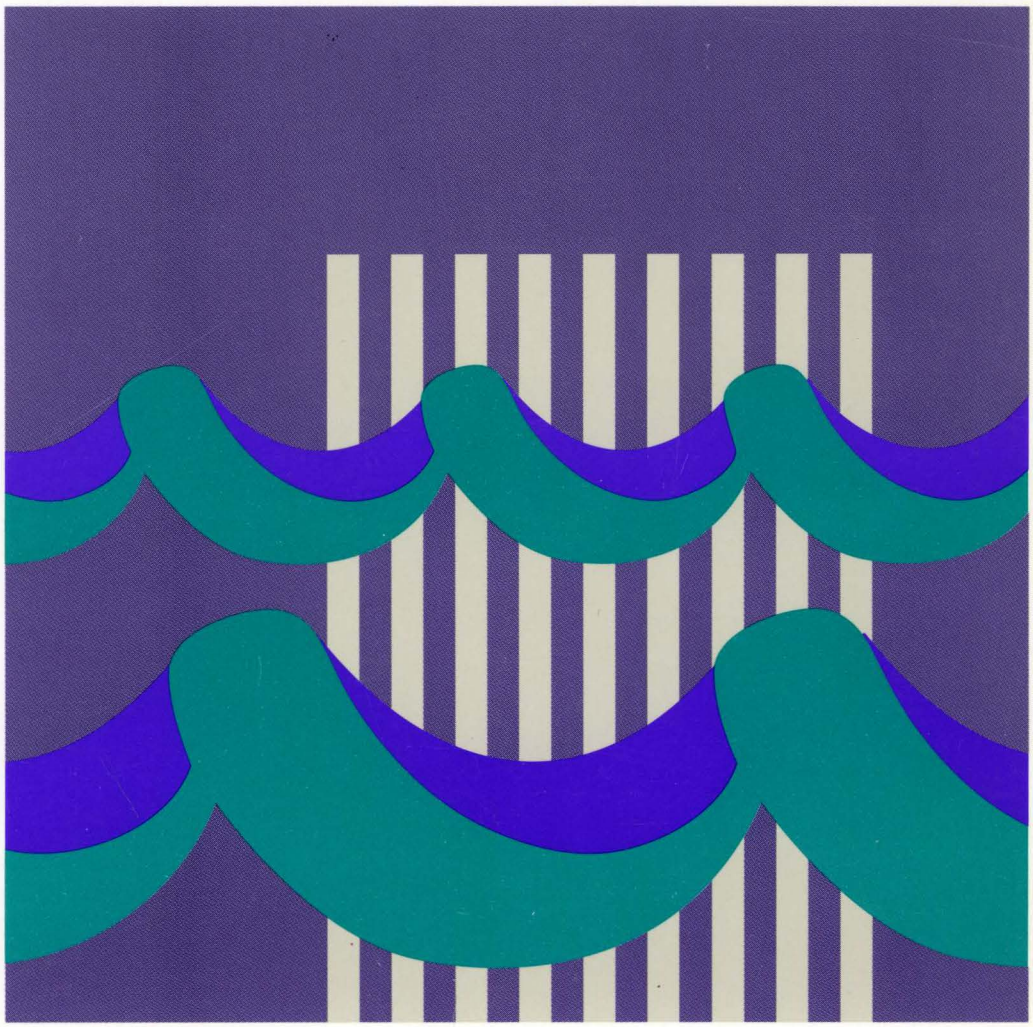
LY43-0033-01

Network Control Program
System Support Programs
Emulation Program

Diagnosis Guide

NCP Version 7 Release 2
SSP Version 4 Release 2
EP Release 12



LY43-0033-01

Network Control Program
System Support Programs
Emulation Program

Diagnosis Guide

NCP Version 7 Release 2
SSP Version 4 Release 2
EP Release 12

Note

Before using this document, read the general information under "Notices" on page xiii.

This book is also provided as an online book that can be viewed with the IBM BookManager* READ and IBM Library Reader* licensed programs.

Second Edition (October 1994)

This major revision replaces LY43-0033-00. This licensed document applies to the following IBM licensed programs:

- Advanced Communications Function for Network Control Program Version 7 (program number 5648-063).
- Advanced Communications Function for System Support Programs Version 4 for MVS (program number 5655-041), for VM (program number 5654-009) Release 1, and for VSE (program number 5686-064) Release 1.
- Emulation Program for IBM Communication Controllers (program number 5735-XXB) Release 12.

Publications are not stocked at the address given below. If you want more IBM publications, ask your IBM representative or write to the IBM branch office serving your locality.

A form for your comments is provided at the back of this document. If the form has been removed, you may address comments to:

IBM Corporation
Department E15
P.O. Box 12195
Research Triangle Park, North Carolina 27709
U.S.A.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Notices

Any reference to an IBM licensed program in this licensed document does not imply that IBM intends to make it available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
International Business Machines Corporation
500 Columbus Avenue
Thornwood, New York 10594
United States of America

The licensed programs described in this document and all licensed material available for them are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Programming Interface Information

This book is intended to help the customer diagnose NCP and EP problems using the programs and utilities available through SSP. This book documents information which is Diagnosis, Modification, or Tuning Information provided by NCP, SSP, and EP.

Warning: Do not use this Diagnosis, Modification, or Tuning Information as a programming interface.

Trademarks

The following terms, denoted by an asterisk (*) at their first occurrence in this publication, are trademarks of the IBM Corporation in the United States or other countries or both:

BookManager	Library Reader	NetView
IBM	MVS/ESA	VM/ESA
IBMLink	MVS/XA	VSE/ESA
IBM OS/2		VTAM

About This Book

This book provides information to help you diagnose Advanced Communications Function for Network Control Program (NCP) and Emulation Program (EP) problems using the programs and utilities available through the Advanced Communications Function for System Support Programs (SSP). Diagnosing an NCP or EP problem involves isolating the cause of the problem and working with IBM Support Center representatives to resolve the problem.

Who Should Use This Book

This book is for programmers and program support personnel who are responsible for isolating, diagnosing, and debugging NCP and EP problems for the IBM* 3720, 3725, and 3745 Communication Controllers.

Before using this book, you should be familiar with the concepts and terminology in *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference*.

How To Use This Book

This book has two parts. Part 1 tells you how to gather data and report problems to the IBM Support Center. It provides information on:

- How to determine if the problem is with NCP
- How to gather appropriate documentation about the problem
- How to use the tools provided with SSP to gather relevant information to describe the problem.

Part 2 explains how to use the trace tools, performance tools, and diagnostic aids to determine the cause of the problem. While reading Part 2, you need to know the hardware and software configurations that determine the tools available to you:

- Which level of NCP you use
- Which communication controller you use
- Which access method you use (VTAM*, TCAM)
- Which operating system you use (MVS, VM, or VSE).

This book shows you how to describe the problem and use diagnostic aids to collect information about the problem. To analyze or interpret the data that these diagnostic aids provide, see *NCP and EP Reference Summary and Data Areas*, Volumes 1 and 2; *NCP and EP Reference*; *VTAM Diagnosis*; and *TCAM Diagnosis Reference*.

The *NCP, SSP, and EP Diagnosis Aid* tool lets you gather information about problems and solving problems online. The following information is contained in the *NCP, SSP, and EP Diagnosis Aid* tool:

- *NCP, SSP, and EP Diagnosis Guide*
- *NCP, SSP, and EP Messages and Codes*
- *NCP and EP Reference Summary and Data Areas*
- *NCP, SSP, and EP Trace Analysis Handbook*.

For assistance beyond the scope of these books, consult the IBM Support Center.

Terms Used in This Book

The following descriptions explain how terms are used in the NCP, SSP, and EP library.

"MVS," "VM," and "VSE"

The term *MVS* means the MVS/XA* and MVS/ESA* systems. The term *VM* means the VM/ESA* systems in the CMS environment. The term *VSE* means the VSE/SP, VSE/ESA*, and VSE/Advanced Function operating systems. If information is applicable to only one system, the specific system name is used.

"Port" and "Channel" Used with LPDA

In discussions concerning link problem determination aid (LPDA) for multiport and data multiplex mode (DMPX) modems, the terms *port* and *channel* are synonymous. Although *port* is the more commonly used term, *channel* can be used in sections describing LPDA.

"IBM Special Products or User-Written Code"

This book sometimes refers to *IBM special products or user-written code.* This phrase means IBM* special products such as Network Terminal Option (NTO), Network Routing Facility (NRF), and X.25 NCP Packet Switching Interface (NPSI), or user-written code.

IBM 3745 Communication Controller Model Numbers

In this book, the term *IBM 3745 Communication Controller* refers to all IBM 3745 models. When particular models are discussed, the appropriate model numbers are specified. Model numbers include IBM 3745-130, 3745-150, 3745-160, 3745-170, 3745-17A, 3745-210, 3745-21A, 3745-310, 3745-31A, 3745-410, 3745-41A, 3745-610, and 3745-61A.

"Ethernet-Type LAN"

The term *Ethernet-type LAN* means a local area network (LAN) that uses either the Ethernet Version 2 or IEEE 802.3 protocol.

"CSS," "37CS," and "3746 Model 900"

The terms *connectivity subsystem (CSS)* and *37CS* refer to the 3746 Model 900, an expansion frame that extends the connectivity and enhances the performance of the IBM 3745 Communication Controller.

"Token Ring"

NCP can connect to an IBM Token-Ring Network using the NCP/Token-Ring interconnection (NTRI) or the 3746 Model 900 connectivity subsystem attachment. This book uses the term *token ring* when referring to either type of connection.

"Frame Relay"

To support frame-relay networks, NCP can use a transmission subsystem (TSS) or high performance transmission subsystem (HPTSS) adapter on the 3745, or NCP can use a communication line processor (CLP) adapter on the 3746 Model 900 connectivity subsystem. Unless otherwise stated, this book uses the term *frame relay* when referring to a 3745 or a 3746 Model 900 connection.

"NCP V6R2", "NCP V6R3", "NCP V7R1", and "NCP V7R2"

In this book, unless otherwise specified, the term *NCP V6R2*, *NCP V6R3*, *NCP V7R1*, and *NCP V7R2* refer to these releases with or without the optional NCP feature for CSS support. To use this feature, you must have the 3746 Model 900 installed in your controller.

How Numbers Are Written

This book shows numbers over 9999 in metric style, which means that a space is used instead of a comma to separate groups of three digits. For example, the number ten thousand five hundred fifty-two is written 10 552. However, if the number is a keyword value, for example, SALIMIT=65535, it does not include a blank.

What Is New in This Book

This edition contains information on the following new NCP and SSP functions, as well as editorial, organizational, and technical changes. New or changed technical information is identified by a vertical bar (|) in the left margin.

Note: The information that was previously (V7R1) contained in "Chapter 4. Gathering Host-Collected Trace and Performance Data," "Chapter 13. Using ACF/TAP," and "Appendix A. Supplementary ACF/TAP Information" of this book has been moved to the *NCP, SSP, and EP Trace Analysis Handbook*, LY43-0037.

Table 1 lists new information for NCP and SSP and tells you where to find it.

Table 1. What Is New in This Book

New Information	Location
Spare SDLC lines	"Activate or Deactivate Error Procedure" on page 40

Supported Releases

Table 2 shows the releases of NCP, SSP, and EP that are currently supported by IBM. If you need information on an unsupported release of NCP, SSP, or EP, see an earlier edition of this book.

Table 2. Supported Releases of NCP, SSP, and EP

Product	Release	Operating Systems
NCP	V4R1	VSE
	V4R2	MVS, VM
	V4R3.1	MVS, VM, VSE
	V5R3	VSE
	V5R4	MVS, VM, VSE
	V6R1	MVS, VM
	V6R2	MVS, VM
	V6R3	MVS
	V7R1	MVS, VM, VSE
	V7R2	MVS
SSP	V3R5	VSE
	V3R6	VSE
	V3R7	MVS, VM
	V3R8	MVS, VM
	V3R9	MVS
	V4R1	MVS, VM, VSE
	V4R2	MVS
EP	R3	VSE
	R4	MVS, VM
	R6.1	MVS, VM, VSE
	R7	VSE
	R8	MVS, VM, VSE
	R9	MVS, VM, VSE
	R10	MVS, VM
	R11	MVS, VM
	R12	MVS, VM, VSE

Where to Find More Information

A good place to start any task regarding NCP, SSP, or EP is *NCP V7R2, SSP V4R2, and EP R12 Library Directory*. This directory introduces the enhancements for the current release and shows where these enhancements are described in the NCP library. It gives you an overview of NCP, SSP, and EP and directs you to information on a variety of tasks related to these programs. When you are using the book online, you can use *hypertext links*[1] to move directly from task and enhancement descriptions to the appropriate chapters of other books in the library.

[1] A *hypertext link* is a pointer from a location in an online book to another location in the same book or another book. By selecting highlighted information, such as a message number, you can move quickly to related information and, if desired, back again.

Information for NCP Tasks

The books in the NCP, SSP, and EP library are listed here according to task, along with closely related books and tools you may find helpful. See "Bibliography" on page 423 for brief summaries of each book in the NCP, SSP, and EP library and listings of related publications.

