor positioning keys are used to move the cursor to the first position within the field name.

If the cursor is positioned on a screen field, then pressing the HELP key will switch the user to a special TCM FIELD INFORMATION screen on which the definition and other information is displayed. The user can return to the MMPPLEX screen by pressing the PA2

(NEXT MESSAGE) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

Similarly, if the cursor is positioned in the MMPPLEX screen title, then pressing the HELP key will return a list of valid function keys for that screen.

If the cursor is positioned in the TCM error, warning, or informational message, then pressing the HELP key switches the user to the CSAS Formatted Message Help screen (for MHELPF) on which the directions and appropriate actions for the condition are displayed. The user can return to the MMPPLEX screen by pressing the PF7 (LAST SCREEN) key. The returned screen will contain the same data as was on it when the HELP key was invoked.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

8-3

CONFIDENTIAL — RESTRICTED ACCESS

**TCM Network Administration**
**Format MMPPLEX Description**
**Release 8.5**

**BR 252-573-304**
**Issue 17, December 1996**

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

8-4

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Backup and Recovery
Release 8.5

# 9.    Backup and Recovery

Recovering from errors caused by system outages can be extremely difficult or impossible. It is important to take all possible precautions to attempt to avoid situations that can cause error. For example, in the event of a planned system outage, all interfacing systems should be informed well in advance of the outage, allowing them to turn down their affected links before the outage begins.

## 9.1    Physical Link Verify and Multiple System Coupling Links

### 9.1.1    Physical Link Verify

An important precautionary measure is the use of VMMPNP, the Physical Link Verify routine. VMMPNP is an online transaction that verifies the availability of the links known to a TCM. When VMMPNP finds that a link has become unavailable, it changes the value of the CAN-I flag in the SEC database from "Y" to "N", which in turn causes TCM to defer those messages to the SENDQ database[1]. When the link again becomes available, VMMPNP will send as many messages as are indicated by the DEQUEUE COUNT value. (DEQUEUE COUNT is a user-populated field on format MMPNET. The user may set any value in this field. The default value is fifty.) It is recommended that the Cron BMP be used with a control card that will run VMMPNP at one minute intervals if the system is busy, or up to five minute intervals if message volume is light. Each time VMMPNP runs, it will dequeue the amount of messages indicated by the DEQUEUE COUNT value (so long as there are messages to be dequeued). If VMMPNP is not running, users should perform *frequent manual inspections* of their links. Users may determine how many messages are deferred by running TQS query MTCQQ01, or via format MMPSTS.

#### 9.1.1.1    Work Load Router II and Multiple System Coupling Links

If VMMPNP determines that Work Load Router, Version II (WLR II) is installed, an IMS CHNG call for Multiple System Coupling (MSC) links is issued. If an A1 status is returned, TCM determines that the MSC link is down. WLR II must have its program NOQUE option set to NOQUE, and its QUE/NOQUE option set to A1. Your IMS System Administrator must be notified to set this default. If the status is blank, TCM checks the MSNAME returned by WLR II, and if it has changed, it will determine that WLR II is telling TCM there is at least one working link and will route the data over the good link.

---

1. The sizing of the SENDQ database is important. The purpose of the SENDQ database is storage of deferred messages. Should the capacity of the SENDQ database be exceeded, messages may be lost. When calculating the size of the SENDQ database, it is important to allow enough space to hold all deferred messages under a "worst case" scenario.

These links are defined in the WLR II options by your IMS System Administrator. If the format MMPNET  link status flag is an "N", it will be changed to a "Y". If there are any deferred messages, the VMMPNP transaction will issue VMMPD transactions to dequeue the data relative to the dequeue count on format MMPNET. If TCM has been told it is in a datasharing environment, by the SYSPLEX flag on the TCM USER CONTROL TTS table, then TCM will attempt to remove the Control Region Name it is running under. In this case, if there are other Control Regions with a link problem for this SEC and PATH, they must have VMMPNP run in them before the CAN-I flag is able to change back to a "Y".

### 9.1.1.2      Manually Resending Deferred Messages

Users may also handle deferred messages manually via format MMPMSG. In this situation, the user would change the status of the messages from "deferred" to "TCM error", via the MOVE or BMOV command, and then resend the messages.

If a sending IMS drops, there may be queued messages. Care must be taken in restarting the system, or queued messages may be lost. If at all possible, the system should be warm started. If the system is cold started, it is probable that *all queued messages will be lost, and recovery will be very difficult*. In the case of a cold start, the only way to be certain messages are not lost is to precede the restart with a memory dump. IMS System Support should be able to analyze the dump and determine the identity of the messages that were lost, if any.