Table 3. Sources of Information by Task

Order No.	Title	Hardcopy	Softcopy
Planning			
SC31-7122	*Planning for NetView, NCP, and VTAM*	■	■
SC31-7123	*Planning for Integrated Networks*	■	■
SX75-0092	*Planning Aids: Pre-Installation Planning Checklist for NetView, NCP, and VTAM*	■	
SC31-6259	*NCP V7R2, SSP V4R2, and EP R12 Library Directory*	■	■
Installation and Resource Definition			
SC31-6221	*NCP, SSP, and EP Generation and Loading Guide*	■	■
SC31-6258	*NCP V7R2 Migration Guide*	■	■
SC31-6223	*NCP, SSP, and EP Resource Definition Guide*	■	■
SC31-6224	*NCP, SSP, and EP Resource Definition Reference*	■	■
Customization			
LY43-0031	*NCP and SSP Customization Guide*	■	
LY43-0032	*NCP and SSP Customization Reference*	■	
Operation			
SC31-6222	*NCP, SSP, and EP Messages and Codes*	■	■
N/A	*Online Message Facility*		D
Diagnosis			
LY43-0033	*NCP, SSP, and EP Diagnosis Guide*	■	
LY43-0037	*NCP, SSP, and EP Trace Analysis Handbook*	■	
LY43-0029	*NCP and EP Reference*	■	
LY43-0030	*NCP and EP Reference Summary and Data Areas*	■	
LK2T-1999	*NCP, SSP, and EP Diagnosis Aid*		D
Monitoring and Tuning			
SC31-6247	*NTune User's Guide*	■	■
LY43-0035	*NTuneNCP Reference*	■	

D Available on diskette for the IBM OS/2 environment.

Those publications available as softcopy books have cross-document search and hypertext links for speedy, online information retrieval. These softcopy books are grouped together on an electronic bookshelf and are part of the *IBM Networking Systems Softcopy Collection Kit* on compact disc read-only memory (CD-ROM).

You can view and search softcopy books by using BookManager* READ products or by using the IBM Library Reader* product included on CD-ROM. For more information on CD-ROMs and softcopy books, see *IBM Online Libraries: Softcopy Collection Kit User's Guide* and BookManager READ documentation.

Part 1. Reporting Problems to the IBM Service Center

Chapter 1. Overview of the Diagnosis Procedure

To diagnose an NCP problem, you first identify the problem, then determine if it is a problem with NCP, and, finally, gather information about the problem so that you can report the source of the problem to the IBM Support Center. With this information available, you can work with IBM Support Center representatives to resolve the problem. The object of this book is to help you identify the source of the problem.

Figure 1 on page 4 summarizes the procedure to follow to diagnose a problem. The text following the figure provides more information about this procedure.

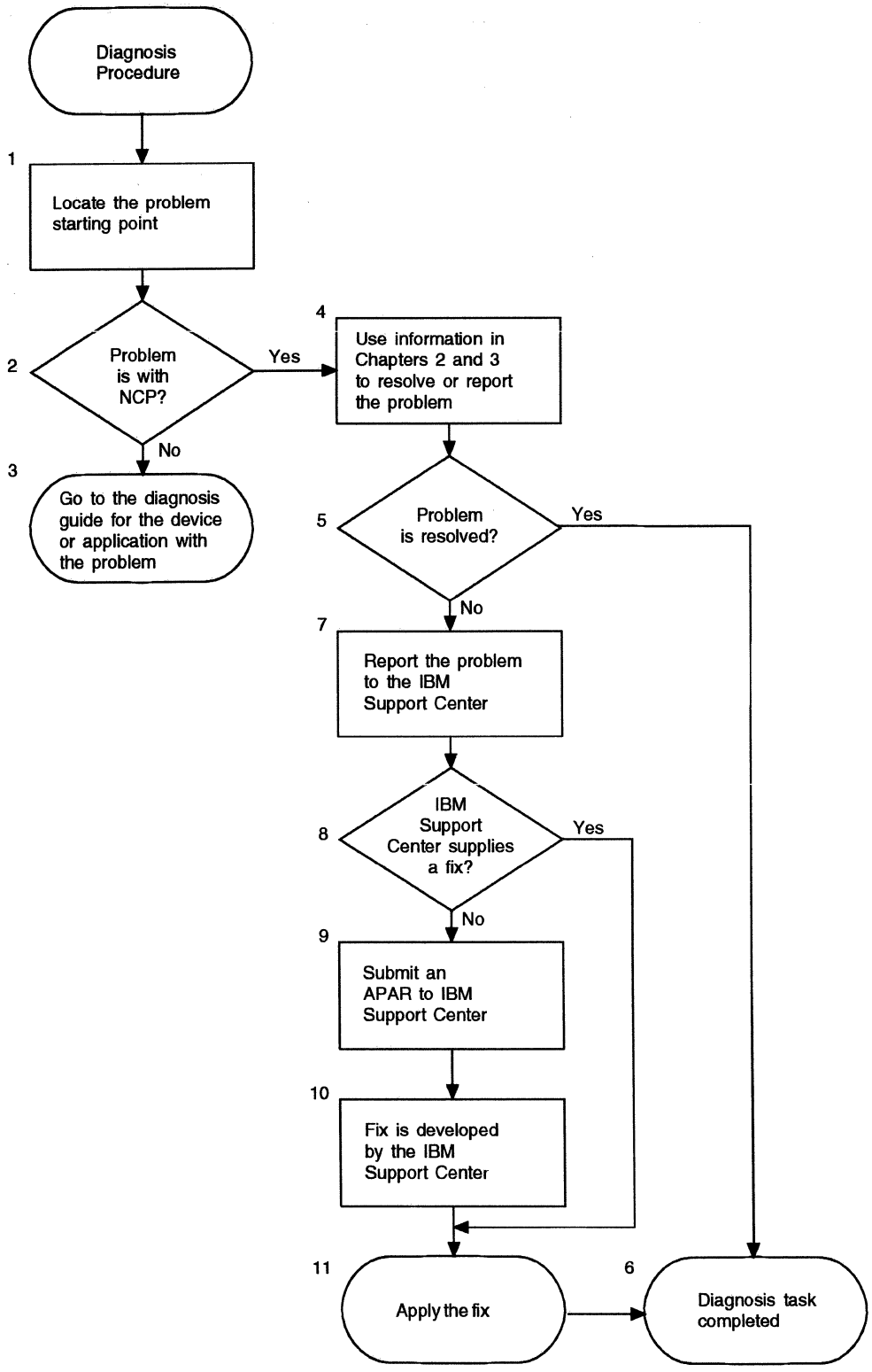


Figure 1. Overview of the Diagnosis Procedure

Step 1. **Locate the problem starting point.**

Various messages, alerts, and diagnostic aids provide information that isolate the starting point of a problem.

Step 2. **Determine if the problem is with NCP.**

Because NCP interacts with programs in the host processor and with terminals in a network, it is easy to mistake an error in an access method or a hardware failure in a terminal for an NCP problem. Chapter 2 tells you how to make certain that the problem is with NCP. If the problem is with NCP, go to Step 4; otherwise, go to Step 3.

Step 3. **Check appropriate books.**

See the diagnosis guide of the hardware device or software application that has the problem.

Step 4. **Gather information.**

When you are sure that the problem is with NCP, gather information to describe the problem. Chapter 2 tells you what information to gather.Chapter 3 explains diagnostic procedures and how to collect information relevant to the problem.

Step 5. **Try to resolve the problem.**

If you can resolve the problem, go to Step 6; otherwise, go to Step 7.

Step 6. **The diagnosis task is completed.**

The problem has been resolved.

Step 7. **Report the problem to the IBM Support Center.**

After you have gathered the information that describes the problem, report it to the IBM Support Center. If you are connected to the RETAIN database, you can perform your own RETAIN searches to help identify problems. Otherwise, a representative uses your information to build keywords to search the RETAIN database for a solution to the problem.

The object of this keyword search using RETAIN is to find a solution by matching the problem with a previously reported problem. When IBM develops a solution for a new problem, it is entered into RETAIN with a description of the problem.

Step 8. **Work with IBM Support Center representatives.**

If a keyword search matches a previously reported problem, its solution may also correct the problem. If so, go to Step 11 on page 6. If a solution to the problem is not found in the RETAIN database, the IBM Support Center representatives will continue to work with you to solve the problem. Go to Step 9.

Step 9. **Submit an APAR.**

If the IBM Support Center does not find a solution, you will be asked to submit an authorized program analysis report (APAR) to the IBM Support Center.

Step 10. **A fix is developed by the IBM Support Center.**

Using information supplied in the APAR, IBM Support Center representatives determine the cause of the problem and develop a solution for it.

Step 11. **Apply the fix.**

Apply the corrective procedure supplied by the IBM Support Center to correct the problem.

Resolving Problems in High-Severity Situations

If the IBM Support Center cannot find a solution to the problem by searching the RETAIN database, the problem is forwarded to a component specialist (Level 2). This specialist requires detailed information about the problem. For help in carrying out an in-depth analysis of the problem, See *NCP and EP Reference Summary and Data Areas*, Volumes 1 and 2, and the *NCP and EP Reference*. By answering questions and following procedures as directed by the component specialist, you can provide the necessary information to resolve the problem.

Working with a component specialist by telephone to solve a high-severity problem requires a detailed analysis of the problem. If you think you are not qualified to do an in-depth analysis or if you feel the error is too severe, you can request that the local IBM branch office dispatch someone to assist you. The IBM Support Center can help you arrange this.

Command Syntax Diagrams

This book uses standard IBM syntax diagrams to describe the syntax commands, macros, and control statements. These diagrams use the following conventions:

- Read the diagrams from left to right. In general, any path between the start symbol (►►) and the end symbol (►◄) represents valid coding for a keyword.

  ```
  ►►─┤ Syntax diagram ├─►◄
  ```

- A long diagram may be broken into two or more lines.

  ```
  ►►─┤ First line ├─►
  
  ►─┤ Second line ├─►◄
  ```

- A keyword that appears on the main path is required. You must code all required keywords.

  ```
  ►►─KEYWORD=value─►◄
  ```

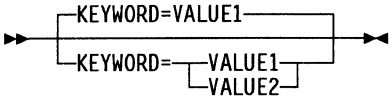
- A keyword that appears below the main path is optional. You do not need to code optional keywords. Most NCP keywords are optional.

  ```
  ►►─┬──────────────┬─►◄
     └─KEYWORD=value─┘
  ```

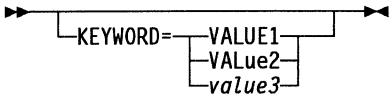
- When you can choose from more than one keyword value, those values are stacked vertically below the main path.

  ```
  ►►─┬──────────────┬─►◄
     └─KEYWORD=─┬─VALUE1─┬─┘
                └─VALUE2─┘
  ```

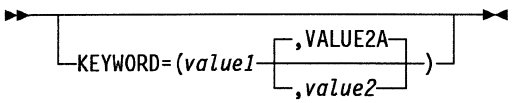
- If a keyword has a default value, the keyword and value appear above the main path.



- Uppercase characters show values you code exactly as shown (VALUE1 below). Uppercase characters in a mixed-case string indicate that you can code an abbreviation (VALue2 below means you can code VAL or VALUE2). Lowercase italics show variables for which you need to supply a value, such as a number or string (*value3* below). Do not code a space or comma between the digits of a numeric value.

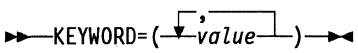


- Multiple keyword values in parentheses are called *suboperands*. Required suboperands appear on the main path between the parentheses (*value1* below). Optional suboperands appear below the main path between the parentheses (*value2* below). Default values for optional suboperands appear above the main path between the parentheses (VALUE2A below). All suboperands must be separated by commas.

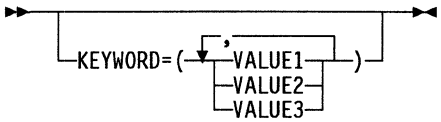


  Note: If a default is not shown for an optional suboperand, this means that either there is no default or that the default depends on what you code on other keywords or suboperands. You have to read the keyword description to find out about this.

- An arrow returning to the left above a suboperand indicates that you can code multiple values, enclosed in parentheses and separated by commas.

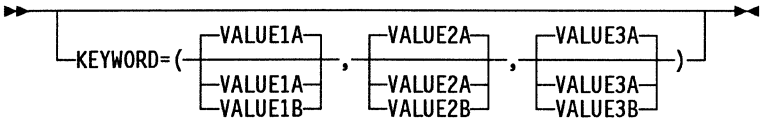


- An arrow returning to the left above a stacked list of suboperands means that you can code as many of the suboperands as you need and in any order. Do not code the same suboperand more than once. Separate each suboperand you code with a comma. For example you could code KEYWORD=(VALUE3,VALUE1) for the keyword below.

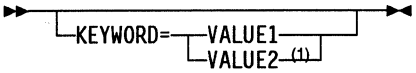


- If you omit an optional suboperand, code a comma to indicate its position. For example you could code KEYWORD=(VALUE1B,,VALUE3B) for the keyword below to omit the second suboperand. Commas are not required if you omit optional suboperands at the end of a suboperand list. For example you could

code KEYWORD=(VALUE1B,VALUE2A) or KEYWORD=(VALUE1B,VALUE2A,) to omit the last suboperand for the keyword below; the result would be the same. If you code only the first suboperand, parentheses are not required. For example you could code KEYWORD=VALUE1B or KEYWORD=(VALUE1B) for the keyword below; the result would be the same. If you omit all suboperands or do not code the keyword, the defaults are used. For example you could code KEYWORD=(), KEYWORD=(,,), or not code the keyword at all for the keyword below; the result would be the same.

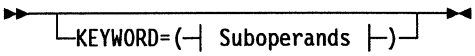


- Restrictions on the use of a keyword value are indicated by superscript numbers in parentheses and are explained below the diagram. Do not code the superscript number or parentheses.

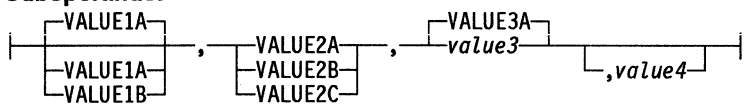


Note:
[1] Restriction on VALUE2.

- A section of a long diagram may appear separately below the main diagram.



Suboperands:



Chapter 2. Identifying the Problem and Gathering Information

This chapter contains information that helps you identify the problem you have and gather information to document the problem.

Making Sure the Problem Is with NCP

The most important step in problem diagnosis is finding the source of the problem. The first step of this search involves identifying the component in which the problem occurred. Because NCP interacts directly with both the host processor and the terminals in a network, an error in an access method or a hardware failure in a terminal may appear as NCP's failure to route data properly. If NCP did not cause the failure, you can waste time analyzing NCP for its cause. This book aids in NCP diagnosis and contains information to help you define the problem.

To determine whether NCP caused the problem, analyze how the data flows through the network. You may need diagnostic aids—such as a console log, path information unit (PIU) traces, and line traces—to help find the cause of the problem. The *NCP, SSP, and EP Trace Analysis Handbook* and Chapter 4 in this guide contain information about these and other types of diagnostic aids. Also, see the *Trace Analysis Handbook* for information about using ACF/TAP.

As you examine your network flow, look for the first symptom of a problem. For example, if more than one message was issued, find the first one and determine why it was issued. If a PIU did not get through the network, find out how far it went. Did it get a negative response? Which component responded? Why? Was the PIU valid? The console log is a useful tool for validating operational problems or sequences.

After you identify the first symptom of the problem, see "Determining the Problem Type" on page 10. This section helps you determine a problem type based on the symptom you identify and refers you to the section in Chapter 3 that describes how to diagnose the problem.

If a diagnostic procedure requires specific information from an NCP dump or a communication controller's operation panel, you will get pointers to the information. A pointer to a control block is usually a fullword location in NCP storage that contains the address of the control block. To find the address of the control block, display the address shown at the pointer's location in NCP storage. To find the contents of a specific field inside a control block, add the offset given to the address of the control block and display the resulting address.

It can be difficult to interpret the information you obtain from dumps, traces, and other diagnostic aids. This book does not teach you how to analyze these materials, but instead tells you about the available types of service aids and how to use them. For more information on how to interpret traces, dumps, and other service aids, see *NCP and EP Reference Summary and Data Areas*, Volume 1; *NCP and EP Reference*, *NCP, SSP, and EP Trace Analysis Handbook*, and the diagnosis guides and diagnosis reference manuals for VTAM and TCAM (*VTAM Diagnosis*, *TCAM Diagnosis Reference*, and *TCAM Diagnosis Guide*). You can also call the IBM Support Center for help in analyzing your diagnostic aid data. If, after ana-

lyzing the data flow through the network, you find that the problem does not seem to originate in NCP, see the diagnosis guide for the product that you believe caused the error.

Before You Start Diagnosing a Problem

Before trying to determine the type of problem you have, consider the following questions:

- Has the system run successfully before?
- Have you made any changes since the last successful run: authorized program analysis report (APAR) fixes, program temporary fixes (PTFs) user modifications, application changes, hardware changes, table changes?
- If you have applied fixes, have you reassembled and link-edited all modules? Did you have any problems applying the fixes?
- If you have applied fixes, does the system execute successfully if you back out the fixes?
- Are the parameters you used to start the system the same as when you successfully ran the system?
- Can you re-create the problem?
- If the problem is recurrent, does it always show the same symptoms?
- Does the problem relate to a certain application program or application program request, for example, RECEIVE, SEND, CLSDST?
- Does the problem depend on processor load, network activity, or time?
- Does the problem affect the complete network? If not, does it affect a certain line, line type, terminal, or terminal type?
- Are there record maintenance statistics (RECMS) in the LOGREC data set for the problem?
- Is there a network management vector transport (NMVT) in the NetView* program for the problem?

Determining the Problem Type

The following problem types can be used to categorize NCP or EP problems:

- EP error in PEP
- Abend
- Activate or deactivate
- Selective scanning
- Communication controller alert
- Documentation
- NDF generation
- Hung session and resource
- Link problem determination aid (LPDA) solicited tests
- LPDA unsolicited tests
- Message
- NCP load and initialize
- Loop

- Performance
- Internet Protocol
- Frame-relay link
- Network flow control.

Chapter 3 includes procedures to diagnose problems in each of these categories. To determine the category for the problem, see the following table. This table lists symptoms alphabetically, identifies the problem type, and shows the page where the diagnosis procedure is documented.

Find the symptom you are experiencing and see the page indicated. If none of the symptoms matches yours exactly, choose the one most similar to your symptom.

Table 4 (Page 1 of 3). Mapping Symptoms to Problem Types

Symptom	Problem Type	Page
ABEND message is issued	NCP or EP abend	25
Abnormal condition occurs during NCP generation	NCP generation	53
Activate failure of NCP occurs (channel-attached communication controller)	NCP load and initialize	86
Activate resource failure because of lack of resources	Activate or deactivate	40
Alarm is generated at the MOSS console	Communication controller alert	49
Alert is generated at the host console (the NetView program)	Communication controller alert	49
Book contains wrong or ambiguous information	Documentation	51
Book is missing information	Documentation	51
Books contradict each other	Documentation	51
BSC lines are not being polled	NCP performance (slowdown)	94
Busy condition occurs at a user terminal	Hung session and hung resource	57
DATA-INVALID-FOR-THIS-NODE message is issued	NCP or EP abend	25
Dynamic routes are not recognized by NCP	Internet route error	105
Frame-relay link stations are hung (PCTD1)	NCP frame-relay link	109
EP dial connection is broken	EP in a PEP environment	19
Equipment check is received at the host	EP in a PEP environment	19
Hung resource occurs	Hung session and hung resource	57
Hung session occurs	Hung session and hung resource	57
Initialize failure of NCP occurs (channel-attached communication controller)	NCP load and initialize	86
Internet traffic is lost or not flowing	Internet route error	101 or 105

1 This may also be a *loop* problem.

2 This may also be a *network flow control* problem.

Table 4 (Page 2 of 3). Mapping Symptoms to Problem Types

Symptom	Problem Type	Page
I/O error occurs for the communication controller's channel address (channel-attached communication controller)	NCP or EP abend	25
Invalid response to LPDA test occurs	LPDA	75
LOAD FAILURE message is issued (sense code X'081C 0020' or X'081C 0014')	NCP or EP abend	25
Load failure of NCP occurs (channel-attached communication controller)	NCP load and initialize	86
LOST-CONTACT-WITH-NCP'S-SUBAREA message is issued	NCP or EP abend	25
LPDA unsolicited test error occurs	LPDA	75
Message indicates an error in the message itself	Message	84
Message is issued under inappropriate conditions	Message	84
Message is not documented in *NCP, SSP, and EP Messages and Codes*	Message	84
Message is wrong or formatted incorrectly	Message	84
Message text does not explain condition	Message	84
Multiple lines are failing	Selective scanning	46
NCP does not operate as described in a book	Documentation	51
NCP or EP does not respond to commands entered on the console	NCP or EP loop NCP or EP abend	91 Page 25
NCP or EP functions stop	NCP or EP loop	91
NCST session does not activate	Ethernet-type LAN or Internet Protocol	101 or 105
Negative response to LPDA test occurs	LPDA	75
No Ethernet-type LAN traffic is flowing	Ethernet-type LAN or Internet Protocol	101 or 105
No response to LPDA test	LPDA	75
No response for network users	Network flow control	115
Pacing is withheld by NCP	Hung session and hung resource	57
Performance is degraded after a network outage	NCP performance	94
Performance is poor on an Ethernet-type LAN	Ethernet-type LAN or Internet Protocol	101 or 105
Printers stop	NCP or EP loop	91
Resource fails to respond	Activate or deactivate	40
Resource returns an NCP exception response	Activate or deactivate	40
Response does not occur	NCP performance [1, 2]	94
Response is slow	NCP performance [1, 2]	94
Route activation failure occurs	Activate or deactivate	40
SDLC physical units are receive-not-ready (RNR) polled	NCP performance	94
Session fails to come up	Activate or deactivate	40

[1] This may also be a *loop* problem.

[2] This may also be a *network flow control* problem.

Table 4 (Page 3 of 3). Mapping Symptoms to Problem Types

Symptom	Problem Type	Page
Slow response time	Network flow control	115
Tapes stop	NCP or EP loop	91
Time-out occurs	EP in a PEP environment	19
Traffic between an application program and a terminal stops	Hung session and hung resource	57
Traffic is slow on all lines linked to the scanner	Selective scanning	46
Unit check is received at the host	EP in a PEP environment	19
Virtual route is out of sequence	Hung session and hung resource	57
Virtual route pacing response does not occur	Hung session and hung resource	57
Virtual routes attached to NCP are held	NCP performance (slowdown)	94
Virtual routes on a transmission group are held	Hung session and hung resource	57
Wait light on IBM 3725 panel is off	NCP or EP loop	91

1 This may also be a *loop* problem.

2 This may also be a *network flow control* problem.

Gather Information to Document the Problem

As you follow the procedures in this book to define the problem, you will gather various types of information about the problem. This documentation is important not only for locating the problem's cause, but also for resolving the problem. IBM Support Center representatives need this information to build a keyword string to search the RETAIN database for a solution to the problem. Also, if they submit an APAR, IBM Support Center representatives will include printed copies of this documentation with the APAR.

Before you contact the IBM Support Center to report the problem, be sure you have all necessary documentation. Depending on the type of NCP or EP problem, the documentation requirements will differ.

The IBM Support Center requires three kinds of documentation for all problems that you report: general documentation, release information, and documentation related to specific problems. In addition, you can collect and analyze trace reports to help you and the IBM Support Center solve the problem.

Collecting General Documentation

Table 5 on page 14 lists the general documentation you may need to provide for all problems.

Table 5. Documentation Required for All Problems

Documentation	Description
Program update tapes (PUTs) and PTFs	List all the PUTs and PTFs that you applied to your system. Also, list all the fixes or APARs you applied to your system as well as any changes you made to the hardware.
Problem description	List all the problem's symptoms and the first indication you had of the problem.
Terminal types	List all terminal types affected by the problem.
Line discipline	List the link protocol you used.
Recovery attempts	List the types of recovery attempts you made before taking a dump or trace.
List of changes to the network configuration	List any application programs, new devices, new products, new releases of the product, or new levels of the operating system you added.
Version and release numbers	List the version and release numbers for NCP and any related products included in your NCP load module—for instance, Network Terminal Option (NTO), EP, or X.25 NCP Packet Switching Interface (NPSI).
System console or hard-copy log	Supply the console or hard-copy log to show all messages sent to and commands received from the operator. This log provides clues about when the system began having problems. (NCP or EP problems may not be apparent at the time they occur.)
NCP generation definition	Supply the NCP generation definition, a set of definition statements for resources in your NCP and other related products if they are installed. Detailed information about the NCP generation definition is in *NCP, SSP, and EP Resource Definition Reference.*

Collecting Release Information

Table 6 lists NCP, SSP, and EP release information. Refer to this table to gather release information about your network.

Table 6 (Page 1 of 2). NCP, SSP, and EP Release Information Needed to Report a Problem

IBM Licensed Program	Program ID Number	Component ID Number	Field Maintenance ID Number or VSE Component Level Code	Release Level
NCP Version 4				
R1 VSE	5668-854	5668-854-01	A65	165
R2 MVS	5668-854	5668-854-01	HNC4205	205
R2 VM	5668-854	5668-854-01	N/A	425
R3.1 MVS	5668-854	5668-854-01	HNC4310	310
R3.1 VM	5668-854	5668-854-01	N/A	431
R3.1 VSE	5668-854	5668-854-01	D34	434
NCP Version 5				
R3 VSE	5668-738	5668-738-01	E61	561
R4 MVS	5668-738	5668-738-01	HNC5402	402
R4 VM	5668-738	5668-738-01	N/A	542
R4 VSE	5668-738	5668-738-01	CH0	380
NCP Version 6				
R1 MVS	5688-231	5688-231-00	HNC6102	102
R1 VM	5688-231	5688-231-00	N/A	612
R2 MVS	5688-231	5688-231-00	HNC6202	202

Table 6 (Page 2 of 2). NCP, SSP, and EP Release Information Needed to Report a Problem

IBM Licensed Program	Program ID Number	Component ID Number	Field Maintenance ID Number or VSE Component Level Code	Release Level
R2 VM	5688-231	5688-231-00	N/A	622
R3 MVS	5688-231	5688-231-00	HNC6302	302
NCP Version 7				
R1 MVS	5648-063	5648-063-00	HNC7102	102
R1 VM	5648-063	5648-063-00	N/A	712
R1 VSE	5648-063	5648-063-00	3A0	3A0
R2 MVS	5648-063	5648-063-00	HNC7202	202
SSP Version 4				
R1 MVS	5655-041	5655-041-00	HSP4410	410
R1 VM	5654-009	5654-009-00	N/A	410
R1 VSE	5686-064	5686-064-00	F41	390
R2 MVS	5655-041	5655-041-00	HQP2420	420
EP				
R6.1 MVS	5735-XXB	5748-EP-115	HEP1611	611
R6.1 VM	5735-XXB	5748-EP-115	N/A	621
R6.1 VSE	5735-XXB	5748-EP-115	F12	612
R7 VSE	5735-XXB	5748-EP-115	I09	909
R8 MVS	5735-XXB	5748-EP-115	HEP1800	800
R8 VM	5735-XXB	5748-EP-115	N/A	810
R8 VSE	5735-XXB	5748-EP-115	159	959
R9 MVS	5735-XXB	5748-EP-115	HEP1900	900
R9 VM	5735-XXB	5748-EP-115	N/A	910
R9 VSE	5735-XXB	5748-EP-115	CH6	386
R10 MVS	5735-XXB	5748-EP-115	HEP1005	005
R10 VM	5735-XXB	5748-EP-115	N/A	B10
R11 MVS	5735-XXB	5748-EP-115	HEP1B00	B00
R11 VM	5735-XXB	5748-EP-115	N/A	B11
R12 MVS	5735-XXB	5748-EP1-15	HEP1C00	C00
R12 VM	5735-XXB	4748-EP1-15	N/A	1C0
R12 VSE	5735-XXB	5748-EP1-15	4A1	4A1
NCP/EP Common Code (PEP)				
V4R1 VSE	5668-854	5668-854-01	A64	164
V4R2 MVS	5668-854	5668-854-01	HNC4203	203
V4R2 VM	5668-854	5668-854-01	N/A	423

Collecting Documentation for a Specific Problem

Symptoms of a problem are often related to an update to the system, a particular device, or a command. The following sections describe the documentation you should submit to the IBM Support Center if you suspect one of these symptoms as a cause of the problem.