If a receiving IMS drops, TCM will continue to send messages until the CAN-I or MAY-I flag for that link is changed to "N", either manually or by transactions VMMPNP or VMMPNM. But between the time the receiving IMS drops and TCM begins deferring messages to SENDQ, TCM is still attempting to send messages. These messages are stored in the IMS message queue. IMS will also be aware that the receiving system has dropped,[2] and that messages must be held. Another reason that it is important to run VMMPNP is that the IMS message queue may be filled to capacity quickly on a busy system. If the IMS message queue overflows, messages will be lost. So long as the IMS message queue does not overflow, messages will not be lost.

Certain interfaces may also have developed special tools or methods for handling the problem of link outages. For example, a link may become unavailable between systems that share more than one link. In these cases, messages may be re-routed temporarily to the active link(s). Consult a local expert about the existence of such tools or methods.

---

2. Because MSC and ISC links may be shared by more than one application, IMS must also be aware of the status of its links.

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

9-2

# 10.  Field Definitions

The following is an alphabetized list of fields that appear on Formats MMPNET and/or MMPPLEX. For each entry in the following list the fields Full Name, Definition, Data Content and screen occurrence is specified.

ACT

   MMPERR

   Full Name        Error Code Active Flag

   Definition       A flag used by Routing Administration to indicate whether or not
                    the associated error code is to be used in the error exception list
                    process. This field allows the user to temporarily inactivate an error
                    code without having to delete it.

   Data Content     Y (yes, the associated error code is to be used by Routing
                        Administration)
                    N (no, default; the associated error code is not to be used by
                        Routing Administration.)
                    _ (no, value when an error list does not exist for a path.)

APP ERROR LDEST

   MMPNET

   Full Name        Application Error Logical Destination

   Definition       A 3-character destination identifier that will be populated in the
                    optional acknowledgment message transmitted by TCM back to the
                    originating system as the result of application errors.
                    Used in SOAC interfaces.

   Data Content     3 A

APPL HEADER

   MMPNET

   Full Name        Application Header

   Definition       Send SOAC Application Header (*C3/) to Application (in addition
                    to data)

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

10-1

Data Content

## CAN-I

### MMPNET

| | |
|---|---|
| Full Name | Link Status Can-I? |
| Definition | A yes/no indicator that tells whether the named physical link (MSC) or LTERM (ISC) that this TCM logical interface path uses is physically available or unavailable. |
| Data Content | 1 A |
| Valid Entries | Y (yes, link or LTERM is available<br>N (no, link or LTERM is not available) |

## CURRENT MESSAGE STATUS

### MMPSTS

| | |
|---|---|
| Full Name | Current Message Status |
| Definition | This is the title over a set of nine statistics fields that tell the TCM Network Administrator how many messages are currently stored in the TCM databases (TLOG and/or SENDQ) for a particular logical interface path. The nine fields are: *DEFERRED, HELD, PEND ACK, TCM, PARSE, MAP, TRNSLTN, APPLCTN, RETURND.* |
| Data Content | 15 N |

## DATE

### MMPSTS, MMPNET, MMPERR

| | |
|---|---|
| Full Name | Current Message Status |
| Definition | The calendar date on which the format is displayed. The Julian date [YY.DDD] precedes the "DATE" label and the standard Gregorian date [MM/DD/YY] follows the DATE label. |
| Data Content | 5 N, 6 N |
| Sample | 84.054 or 02/23/84 |

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

10-2

## DEF OFFSET

### MMPNET

| | |
|---|---|
| Full Name | Defer Time Offset |
| Definition | Defer Time Offset in HH and MM. |
| Data Content | 4 N (In the form of HH:MM) |

> **WARNING** — When updating the DEF OFFSET field value to a lesser amount, if there are deferred messages for this path, it may cause sequencing errors when there are new incoming messages for the same Activity Number (ACNO), which are deferred for a lesser amount of time than messages already in the database.