APAR or PTF Number

If the problem is related to an APAR fix, supply the APAR number. If the fix was a PTF, supply the PTF number. The format of APAR and PTF numbers for all operating systems is as follows:

APAR	IRnnnnn
PTF	URnnnnn

Device Type

If the problem is related to a terminal type or other hardware unit, supply the device type, such as 3278 Model 2. If the problem is related to a type of communication link, supply the appropriate link characteristics, such as Synchronous Data Link Control (SDLC), binary synchronous communication (BSC), Systems Network Architecture (SNA), or non-SNA. Also, identify any recent microcode activity on the control units involved.

Hardware Error Condition

If the problem is related to a hardware error, note the failure condition that accompanied it, such as UNIT CHECK or TIMEOUT. Hardware errors might be detected and reported in one or more of the following ways:

- An operating system message
- A VTAM application program message
- A notification from the system operator
- A notification from a terminal user (an indicator of the error status appears in the operator information area at the bottom of the terminal screen)
- A VTAM buffer filling with identical information from one device
- A LOGREC message (MVS or VM)
- A SYSREC or RMS message (VSE)
- An alert to the NetView program.

If you suspect hardware problems, use the NetView program or Network Problem Determination Application (NPDA), if they are available on your system, or use the system console message, which identifies the affected subarea. If you do not have the NetView program, see the *NCP, SSP, and EP Trace Analysis Handbook* ("Buffer Trace Capture of NMVTs"). for information on capturing alerts flowing between NCP and VTAM. If you still need assistance, contact your local IBM branch office.

See the *NCP and EP Reference Summary and Data Areas, Volume 2* for detailed alert information.

Hardware Failures

If the problem is related to hardware failure, use the following tools to collect information about the failure:

- SDLC link level 2 test
- NCP intensive mode error recording
- The NetView program or NPDA (if available on your system)
- MVS or VM LOGREC (or similar operating system facilities)
- VSE SYSREC (or similar operating system facilities).

Definition Statements

If the problem is related to an NCP definition statement, supply the definition statement name and include any keywords associated with the problem.

Coding Changes

If your problem is related to a coding change to an NCP definition statement or a user-coded exit routine, supply the definition statement changes or user-coded exit routine changes.

Using Trace Reports to Gather Information

To solve a problem the IBM Support Center may require trace information of the malfunction. See The *NCP, SSP, and EP Trace Analysis Handbook* for information on producing trace data and trace reports. The "Trace Data to Trace Report Reference" table shows different types of trace data and the reports to create for that data. These reports are the minimum that IBM may request when assisting you in resolving a problem.

Chapter 3. Procedures for NCP or EP Problems

This chapter discusses how to document and diagnose the major NCP or EP problems:

- EP error in partitioned emulation program (PEP)
- Abend
- Activate or deactivate
- Selective scanning
- Communication controller alert
- Documentation
- NCP generation
- Hung session and resource
- Link problem determination aid (LPDA) solicited tests
- LPDA unsolicited tests
- Message
- NCP load and initialize
- Loop
- Performance
- Ethernet-type LAN or Internet Protocol
- NCP frame-relay link
- Network flow control.

This chapter describes each problem, provides a documentation checklist that outlines what information to gather about the problem, and specifies a diagnostic procedure or checklist to help you troubleshoot the problem. Each diagnostic procedure section contains a flowchart with a corresponding step-by-step analysis of how to diagnose the problem.

EP Error Procedure in a PEP Environment

Because EP interacts with programs in the host processor and with terminals in a network, it is easy to mistake an error in an access method or a hardware failure in a terminal for an EP problem. The following symptoms indicate an EP problem in PEP:

- EP dial connection is broken.
- Equipment check is received at host.
- Time-out occurs.
- Unit check is received at host.

Documentation Checklist

If the problem is caused by an EP error, use the procedure in Figure 4 on page 27 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- The EP level you are running, such as EP Release 12
- The ID numbers and the release level for your networking systems product (see Table 6 on page 14)
- The access method that supports your EP, such as BTAM or TCAM
- A copy of your NCP generation definition

- A list of all fixes, such as program temporary fixes (PTFs) and authorized program analysis report (APAR) fixes, that have been applied to your system
- Any recent changes made in your system.

In addition, the IBM Support Center representative may request printed output from the diagnostic aids and dump utilities discussed in "Part 2. Diagnostic Aids." If you send any printed output to IBM, write the problem number or the APAR number given to you by the IBM Support Center representative on the output.

Diagnostic Procedure

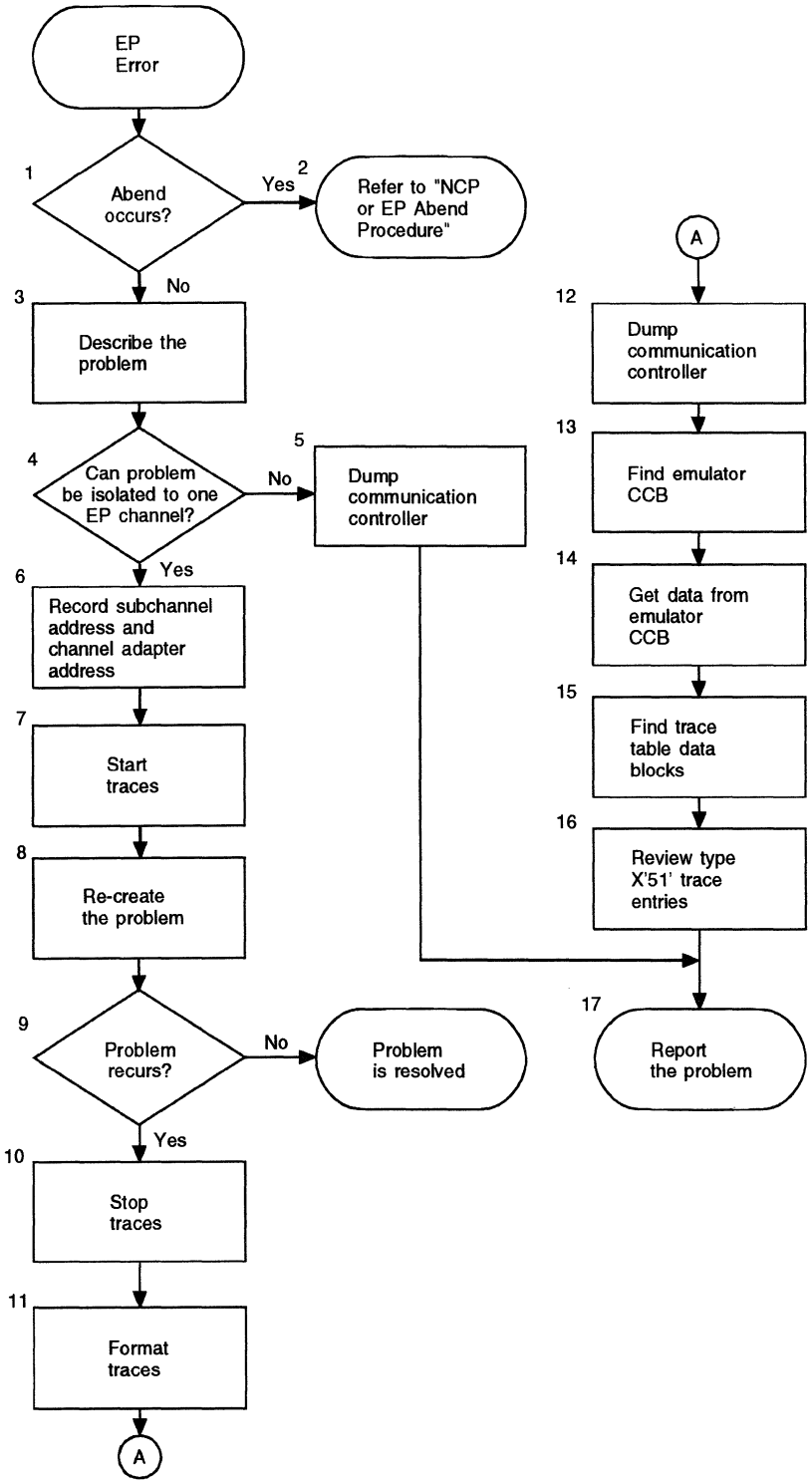


Figure 2. Overview of the EP Error Diagnostic Procedure

Step 1. Check for Abend

If the system abended, go to "NCP or EP Abend Procedure" ; otherwise, go to "Step 3. Describe the Problem."

Step 2. See Abend Error Procedures

See "NCP or EP Abend Procedure" on page 25 for detailed instructions on diagnostic procedures for abend problems.

Step 3. Describe the Problem

Describe the symptoms of the problem. Consider the following questions:

- What was the first indication of a failure?
- Did the host or terminal receive any error messages? If so, record the message number and the text of the error messages.
- Try to summarize the problem. For example:

  The dial connection was broken.
  An equipment check was received at the host.
  A unit check was received at the host.
  A specific command was rejected.
  A time-out occurred.

Step 4. Can Problem Be Isolated

If the problem can be isolated to one EP channel, go to "Step 6. Record the Problem Subchannel Address" ; otherwise, go to "Step 5. Dump Communication Controller."

Step 5. Dump Communication Controller

Request a communication controller dump using the dynamic dump utility or the SSP dumper utility. For information on using the SSP dumper utility, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

  You can format and print the dump or view the unformatted dump using SSP CLISTs. See Chapter 11 for more information on SSP CLISTs.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

For information on using the dynamic dump utility, see Chapter 1.

Go to "Step 17. Report Problem."

Step 6. Record the Problem Subchannel Address

Record the problem subchannel address and the channel adapter address of the subchannel.

Step 7. Start Traces

Attempt to start an EP level 2 or level 3 trace using a scanner interface trace (SIT) on an active line using the failing subchannel.

If you specified the DYNADMP keyword in your generation definition, use the DYNADMP DYNAMIC control statement to transfer the trace blocks to a host data set. See the *NCP, SSP, and EP Trace Analysis Handbook* for more information.

If you did not specify the DYNADMP keyword in your generation definition, the trace entries will appear in the dump. Some entries may be overwritten because the trace table has a fixed amount of storage.

Note: For information about running SIT, see *NCP, SSP, and EP Trace Analysis Handbook* For information about starting traces with the dynamic dump utility, see "Utility Control Statements" on page 243. For information about starting traces from the maintenance and operator subsystem (MOSS) console, see *3725 Communication Controller Operating Guide*, *3720/3721 Communication Controller Extended Services Guide*, or *IBM 3745 Advanced Operations Guide*.

Step 8. Re-create Problem

Attempt to re-create the problem.

Step 9. Check if Problem Recurs

If the problem recurs, go to "Step 10. Stop Traces" ; otherwise, the problem has been resolved.

Step 10. Stop Traces

When the problem recurs, stop the traces that are running.

Note: For information about running SIT, see *NCP, SSP, and EP Trace Analysis Handbook* For information about starting traces with the dynamic dump utility, see "Utility Control Statements" on page 243. For information about starting traces from the maintenance and operator subsystem (MOSS) console, see *3725 Communication Controller Operating Guide*, *3720/3721 Communication Controller Extended Services Guide*, or *IBM 3745 Advanced Operations Guide*.

Step 11. Format Traces

If you specified the DYNADMP keyword in your generation definition, use the print option to format the trace entries. Use the Advanced Communications Function/Trace Analysis Program (ACF/TAP) to format the SIT records. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using the ACF/TAP program, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 12. Dump Communication Controller

Request a dump using the dynamic dump utility or the SSP dumper utility. See "Utility Control Statements" on page 243 for more information.

You can format and print the dump or view the unformatted dump using SSP CLISTs. See Chapter 11 for more information on using SSP CLISTs.

Step 13. Find the (CCB)

Find the emulator character control block (CCB) for the failing subchannel in the formatted dump

You can display CCB online using SSP CLIST IFWIEPCB.

Step 14. Get Data From Emulator CCB

Using CCB, record the data found at each of the following locations:

Offset	Name of Field	Length
X'38'	Subchannel address	1 byte
X'39'	CCBCFLG	1 byte
X'3A'	CCBSTAT	1 byte
X'3B'	CCBSENSE	1 byte
X'40'	CCBCMD	1 byte
X'4A'	CCBOPT	1 byte
X'4B'	CCBOPT2	1 byte
X'4C'	CCBSTMOD	1 byte
X'4D'	CCBLCD	1 byte
X'64'	Variable meaning	1 byte
X'65'	Variable meaning	1 byte
X'66'	Variable meaning	1 byte

Step 15. Find Trace Table Data Blocks

Find the trace table in the EP dump. See the "EP Line Trace" section in the *NCP, SSP, and EP Trace Analysis Handbook* On the printout of the dump, mark or highlight each block of data that begins with a trace entry of type X'31' and ends with a trace entry of type X'51'. See Figure 3 for an example.

```
                          A  B
                          |  |
02B900  00090001 000001F8 3100902F 88002400   32029650 08800A51 81009000 0240000C   *.......8..................... ..*
02B920  82029680 08800000 83010FAE 0A51F100   81009000 0240000C 82029680 08800000   *.............1..... .........*
02B940  83010FD0 0A510300 11009000 00011088   1240039C 40000303 13000000 0A5A7800   *................. .. ..........*
02B960  16000000 00008000 81009001 0240030C   82029680 08800000 830110B6 0A5A4100   *............. .................*
02B980  5100900C 0A5A7C00
        |     |
        C     D
```

Figure 3. Sample Block between a Type X'31' Entry and a Type X'51' Entry

Figure 3 is keyed to the following descriptions.

A Type X'31' trace entry. This byte is always the first byte of a fullword.

B Emulation subchannel address. This byte is always the third byte of a fullword that begins with X'31'.

C Type X'51' trace entry. This byte is always the first byte of a fullword.

D X'0C' in type X'51' trace entry. This byte should always be the last byte of a fullword that begins with X'51'.

Step 16. Review Type X'51' Trace Entries

Review the type X'51' trace entries. Circle any of these trace entries that do not have an X'0C' as the last byte of the fullword in which the byte X'51' occurs.

Step 17. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

NCP or EP Abend Procedure

NCP or EP checks for certain conditions and abends when unusual events occur (for example, if a buffer containing a pointer is overlaid during normal operation). In most cases, the abend occurs when the hardware or data integrity is compromised, causing NCP or EP to stop because of the severity of the error. The following symptoms indicate an NCP or EP abend problem:

- ABEND message is issued.
- NCP or EP does not respond to commands entered on the host console.
- I/O error occurs for the communication controller's channel address (channel-attached communication controller).
- LOAD FAILURE message (sense code X'081C 0020' or X'081C 0014') is issued.
- LOST CONTACT WITH NCP'S SUBAREA message is issued.
- DATA-INVALID-FOR-THIS-NODE message is issued.

If the abend occurred when the communication controller was being loaded or dumped, check the MOSS console: the problem may be a controller load and dump program (CLDP) abend, not an NCP or EP abend. For information on CLDP abend codes, see *NCP, SSP, and EP Messages and Codes*

When an abend occurs, use the abend diagnostic procedure, which outlines the steps to follow. You must always obtain an unformatted or formatted dump of the NCP or EP that issued the abend. During the abend diagnostic procedure, gather information from this dump before you call your IBM Support Center about the problem.

In this NCP or EP abend diagnostic procedure, each control block mentioned is displayed in a formatted dump. It is simpler to find the fields in a formatted control block than to follow pointers to the given control block.

You can also use SSP CLISTs to display selected control block information online.

For your convenience, it is recommended you use a formatted dump or CLIST to obtain the information that IBM requests from you.

Use the abend recording forms shown on page 38 along with the NCP or EP abend diagnostic procedure. The step numbers on the form correspond to step numbers used in the procedure.

As you perform the procedure, you will probably not do every step in the procedure. If a particular step is not required or does not pertain to your situation, you do not have to fill out that step on the form. Make additional copies of these forms and keep them in this book so that you will have them available.

Documentation Checklist

If the problem results in an NCP or EP abend, use the procedure in Figure 4 on page 27 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- The level of NCP or EP you are running, such as EP Release 9
- The ID numbers and the release level for your networking systems product (see Table 6 on page 14)
- The access method that supports your NCP or EP, such as BTAM, VTAM, or TCAM
- A copy of your NCP generation definition
- A list of all fixes, such as PTFs and APAR fixes, that have been applied to your system
- Any recent changes made to your system
- Abend recording form
- NCP stand-alone dump.

Diagnostic Procedure

In this procedure, anything mentioned about NCP also applies to EP running with NCP in a partitioned emulation program (PEP) environment unless the differences are specifically noted.

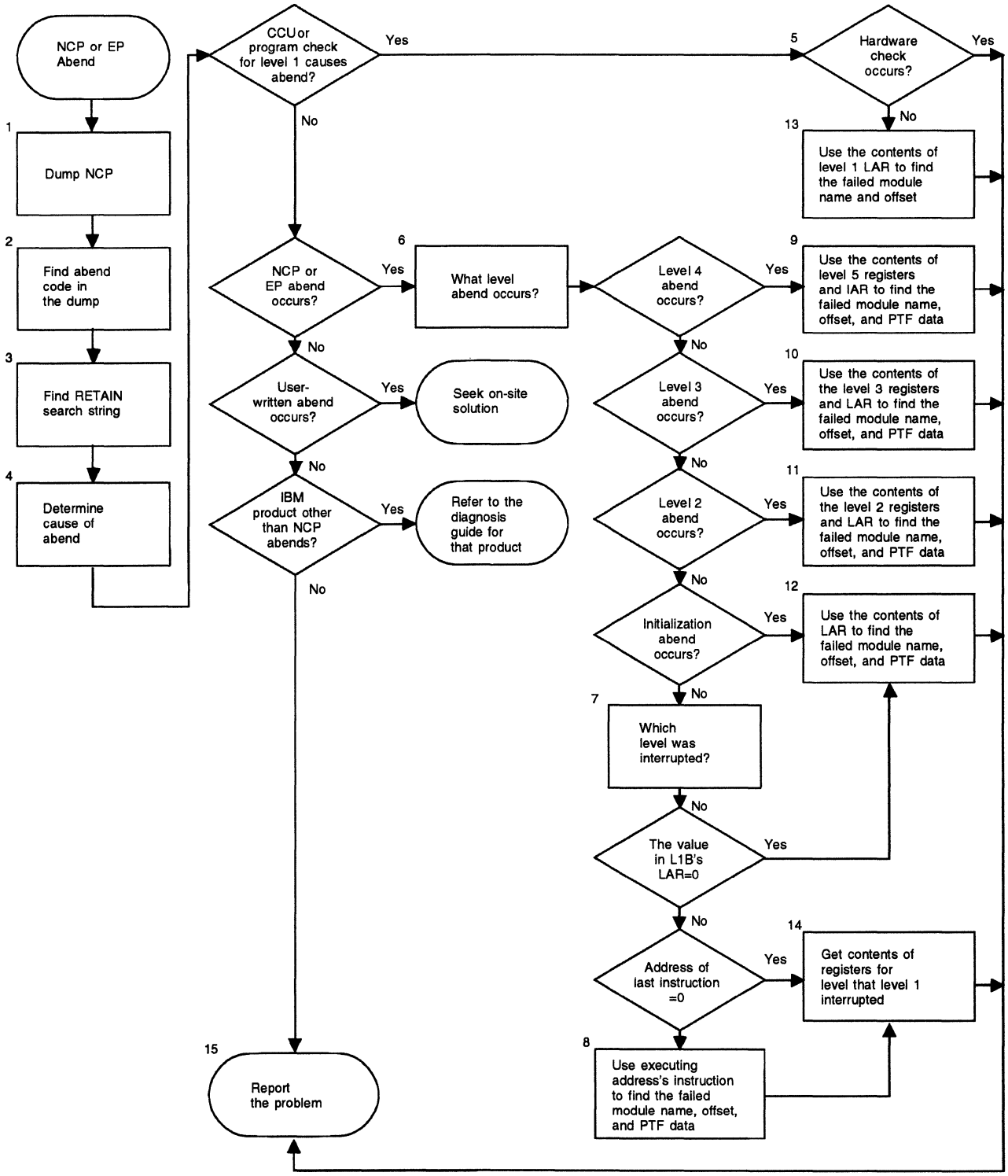


Figure 4. Overview of the NCP or EP Abend Diagnostic Procedure

Step 1. Dump NCP

The first indication of an abend is usually a message at the host console. The message states that an I/O error has occurred for the channel address of the communication controller and that an initial program loader (IPL) is required.

You also get explicit route and virtual route INOP messages, a message that you have lost contact with NCP's subarea, and a message giving you the option to dump NCP.

For information on dumping NCP, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 2. Find Abend Code in the Dump

Find the abend code in the NCP dump. In a formatted dump, the abend code is at the top of every page. Look for corresponding box event records (BERs) in the MOSS under the ELD option.

In an unformatted dump, find the abend code by using the following pointers:

- XDH pointer at X'6E4'
- **NCP V6R1 and Later:** XDH pointer at X'34' (IBM 3745)
- XDH + X'60'= abend code (halfword field).

You can use the SSP CLIST IFWIREGS to display the abend code and register contents online.

Step 3. Find RETAIN Search String

When NCP abends, the SSP dump formatter utility prints the exact input required to search the RETAIN database to see if this problem was previously identified and solved. The RETAIN search string appears on the first page of the report in the format:

```
RIDS/wwwwwwww PIDS/xxxxxxxxx AB/Syyyy ADRS/zzzzzz
```

where:

- wwwwwwww is the module name where the abend occurred
- xxxxxxxxx is the component identification (a 9-byte field from the product set identifier (PSI) control block)
- yyyy is the abend code
- zzzzzz is the offset into the module where the abend occurred.

Be sure to give your IBM Support Center representative this search string when you discuss your NCP abend.

Step 4. Determine Cause of Abend

NCP, another program running in the communication controller, or hardware can cause an abend. Use the following list of abend codes obtained in "Step 2. Find Abend Code in the Dump" to determine the cause of the abend and appropriate action.

X'0000'	Hardware central control unit (CCU) check or a program check for NCP level 1 occurred. If a CCU check or a program check for NCP level 1 occurred and caused an abend, go to "Step 5. Check for Hardware CCU Check."
X'0001'–X'7FFF'	NCP abended or CLDP abend occurred. If NCP abended, go to "Step 6. NCP Abended"
X'8000'–X'80FF'	Network Terminal Option (NTO) abended. See the appropriate diagnosis guide for that product.
X'8100'–X'81FF'	Network Routing Facility (NRF) abended. See the appropriate diagnosis guide for that product.
X'0A00'–X'0AFF'	X.25 NCP Packet Switching Interface (NPSI) abended. See the appropriate diagnosis guide for that product.
X'C000'–X'FFFF'	User-written program abended. Seek an on-site solution. Call the person in your organization who corrects user program problems.

If the abend code defined in "Step 2. Find Abend Code in the Dump" is not listed above, go to "Step 15. Report Problem."

For more information on abend codes, see *NCP, SSP, and EP Messages and Codes*. The ABN extension contains a diagnostic area where certain abends store information before abending. See the individual abend code for details.

Step 5. Check for Hardware CCU Check

Check if a hardware CCU check has occurred. A hardware CCU check causes most X'0000' abends. However, level 1 program checks can also cause this kind of abend. Look at the failing communication controller and verify that a hardware check has occurred.

Go to the MOSS console to see if a CCU check was logged and the CCU was stopped.

The hardware sets three external registers when a CCU check occurs. These registers are located in the formatted level 1 control block (L1B). If you have a formatted NCP dump, you can use the "Formatted Dump Contents" on page 195 to locate L1B. In an unformatted dump, find L1B by using the following pointers:

- XDA pointer at X'6E8'
- **NCP V6R1 and Later:** XDA pointer at X'38' (IBM 3745)
- XDA + X'40' = L1B pointer.

Find the external registers at the following offsets:

L1B + X'04' External register X'7E'. Indicates level 1 CCU interrupt requests.

L1B + X'08' External register X'76'. Indicates level 1 IOC interrupt requests.

L1B + X'28' External register X'7D'. Indicates level 1 CCU hardware checks.

You can use the SSP CLIST IFWIERP to display L1B and external registers online.

Gather the information from these locations.

If the contents of these external registers are all 0's, a hardware CCU check did not occur. NCP level 1 probably abended or a WRITEIPL command was received.

If a hardware check did not occur (contents of these external registers are all 0's), go to "Step 13. Use Contents of Level 1 IAR" ; otherwise, go to "Step 15. Report Problem."

Step 6. NCP Abended

Find information on the abend code in *NCP, SSP, and EP Messages and Codes*.

Identify which level's register 1 contains X'2000' to determine which level abended. Look in the general registers printed before the storage protect keys, which are just before the hexadecimal section of the NCP dump.

You can use the SSP CLIST IFWIREGS to display the general register contents online.

If the abend occurred in level 4, go to "Step 9. Use Contents of Level 5 Registers" ; otherwise, continue.

If the abend occurred in level 3, go to "Step 10. Use Contents of Level 3 Registers" ; otherwise, continue.

If the abend occurred in level 2, go to "Step 11. Use Contents of Level 2 registers" ; otherwise, continue.

If your NCP abended immediately after it was loaded and before it became active, the abend probably occurred during the NCP initialization phase. For information on NCP's initialization phase, see Figure 16 on page 88. If the abend code description in *NCP, SSP, and EP Messages and Codes* states that this problem can occur during initialization, go to "Step 12. Use Contents of LAR" ; otherwise, go to "Step 7. What Level Was Interrupted By Level 1."