## DEQUEUE COUNT

### MMPNET

| | |
|---|---|
| Full Name | Dequeue Count |
| Definition | The maximum number of deferred messages to be processed during each dequeue session initiated by transaction VMMPBW. |
| Data Content | 6 N |

## DESCRP

### MMPNET

| | |
|---|---|
| Full Name | Description |
| Definition | A 40-character, free-format field for describing the system identified by the SEC (system entity code). |
| Data Content | 40 A/N |

## ERROR

### MMPNET

| | |
|---|---|
| Full Name | Error Code |
| Definition | An Application Generated Error Code |
| Data Content | Up to 8 A/N characters that do not start with "TCM". |
| Sample | GOC0333E |
| NOTE: | The presence of an "E" or a "W" at the end of an error code has nothing to do with whether the acknowledgment (ACK) is a warning or an error type ACK. A field in the ACK (ACKTYPE) is used to determine whether the ACK is an application error (ACKTYPE = 005) or a warning (ACKTYPE = 006). |

## INPUT MFD

### MMPNET

| | |
|---|---|
| Full Name | Input Message Format Descriptor |
| Definition | This is the name of the "Message Format Descriptor (MFD)" that the TPAM Parser must use to interpret the message data it receives from a CSAS System application (Scenario type "A", "Z" or "N") or from a remote TCM supported sending application that elected to bypass its TCM (Scenario type "D"). (Required for all messages. Some class 2 messages, however, can use the TCM-supplied default.) |
| Data Content | 8 A/N |
| Sample | VMGCA80 |

## LINK NAME

### MMPNET

| | |
|---|---|
| Full Name | Link Name |
| Definition | The name of a physical communication channel designated by assigned SECs. This may be either an MSC link name (MSNAME) or an ISC LTERM name. |
| Data Content | 8 A/N |

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

10-4

**CONFIDENTIAL — RESTRICTED ACCESS**

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Field Definitions
Release 8.5

Sample       MSC1920

## LINK TYPE

### MMPNET

Full Name       Link Type

Definition       A code that defines a type of physical communication channel.

Data Content       1 A

Valid Entries       M meaning MSC (Multiple System Coupling),
I   meaning ISC (Inter System Communications), or
L  meaning LU6.2 (APPC)

## MAY-I

### MMPNET

Full Name       May-I?

Definition       A yes/no indicator that tells whether the application is or is not accepting messages. Format MMPNET has three MAY-I indicators:

LINK STATUS (TO) MAY-I (at the SEC level)
LINK STATUS (FROM) MAY-I (at the SEC level)
LINK STATUS MAY-I (at the path level)

The LINK STATUS (TO) and LINK STATUS (FROM) MAY-I indicators apply to overall communication to and from the SEC. They tell whether or not the application is accepting messages and/ or TCM is sending messages on any path. The LINK STATUS MAY-I applies to a single logical interface path. It tells whether or not the application is accepting messages or TCM is sending messages on a single specific logical interface path.

Data Content       1 A

Valid Entries       Y  (messages are being accepted)
N  (messages are not being accepted)

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Field Definitions
Release 8.5

BR 252-573-304
Issue 17, December 1996

## MESSAGE CLASS

### MMPNET

| | |
|---|---|
| Full Name | Message Class |
| Definition | A code that indicates the type of message being routed through TCM. |
| Data Content | 1 N |
| Valid Entries | 1,3,4 (application-to-application message) 2,5 (application-to-TCM acknowledgment), if SCTYPE is either Z or I in message header, OR TCM-to-application acknowledgment, if SCTYPE = R, S, or A. Used when EPATHID or PPATHID is specified in the TCM header of the original message. |

## OUTPUT MFD

### MMPNET

| | |
|---|---|
| Full Name | Output Message Format Descriptor |
| Definition | This is the name of the "Message Format Descriptor (MFD)" that the TPAM Mapper must use to place the message data into the internal format required by the CSAS application. (Required for all messages. Some class 2 messages, however, can use the TCM-supplied default.) |
| Data Content | 8 A/N |
| Sample | VMGCA80 |

## PRIMARY & SECONDARY (LTERMs)

### MMPNET

| | |
|---|---|
| Full Name | Primary and Secondary Logical Terminals |
| Definition | Code names of the PRIMARY and SECONDARY LTERMS (printers or TTYs) to which exception notices are to be sent. The PRIMARY LTERM is the default if the ELTERM is not present in the original message TCM header. The SECONDARY LTERM is always used providing it differs from the ELTERM or PRIMARY LTERM, whichever applies. The TSA LTERM (in the TCM USER |

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

10-6

CONTROL TTS table) is used if neither the PRIMARY (or ELTERM) nor the SECONDARY LTERM is specified for the path.

If the user enters "NONE" as the value for the PRIMARY LTERM, TCM will not allow any entry in the SECONDARY LTERM field, and error and warning messages will not be generated at all.