Step 7. What Level Was Interrupted By Level 1

If level 1 detected the abend condition, a byte from the external register X'79', located at L1B + X'07', indicates which level was interrupted by level 1. This register is located in the formatted L1B. In an unformatted dump, find L1B by using the following pointers:

- XDA pointer at X'6E8'
- **NCP V6R1 and Later:** XDA pointer at X'38' (IBM 3745)
- XDA + X'40'= L1B pointer.

You can also use the SSP CLIST IFWIERP to display L1B.

To determine which level was interrupted by level 1, compare the byte from L1B with the following list:

X'80' Level 2
X'40' Level 3
X'20' Level 4
X'10' Level 5.

The following fields in L1B contain information useful in solving abends detected by level 1.

L1B + X'00' External register X'74' or lagging address register (LAR) (4 bytes)

You can also use the SSP CLIST IFWIREGS to display LAR.

L1B + X'07' The level executing when the level 1 interrupt occurred (1 byte)

L1B + X'0C' The instruction address register (IAR), register 0, for the level executing when the level 1 interrupt occurred (4 bytes)

L1B + X'10' Address of the instruction executing when the level 1 interrupt occurred (4 bytes)

L1B + X'14' The first 2 bytes of the instruction executing when the level 1 interrupt occurred (2 bytes)

L1B + X'52' The abend code (2 bytes).

Gather the following information from the preceding L1B list:

1. If the value of LAR in L1B is 0, go to "Step 12. Use Contents of LAR" ; otherwise continue.
2. If the address of the instruction executing when the level 1 interrupt occurred is 0, go to "Step 14. Get Registers for Interrupted Level" ; otherwise, go to "Step 8. Use Executing Address Instruction."

Step 8. Use Executing Address Instruction

Use the address of the instruction executing when the level 1 interrupt occurred to find the name of the module at that address and the offset into the module. You can find the module name and offset in the hexadecimal section of the NCP dump or in the load map printed as part of the NCP formatted dump.

You can use the SSP CLIST IFWIWHER to display the module name, offset, and PTF maintenance level. Record this information on your abend recording form. Go to "Step 14. Get Registers for Interrupted Level."

In the dump's hexadecimal section, the module name is at the end of the module. To find the beginning of the module, return to the previous module name and then go forward 8 bytes. You will then be at the beginning of the NCP module.

To use the load map, find the row containing a START column and an END column. The address is located between these columns, and the module name is at the beginning of the row.

To calculate the offset into the module, subtract the starting address of the module from the IAR.

If the module name starts with the letters *CY*, it is an EP module. EP modules have the module name at both the beginning and the end of the module. To determine the beginning of the EP module, back up from the module name that you have found to the previous module name. If this previous module name is the same as the one you started from, it is the beginning of the module. If the module name that you back up to is different from the module name you started with, go forward 8 bytes. You will then be at the beginning of the EP module.

After you record the module's name and offset on your abend recording form, determine the PTF maintenance level of this particular module. Locate the level as follows:

- For NCP, find the number preceded by the letters *UR* printed just before the module's name in the unformatted section of the NCP dump.
- For EP, find the number preceded by the letters *IR* at approximate offset X'0A' from the beginning of the module.

Record this number on your abend recording form.

Go to "Step 14. Get Registers for Interrupted Level."

Step 9. Use Contents of Level 5 Registers

Use the contents of the level 5 registers and IAR to find the name, offset, and PTF of the failed module. If X'2000' is in register 1 for level 4, level 5 probably issued an erroneous supervisor call (SVC) or issued an abend. Record the contents of all the level 5 registers. Find them either in the register save areas in ABN (see "Step 14. Get Registers for Interrupted Level" for a description of ABN) or in the registers printed at the beginning of the load map, just before the hexadecimal section of the NCP dump. The level 5 IAR, register 0, points to the attempted SVC instruction in the hexadecimal dump. This is preceded by an Exit instruction, which is X'0070'.

This Exit instruction is part of the SVC that level 5 executed. Find the name of the module that contains the SVC and the offset into the SVC module. You can use the hexadecimal section of the NCP dump or the load map printed as part of the NCP formatted dump.

You can use the SSP CLIST IFWIWHER to display the module name, offset, and PTF maintenance level. Record this information on your abend recording form. Go to "Step 15. Report Problem."

In the dump's hexadecimal section, the module name is at the end of the module. To find the beginning of the module, return to the previous module name and then go forward 8 bytes. You will then be at the beginning of the NCP module.

To use the load map, find the row containing a START column and an END column. The address is located between these columns, and the module name is at the beginning of the row.

To calculate the offset into the module, subtract the starting address of the module from the IAR.

If the module name starts with the letters *CY*, it is an EP module. EP module names are at both the beginning and the end of the module. To determine the beginning of the EP module, back up from the module name that you have found to

the previous module name. If the previous module name is the same as the one you started from, it is the beginning of the module. If the module name that you back up to is different from the module you started with, go forward 8 bytes. You will then be at the beginning of the EP module.

After you record the module's name and offset on your abend recording form, determine the PTF maintenance level of this particular module. Locate the level as follows:

- For NCP, find the number preceded by the letters *UR* printed just before the module's name in the interpreted section of the NCP dump.
- For EP, find the number preceded by the letters *IR* at approximate offset X'0A' from the beginning of the module.

Record this number on your abend recording form.

Go to "Step 15. Report Problem."

Step 10. Use Contents of Level 3 Registers

Use the contents of the level 3 registers and of LAR to get the name, offset, and PTF of the failed module. If X'2000' is in register 1 for level 3, level 3 has issued an abend. You will need to find the contents of the level 3 registers.

Use the level 3 registers that appear in ABN. To find ABN, see the instructions in "Step 14. Get Registers for Interrupted Level."

Record the contents of LAR. To find LAR, see the instructions in "Step 7. What Level Was Interrupted By Level 1" If LAR points to an EP module, record the module's name, offset, and PTF maintenance level on your abend recording form (see "Step 12. Use Contents of LAR" for further instructions.)

Next, examine the save areas for level 3 to determine level 3 activity. The save areas are formatted near the beginning of the formatted NCP dump. If you have a formatted NCP dump, you can use "Formatted Dump Contents" on page 195 to locate the save areas.

You can also use the SSP CLIST IFWISAVE to display the save areas for level 3.

The format of the save areas is as follows:

Save area + X'00'	Pointer to the previous save area
Save area + X'04'	Pointer to the next save area
Save area + X'08'	Return address
Save area + X'0C'	Register 1
Save area + X'10'	Register 2
Save area + X'14'	Register 3
Save area + X'18'	Register 4
Save area + X'1C'	Register 5
Save area + X'20'	Register 7
Save area + X'24'	Register 6
Save area + X'28'	Pointer to the previous automatic storage area
Save area + X'2C'	Pointer to the next automatic storage area.

In a formatted dump, register 6 of level 3 points to the current save area or the next save area. In an unformatted dump, use register 6 to find the current save area and use the first fullword of the save area to find the pointer to the previous save area.

You can use the SSP CLISTs IFWISAVE to display the module name and offset and IFWIMOD to determine the maintenance level. Record this information on your abend recording form. Go to "Step 15. Report Problem."

Record the contents of the save-area registers pointed to by register 6 and all of the save areas before the target save area. The return address fields of all the save areas point to the module name and the offset into the module. Find the return address in the hexadecimal section of the unformatted dump. In the interpreted section of the dump, find the module name at the end of the module's object code.

The target module that contains the return address starts at the next fullword entry past the name of the module before the target module. To find the offset into the module, subtract the starting address of the module from the return address.

Record the module's name and offset on your abend recording form and determine the PTF maintenance levels of these particular modules. If PTF maintenance was applied to the module, locate the level as follows:

- For NCP, find the number preceded by the letters *UR* printed just before the module's name in the interpreted section of the NCP dump.
- For EP, find the number preceded by the letters *IR* at approximate offset X'0A' from the beginning of the module.

Record this number on your abend recording form.

Go to "Step 15. Report Problem."

Step 11. Use Contents of Level 2 registers

Use the contents of level 2 registers and LAR to obtain the name, offset, and PTF of the failed module. If X'2000' is in register 1 for level 2, and level 1 did not detect the abend, level 2 issued the abend. Level 2 rarely abends because this level controls character service for the communication lines. Register 2 for level 2 contains the address of the adapter control block (ACB) or CCB for EP. This information relates to the line being worked on at the time of the abend.

Record the contents of register 2 for level 2 and the contents of LAR, which is external register X'74'. LAR is printed at the top of each page of the formatted dump.

You can also use the SSP CLIST IFWIREGS to display register information online.

In a formatted dump, obtain the contents of register 2 for level 2 from ABN. If you have a formatted NCP dump, use "Formatted Dump Contents" on page 195 to locate ABN.

In unformatted dumps, use the following pointers to find register 2 and LAR:

- XDA pointer at X'6E8'
- **NCP V6R1 anlater**: XDA pointer at X'38' (IBM 3745)
- HWE pointer at XDA + X'58'
- ABN pointer at HWE + X'38'
- ABN + X'38'= Register 2 for level 2
- XDA + X'28'= LAR.

You can use the SSP CLIST IFWIWHER to display the module name, offset, and PTF maintenance level. Record this information on your abend recording form. Go to "Step 15. Report Problem."

LAR points either to the module name and the offset into that module in the hexadecimal section of the NCP dump or to the load map printed as part of the NCP formatted dump. In the hexadecimal section of the dump, the module name is at the end of the module. To find the beginning of the module, return to the previous module name and then go forward 8 bytes. You will then be at the beginning of the NCP load module.

If the module name starts with the letters *CY*, it is an EP module. EP module names are at both the beginning and the end of the module. To determine the beginning of the EP module, back up from the module name that you have found to the previous module name. If this previous module name is the same as the one you started from, that name is the beginning of the module. If the module name that you back up to is different from the module name you started with, go forward 8 bytes. You will be at the beginning of the EP module.

To use the load map, find the row containing a START and END column. The address is located between these columns, and the module name is at the beginning of the row.

To calculate the offset into the module, subtract the starting address of the module from LAR.

Record the module's name and offset on your abend recording form, determine the PTF maintenance level of this particular module. Locate the level as follows:

- For NCP, find the number preceded by the letters *UR* printed just before the module's name in the interpreted section of the NCP dump.
- For EP, find the number preceded by the letters *IR* at approximate offset X'0A' from the beginning of the module.

Record this number on your abend recording form.

Go to "Step 15. Report Problem."

Step 12. Use Contents of LAR

Use the contents of LAR to get the name, offset, and PTF of the failed module.

Level 1 has issued an abend. Because initialization code runs in level 1 only, this abend usually happens only during NCP initialization. Record the contents of LAR, which is external register X'74'. LAR appears at the top of each page of the formatted dump or can be displayed using the SSP CLIST IFWIREGS.

In unformatted dumps, find LAR by using the following pointers:

- XDA pointer at X'6E8'
- **NCP V6R1 and Later:** XDA pointer at X'38' (IBM 3745)
- XDA + X'28'= LAR.

LAR points either to the module name and the offset into that module in the hexadecimal section of the NCP dump or to the load map printed as part of the NCP formatted dump.

You can use the SSP CLIST IFWIWHER to display the module name, offset, and PTF maintenance level. Record this information on your abend recording form. Go to "Step 15. Report Problem."

In the hexadecimal section of the dump, the module name is at the end of the module. To find the beginning of the module, return to the previous module name and then go forward 8 bytes. You will then be at the beginning of the module.

To calculate the offset into the module, subtract the starting address of the module from LAR.

After you have recorded the module's name and offset on your abend recording form, determine the PTF maintenance level of this particular module. Locate the level as follows:

- For NCP, find the number preceded by the letters *UR* printed just before the module's name in the interpreted section of the NCP dump.
- For EP, find the number preceded by the letters *IR* at approximate offset X'0A' from the beginning of the module.

Record this number on your abend recording form.

Go to "Step 15. Report Problem."

Step 13. Use Contents of Level 1 IAR

Use the contents of the level 1 instruction address register (IAR) to find the name and offset of the failed module.

If you are at this step, it is because there is a level 1 program check. Use the register listing in your dump to find the contents of level 1's IAR (register 0). The register listing appears before the storage protect keys, which are just before the hexadecimal section of the NCP dump.

Subtract 2 bytes from the contents of this register. The resulting address points to the module name and the offset into that module. Use the hexadecimal section of the NCP dump or the load map printed as part of the NCP formatted dump.

You can use the SSP CLIST IFWIWHER to display the module name, offset, and PTF maintenance level. Record this information on your abend recording form. Go to "Step 15. Report Problem."

In the dump's hexadecimal section, the module name is at the end of the module. To find the beginning of the module, return to the previous module name and then go forward 8 bytes. You will then be at the beginning of the NCP module.

To use the load map, find the row containing a START column and an END column. The address is located between these columns, and the module name is at the beginning of the row.

To calculate the offset into the module, subtract the starting address of the module from the IAR.

After you have recorded the module's name and offset on your abend recording form, determine the PTF maintenance level of this particular module. Locate the level as follows:

- For NCP, find the number preceded by the letters *UR* printed just before the module's name in the interpreted section of the NCP dump.
- For EP, find the number preceded by the letters *IR* at approximate offset X'0A' from the beginning of the module.

Record this number on your abend recording form.

Go to "Step 15. Report Problem."

Step 14. Get Registers for Interrupted Level

Get the contents of the registers for the level that level 1 interrupted from the register listing in the NCP dump.

You can use the SSP CLIST IFWIREGS to display register information online.

Obtain these registers from the list of registers printed just before the storage protect keys. These storage protect keys appear just before the hexadecimal section of the NCP dump. You can find these registers in ABN. If you have a formatted NCP dump, you can use "Formatted Dump Contents" on page 195 to locate ABN. In an unformatted NCP dump, find ABN by using the following pointers:

- XDA pointer at X'6E8'
- **NCP V6R1 and Later:** XDA pointer at X'38' (IBM 3745)
- HWE pointer at XDA + X'58'
- HWE + X'38'= ABN pointer.

You can also use the SSP CLIST IFWIERP to display ABN.

The format of the register save areas in ABN is as follows:

ABN + X'10'	Level 1 registers
ABN + X'30'	Level 2 registers
ABN + X'50'	Level 3 registers
ABN + X'70'	Level 4 registers
ABN + X'90'	Level 5 registers.

A few registers in ABN contain different values from the general registers in the NCP dump. If an abend occurs, register 1 for the level that detected the abend will *not* contain X'2000' in ABN. The detecting level's register 1 in the general registers will contain X'2000'.

After obtaining the contents of the registers for the level that level 1 interrupted, go to "Step 15. Report Problem."

Step 15. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Abend Recording Form

Use the abend recording form shown on page 38 to document the problem. The numbers on this form correspond to step numbers used in "Diagnostic Procedure" on page 27 .

Abend Recording Form

1. There is nothing to record for Step 1.
2. Abend code = ____ , XDH ptr. = _____ , XDH + X'60' = _____
3. What is the RETAIN search string? _____
4. What caused the abend? _____
5. CCU check? YES ___ NO ___ CCU stopped? YES ___ NO ___

   L1B + X'04' = _____, L1B + X'08' = _____

   L1B + X'28' = _____
6. Description of the abend code:

7. L1B + X'00' = _____ , L1B + X'07' = _____

   L1B + X'0C' = _____ , L1B + X'10' = _____

   L1B + X'14' = _____ , L1B + X'52' = _____

   Module name _____ , Offset = _____ , Maint. = _____
8. XDA ptr. = _____ , XDA + X'58' = _____ , HWE + X'38' = _____

   level# __ Register 0 = _____ , Register 1 = _____
   Register 2 = _____ , Register 3 = _____
   Register 4 = _____ , Register 5 = _____
   Register 6 = _____ , Register 7 = _____

   ABN + X'__' Register 0 = _____ , Register 1 = _____
   Register 2 = _____ , Register 3 = _____
   Register 4 = _____ , Register 5 = _____
   Register 6 = _____ , Register 7 = _____
9. Level 5 Register 0 = _____ , Register 1 = _____
   Register 2 = _____ , Register 3 = _____
   Register 4 = _____ , Register 5 = _____
   Register 6 = _____ , Register 7 = _____

   Module name _____, Offset = _____, Maint. = _____, SVC _____
10. Level 3 Register 0 = _____ , Register 1 = _____
    Register 2 = _____ , Register 3 = _____
    Register 4 = _____ , Register 5 = _____
    Register 6 = _____ , Register 7 = _____

    LAR = _____ Module name _____, Offset = _____, Maint. = _____

Level 3 save areas:

Save area 1	Save area 2	Save area 3
SA + X'00' = _____	SA + X'00' = _____	SA + X'00' = _____
SA + X'04' = _____	SA + X'04' = _____	SA + X'04' = _____
SA + X'08' = _____	SA + X'08' = _____	SA + X'08' = _____
SA + X'0C' = _____	SA + X'0C' = _____	SA + X'0C' = _____
SA + X'10' = _____	SA + X'10' = _____	SA + X'10' = _____
SA + X'14' = _____	SA + X'14' = _____	SA + X'14' = _____
SA + X'18' = _____	SA + X'18' = _____	SA + X'18' = _____
SA + X'1C' = _____	SA + X'1C' = _____	SA + X'1C' = _____
SA + X'20' = _____	SA + X'20' = _____	SA + X'20' = _____
SA + X'24' = _____	SA + X'24' = _____	SA + X'24' = _____
SA + X'28' = _____	SA + X'28' = _____	SA + X'28' = _____
SA + X'2C' = _____	SA + X'2C' = _____	SA + X'2C' = _____

Save area 4	Save area 5	Save area 6
SA + X'00' = _____	SA + X'00' = _____	SA + X'00' = _____
SA + X'04' = _____	SA + X'04' = _____	SA + X'04' = _____
SA + X'08' = _____	SA + X'08' = _____	SA + X'08' = _____
SA + X'0C' = _____	SA + X'0C' = _____	SA + X'0C' = _____
SA + X'10' = _____	SA + X'10' = _____	SA + X'10' = _____
SA + X'14' = _____	SA + X'14' = _____	SA + X'14' = _____
SA + X'18' = _____	SA + X'18' = _____	SA + X'18' = _____
SA + X'1C' = _____	SA + X'1C' = _____	SA + X'1C' = _____
SA + X'20' = _____	SA + X'20' = _____	SA + X'20' = _____
SA + X'24' = _____	SA + X'24' = _____	SA + X'24' = _____
SA + X'28' = _____	SA + X'28' = _____	SA + X'28' = _____
SA + X'2C' = _____	SA + X'2C' = _____	SA + X'2C' = _____

- Area 1: Mod. name _____, Offset = _____, Maint. = _____
- Area 2: Mod. name _____, Offset = _____, Maint. = _____
- Area 3: Mod. name _____, Offset = _____, Maint. = _____
- Area 4: Mod. name _____, Offset = _____, Maint. = _____
- Area 5: Mod. name _____, Offset = _____, Maint. = _____
- Area 6: Mod. name _____, Offset = _____, Maint. = _____

11. XDA ptr. = _____ , XDA + X'58' = _____ , HWE + X'38' = _____

    (LAR) XDA + X'28' = _____ , (Register 2) ABN + X'38' = _____

    Mod. name _____, Offset = _____, Maint. = _____

12. XDA ptr. = _____ , (LAR) XDA + X'28' = _____

    Mod. name _____, Offset = _____, Maint. = _____

13. Level 1 IAR _____,

    Module name _____ , Offset = _____ , Maint. = _____

14. Date _____ , Name of IBM contact _____

Activate or Deactivate Error Procedure

An activate or deactivate failure occurs when a resource fails to respond or returns an exception response (negative response) to an activate or deactivate session request. The host system, the network control operator, or the user can originate the activate or deactivate request. The following symptoms indicate an activate or deactivate problem:

- Resource fails to respond.
- Resource returns an exception response.
- Route activation failure occurs.
- Session fails to come up.

For the activate or deactivate error diagnostic procedure, a resource can be any of the following:

- A remote NCP
- A line
- A physical unit
- A logical unit
- A cluster controller
- A terminal.

If the resource that causes the problem is a channel-attached NCP that you cannot activate, see "NCP Load and Initialize Error Procedure" on page 86.

Another type of activation failure is a route activation failure. If you try to bring up a session with cross-domain resource managers (CDRMs), NCPs, physical units, logical units, or binary synchronous communication (BSC) or start-stop resources before explicit routes and virtual routes are active, the session may fail to come up. These route activation failures are easily identified by the messages at the network operator's console.

Route activation failures are usually caused by incorrectly coded PATH definition statements in VTAM or NCP. Route failures may occur more often if you are using dynamic path update. Incorrectly coded PATH definition statements may also cause a transmission group activation failure between NCPs. Check the network operator's console for any messages or sense codes that mention route activation or transmission group activation failures.

Route activation failures may also result from an incorrectly coded ERLIMIT keyword on the BUILD definition statement or an SALIMIT keyword on the BUILD (for native networks) or NETWORK (for non-native networks) definition statement.

Documentation Checklist

If the problem results in an activate or deactivate failure, use the procedure in Figure 5 on page 42 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- The configuration report program (CRP) output listings from the latest NCP generation
- A path information unit (PIU) trace
- A VTAM buffer trace
- A VTAM I/O trace
- A line trace
- A SIT
- An NCP dump that also contains the channel adapter I/O halfword (IOH) trace
- An access method dump.

If the failing resource is a remote NCP, you also need the following information:

- A diagram showing the hardware configuration of the remote NCP
- A copy of the generation definition of the local NCP that communicates with the remote NCP
- A copy of the generation definition of the remote NCP.

Diagnostic Procedure

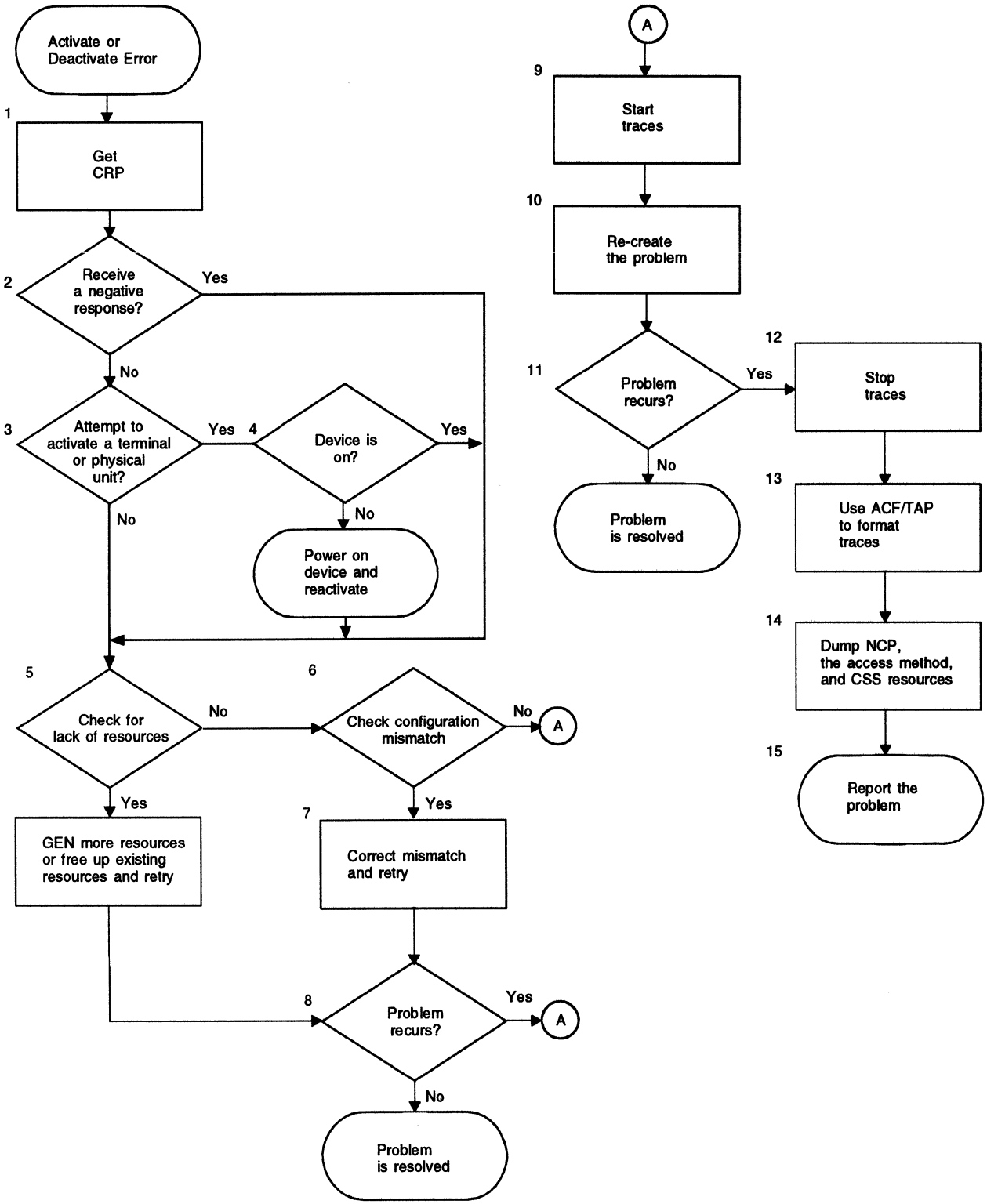


Figure 5. Overview of the Activate or Deactivate Error Diagnostic Procedure

Step 1. Get CRP

To complete the following procedure, obtain the CRP output listings produced when your system was generated. If you need more information on CRP listings, see Chapter 13.

Step 2. Check Response to the Activate or Deactivate

If you attempted to activate or deactivate the resource and received a negative response, go to "Step 5. Check for Lack of Resources" ; otherwise, go to "Step 3. A Terminal or Physical Unit Activated."

Step 3. A Terminal or Physical Unit Activated

If you activated a terminal or physical unit, go to "Step 4. Is Device On and Reactivate" ; otherwise, go to "Step 5. Check for Lack of Resources."

Step 4. Is Device On and Reactivate

Make sure the device is on. If it is on, go to "Step 5. Check for Lack of Resources" ; otherwise, power on the device and attempt to reactivate.

If it does not reactivate go to "Step 5. Check for Lack of Resources," otherwise, the problem has been resolved.

Step 5. Check for Lack of Resources

Look up the NCP exception response in *NCP, SSP, and EP Messages and Codes*.

- It could be a lack of resources. To determine if there is a lack of resources:
  - Check NetView for a generic alert related to NCP control blocks. Follow the actions described for the generic alert. For more information on control block pools, see the *NCP and EP Reference*.
  - Run NTuneMON to check control block pool usage for various pools to determine which pool was lacking.
  - Run NPM to collect control block information for the NCP.

  If it is a lack of resources, generate more resources or free up existing resources, and retry.
- If it is not a lack of resources, it could be a configuration mismatch. Go to "Step 6. Check for Configuration Mismatch."