Data Content     8 A/N

Sample           PY250100


PROCESSING LEVEL

MMPNET

Full Name        Processing Level for Resend and Hold

Definition       These (required) fields enable the user to specify types of RESEND and HOLD processing. The fields are independent — users may set either field or both fields to either of the two acceptable values, "P" or "S", but both fields must be populated. When the user sets a value of "S", the system will handle processing based on message activity number (ACNO), scenario type (SCEN_TYPE) and remote SEC. When the user selects "P", the system will process based on the "S" value criteria (ACNO, SCEN_TYPE, and remote SEC) *plus* PATHID.

Data Content     1 A

Sample           S


RELEASE LEVEL

MMPNET

Full Name        Release

Definition       The "release level" under which another system that contains TCM (SEC TYPE = T) is operating.

Data Content     10 N

Sample           R14.1

## REMOTE NOTIFICATION

### MMPNET

| | |
|---|---|
| Full Name | Remote Notification Logical Terminal |
| Definition | Coded designation for an LTERM/printer in a CSAS (sending) application defined to receive Exception Notices generated for errors encountered at a remote (receiving) application that also communicates via TCM. |
| Data Content | 8 A/N |
| Sample | PY350200 |

## RULE ID

### MMPNET

| | |
|---|---|
| Full Name | Rule Identification |
| Definition | A code that identifies a TPAM Translation Rule Set. |
| Data Content | 8 A/N |
| Sample | SOACRULE |

## SCENARIO TYPE

### MMPNET, MMPSTS

| | |
|---|---|
| Full Name | Scenario Type |
| Definition | A code that identifies the types of systems between which communications are being sent and the direction of the communication. |
| Data Content | 1 A |
| Valid Entries | S TCM (sending) to TCM<br>R TCM to TCM (receiving)<br>A TCM to non-TCM<br>Z  non-TCM to TCM<br>I   intra-TCM<br>N TCM (sending) to SOAC<br>D Application (bypass sending TCM) to TCM |

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

10-8

CONFIDENTIAL — RESTRICTED ACCESS

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Field Definitions
Release 8.5

## SCENARIO TYPE

MMPERR, MMPPLEX

| | |
|---|---|
| Full Name | Scenario Type |
| Definition | A code that identifies the types of systems between which communications are being sent and the direction of the communication. |
| Data Content | 1 A |
| Valid Entries | R TCM to TCM (receiving) |
| | Z  non-TCM to TCM |
| | A TCM to non-TCM |
| | N TCM (sending) to SOAC |
| | S TCM (sending) to TCM |

## SEC

MMPNET, MMPSTS, MMPERR, MMPPLEX

| | |
|---|---|
| Full Name | System Entity Code |
| Definition | A code that identifies a computer-based operating system, whether that system uses TCM for communications or not. |
| Data Content | 8 A/N |
| Valid Entries | See the standards defined in Common Language Standard 255. |

## SEC TYPE

MMPNET

| | |
|---|---|
| Full Name | System Entity Code Type |
| Definition | An indicator to distinguish among a TCM, non-TCM and SOAC SEC. |
| Data Content | 1 A |
| Valid Entries | T   (TCM) |
| | N   (non-TCM) |
| | S   (SOAC) |

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

10-9

**CONFIDENTIAL — RESTRICTED ACCESS**

TCM Network Administration
Field Definitions
Release 8.5

BR 252-573-304
Issue 17, December 1996

## STATISTICS

### MMPNET

| | |
|---|---|
| Full Name | Statistics Flag |
| Definition | A user entered field to turn off Statistics Counter. |
| Data Content | A single alpha character, Enter "Y", "N" or Blank |
| Sample | N |
| NOTE | Any Blank entry will automatically default to "Y", which keeps all statistics counters. |

## SYSTEM 1

### MMPPLEX

| | |
|---|---|
| Full Name | System 1 |
| Definition | First control region name in the list of names which has a link problem over the noted path. |
| Data Content | 8 A/N |

## SYSTEM 2

### MMPPLEX

| | |
|---|---|
| Full Name | System 2 |
| Definition | Second control region name in the list of names which has a link problem over the noted path. |
| Data Content | 8 A/N |

## SYSTEM 3

### MMPPLEX

| | |
|---|---|
| Full Name | System 3 |
| Definition | Third control region name in the list of names which has a link problem over the noted path. |
| Data Content | 8 A/N |

## SYSTEM 4

### MMPPLEX

Full Name      System 4

Definition     Fourth control region name in the list of names which has a link
               problem over the noted path.

Data Content   8 A/N


## SYSTEM 5

### MMPPLEX

Full Name      System 5

Definition     Fifth control region name in the list of names which has a link
               problem over the noted path.

Data Content   8 A/N


## SYSTEM 6

### MMPPLEX

Full Name      System 6

Definition     Sixth control region name in the list of names which has a link
               problem over the noted path.

Data Content   8 A/N


## SYSTEM 7

### MMPPLEX

Full Name      System 7

Definition     Seventh control region name in the list of names which has a link
               problem over the noted path.

Data Content   8 A/N

## SYSTEM 8

### MMPPLEX

Full Name       System 8

Definition      Eighth control region name in the list of names which has a link
                problem over the noted path.

Data Content    8 A/N

## SYSTEM 9

### MMPPLEX

Full Name       System 9

Definition      Ninth control region name in the list of names which has a link
                problem over the noted path.

Data Content    8 A/N

## SYSTEM 10

### MMPPLEX

Full Name       System 10

Definition      Tenth control region name in the list of names which has a link
                problem over the noted path.

Data Content    8 A/N

## TREAT ALL ERRORS AS WARNINGS

### MMPERR

Full Name       Treat all Errors as Warnings

Definition      A flag used by routing administration to indicate whether or not all
                application error acknowledgments (ACKS) should be treated as
                application warning ACKS. A warning ACK causes the deletion of
                the message being acknowledged from the TLOG (VMMPTLDD)
                database. An error ACK causes the message being acknowledged to
                be logged in the TLOG database with an error status. The printing

BELLCORE CONFIDENTIAL — RESTRICTED ACCESS
See confidentiality restrictions on title page.

10-12

**CONFIDENTIAL — RESTRICTED ACCESS**

BR 252-573-304
Issue 17, December 1996

TCM Network Administration
Field Definitions
Release 8.5

and/or sending of the error notice(s) continues whether the ACK is a warning or an error.

Data Content    Y  (yes, treat all error ACKS as warning ACKS.)
N  (no, do not treat all error ACKS as warning ACKS.)
_  (no, value when an error list does not exists for a path.)

NOTE: Setting of this flag to "Y" forces the error list table to be ignored.


## TREAT ALL WARNINGS AS ERRORS

### MMPERR

Full Name       Treat all Warnings as Errors

Definition      A flag used by routing administration to indicate whether or not all application warning acknowledgments (ACKS) should be treated as application error ACKS. A warning ACK causes the deletion of the message being acknowledged from the TLOG (VMMPTLDD) database. An error ACK causes the message being acknowledged to be logged in the TLOG database with an error status. The printing and/or sending of the error notice(s) continues whether the ACK is a warning or an error.

Data Content    Y  (yes, treat all error ACKS as warning ACKS.)
N  (no, do not treat all error ACKS as warning ACKS.)
_  (no, value when an error list does not exists for a path.)

NOTE: Setting of this flag to "Y" forces the error list table to be ignored.


## TCM ERROR LDEST

### MMPNET

Full Name       TCM Error Logical Destination

Definition      A 3 character destination identifier that will be populated in the optional acknowledgment message transmitted by TCM back to the originating system as the result of TCM errors. Default value is "TSA" for TCM errors. Used in SOAC interfaces.

**CONFIDENTIAL — RESTRICTED ACCESS**

**TCM Network Administration**
**Field Definitions**
**Release 8.5**

**BR 252-573-304**
**Issue 17, December 1996**

Data Content     3 A

## TOTAL MESSAGE VOLUMES

### MMPSTS

Full Name      Total Message Volumes

Definition     This is the title over a set of fifteen statistics fields that tell the TCM
               Network Administrator the cumulative number of messages that
               were handled today and yesterday. The fifteen fields are: *INPUT,
               DELIVERED, DEFERRED, HELD, ACKNOWLEDGED, RESENT
               TO MYSEC, RESENT BY MYSEC, TCM ERRORS, PARSER
               ERRORS, MAPPER ERRORS, TRANSLATION ERRORS,
               APPLICATION ERRORS, APPLICATION WARNINGS,
               RETURNED TO MYSEC, RETURNED BY MYSEC*.

Data Content   15 N


## TRANCODE

### MMPNET

Full Name      IMS Transaction Code

Definition     The code by which IMS (the Information Management System)
               identifies an application's transaction.

Data Content   8 A/N

Sample         VMMPT


## PATHID

### MMPNET, MMPSTS, MMPERR, MMPPLEX

Full Name      Path Identifier

Definition     A mnemonic code that identifies the category of messages that are
               being transmitted between two systems. Previously known as the
               TRANID.

Data Content   8 A/N

Sample         ZSU
               TGSTG

**BELLCORE CONFIDENTIAL — RESTRICTED ACCESS**
See confidentiality restrictions on title page.

**10-16**