Step 6. Check for Configuration Mismatch

See the *NCP and EP Reference Summary and Data Areas, Volume 2* for detailed alert information.

If the device is on and you receive no response, verify that your NCP generation definition for the device, shown in the CRP listings, matches the actual configuration of the device. Items that could be mismatched include:

- Line protocol
- Synchronous Data Link Control (SDLC) station address
- BSC polling/addressing sequence
- Terminal type
- Line defined as a spare line
- VTAM did not activate the line.

If there is a configuration mismatch, go to "Step 7. Correct Mismatch" ; otherwise, go to "Step 9. Start Traces."

Step 7. Correct Mismatch

Correct the configuration of the failing resource or amend the NCP definition statements to match the actual configuration of the device and regenerate NCP. Retry activating or deactivating the resource that failed.

If the same failure recurs, go to "Step 8. Problem Recurs" ; otherwise, the problem has been resolved.

NCP V5R3 (VSE): If you have received an exception response with sense code X'0801 0006' and you are using an IBM 3720 or 3745 Communication Controller, there may be a mismatch between the USGTIER keyword on the BUILD definition statement and the resources generated. See *NCP and EP Reference* or *NCP, SSP, and EP Resource Definition Guide* for more information on usage tier.

NCP V5R4 and NCP V6R1: Sense code X'0801 001E' indicates a usage tier exception for the IBM 3745. An equipment check on an EP line may indicate a usage tier exception on either the IBM 3720 or the IBM 3745.

NCP V7R2: Sense code X'0801 002A' indicates that the line is defined as a spare line. Spare lines cannot be activated. See the *NTune User's Guide* for more information.

VTAM fails to send an ACTLINK. A line might be defined as a spare line to VTAM. See the *NTune User's Guide* for more information.

Step 8. Problem Recurs

If the problem recurs, go to "Step 9. Start Traces" ; otherwise, the problem has been resolved.

Step 9. Start Traces

From the following list, select the traces applicable to your network and access method. For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook.*

- Generalized PIU trace (GPT): Run the trace for NCP that has the problem.
- VTAM buffer trace or TCAM PIU trace: Run trace for failing physical or logical unit. Start the trace from the specific node the physical unit or logical unit communicates with.
- VTAM I/O trace or TCAM channel I/O interrupt trace.
- Channel adapter IOH trace: If it is not already running.
- Connectivity subsystem line trace.
- NCP line trace.

  If you activate an NCP line trace against a line attached to NTRI, the data is returned from a NTRI line trace and an IOH trace, instead of from an NCP line trace.
- Scanner Interface Trace (SIT).

If you activate SIT against an address that has a token-ring interface coupler (TIC) installed at that address rather than a line scanner, the data is returned from a TIC internal trace instead of from SIT.

NCP V6R2 and Later: If you activate SIT for a line attached to a 3746 Model 900, the data is returned from a connectivity subsystem adapter trace.

Step 10. Re-create Problem

Attempt to re-create the problem.

Step 11. Check if Problem Recurs

If the problem recurs, go to "Step 12. Stop Traces" ; otherwise, the problem has been resolved.

Step 12. Stop Traces

When the failure recurs, stop the traces that are running. For information on stopping traces, see the references given in "Step 9. Start Traces" and choose the correct option for stopping each trace.

Step 13. Use ACF/TAP to Format Traces

Use ACF/TAP to format and interpret traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 14. Dump NCP, the Access Method, and CSS

Dump the following:

- The NCP that communicates with the failing resource. If the failing resource is a remote NCP, also dump that NCP. For information on dumping NCP, see the following:
  - For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
  - For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
  - For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."
- The access method that communicates between the host application program and the resource with the activation or deactivation problem. For information on dumping VTAM, see *VTAM Diagnosis*. For TCAM, see *TCAM Diagnosis Guide*.
- **NCP V6R2 and Later:** If the failing resource is a CSS[2] resource, use maintenance and operator subsystem extended (MOSS-E). You can also use a MOSS-E function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

---

2 The 3746 Model 900 connectivity subsystem (CSS) is also known as "37CS."

Step 15. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

IBM 3745 Selective Scanning Error Procedure

On the IBM 3745 Communication Controller, selective scanning (for low-speed scanning) scans only line interface couplers (LICs) with active lines. This selective scanning allows different configurations of active lines so long as the configuration does not exceed the recommended LIC weight. The following symptoms indicate an IBM 3745 selective scanning problem:

- Multiple lines are failing.
- Traffic is slow on all lines linked to the scanner.

If you experience selective scanning problems with an IBM 3745, follow the procedure in Figure 6 on page 47 before calling the IBM Support Center.

Diagnostic Procedure

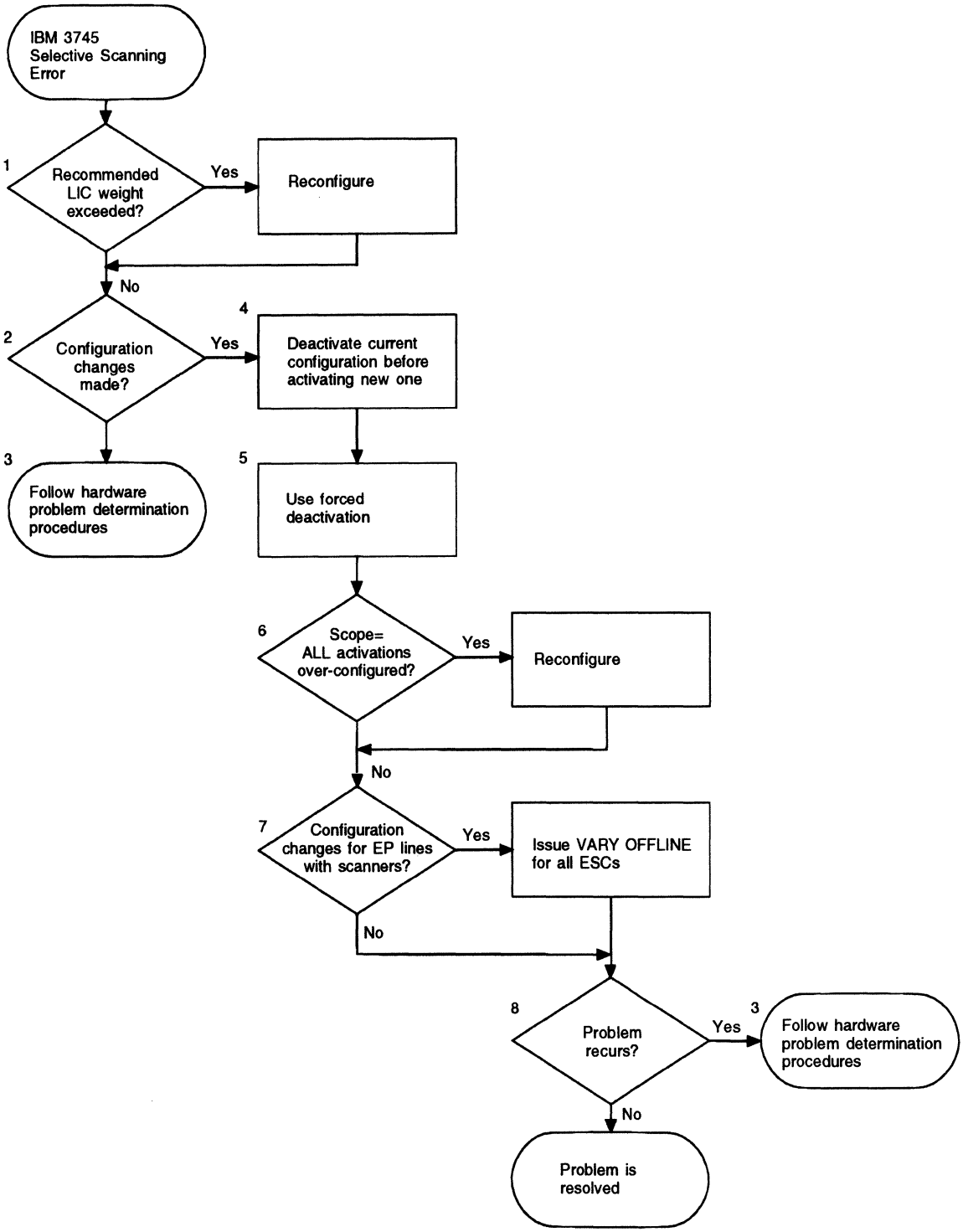


Figure 6. Overview of the IBM 3745 Communication Controller Selective Scanner Error Diagnostic Procedure

Step 1. Check the LIC Weight

Selective scanning (for low-speed scanners) allows only the LICs with active lines to be scanned. Different configurations of active lines are allowed as long as the given configuration does not exceed the recommended LIC weight.

If the configuration does exceed the recommended LIC weight, reconfigure the NCP generation definition. Otherwise, go to "Step 2. Check Configuration Changes."

Step 2. Check Configuration Changes

Check the scanners for configuration changes.

If configuration changes have been made, go to "Step 4. Deactivate Current Configuration" ;, otherwise, go to "Step 3. Follow Hardware Problem Determination Procedures."

Step 3. Follow Hardware Problem Determination Procedures

If problems still occur, follow normal hardware problem determination procedures for your scanner.

Step 4. Deactivate Current Configuration

Deactivate the current configuration before a new configuration is activated. Go to "Step 5. Use Forced Deactivation."

Step 5. Use Forced Deactivation

Use forced deactivation to ensure that any lines that had errors before the configuration change are brought down. Force deactivation even if the lines with errors may appear inactive to the host.

Failure to take the actions mentioned in "Step 4. Deactivate Current Configuration" and "Step 5. Use Forced Deactivation" can result in an insufficient scan rate for the lines. An insufficient scan rate can cause a variety of problems, such as link procedure failures (negative response to activate link) or the generation of box event records (BERs). Go to "Step 6. Check SCOPE=ALL Activations."

Step 6. Check SCOPE=ALL Activations

If SCOPE=ALL activations for scanners are over-configured, reconfigure your lines so that the scanners are no longer over-configured or do not activate the lines using SCOPE=ALL, otherwise, go to "Step 7. Check Configuration Changes with EP lines."

SCOPE=ALL activates all defined lines, which causes the LIC weight to be exceeded.

Step 7. Check Configuration Changes with EP lines

If any configuration changes have been made for scanners with EP lines attached, you must issue the VARY OFFLINE command for all emulation subchannels (ESCs) before you can issue any of the VARY ONLINE commands for the new configuration.

Go to "Step 8. Check if Problem Recurs."

Step 8. Check if Problem Recurs

If the problem recurs, go to "Step 3. Follow Hardware Problem Determination Procedures" ;, otherwise, the problem has been resolved.

Controller Alert Error Procedure

The host console receives communication controller alerts about hardware and software problems. If you have the NetView program installed in your system, these alerts appear on the NetView Alert Dynamic screen; however, if you do not have the NetView program, they appear as alarms on the MOSS console. For more information on capturing alerts flowing between NCP and VTAM without the NetView program, see the "Buffer Trace Capture of NMVTs" section in the *NCP, SSP, and EP Trace Analysis Handbook*

The following symptoms indicate a communication controller alert problem:

- Alarm is generated at the MOSS console.
- Alert is generated at host console (the NetView program).

See the *NCP and EP Reference Summary and Data Areas, Volume 2* for detailed alert information.

Documentation Checklist

If the problem results in a communication controller alert, use the procedure in Figure 7 on page 50 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- BER printout
- Communication scanner processor (CSP) dump.

Diagnostic Procedure

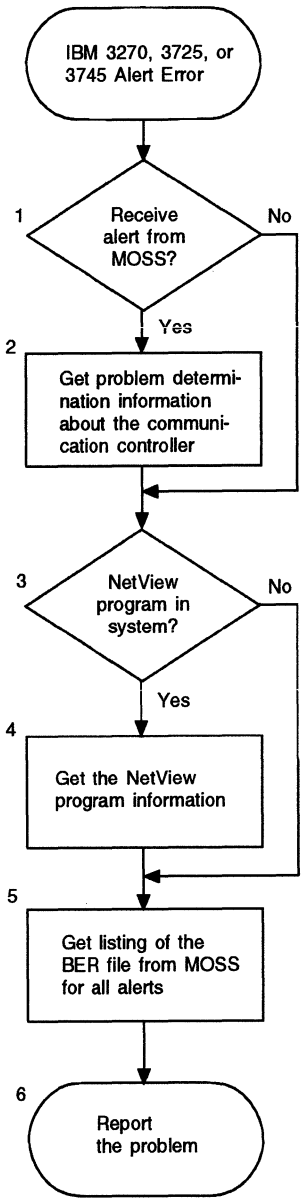


Figure 7. Overview of the Communication Controller Alert Error Diagnostic Procedure

Step 1. Does Information Appear on Your MOSS Console

Alerts report internal hardware and software events to the host access method. These alerts, except for MOSS UNAVAILABLE and CONSOLE UNAVAILABLE alerts, are related to communication controller alarms that the MOSS console reports. If an alarm is generated at your MOSS console, go to "Step 2. Get PD Information on Communication Controller" ; otherwise, go to "Step 3. Check if NetView Program is Installed."

Step 2. Get PD Information on Communication Controller

Find problem determination actions for these alarms in the operating guide or in the problem determination book for your communication controller.

Step 3. Check if NetView Program is Installed

If you have the NetView program installed on your system, go to "Step 4. Get NetView Program Information" ; otherwise, go to "Step 5. Need BER Listing for Alerts or Alarms."

Step 4. Get NetView Program Information

If you think the alert is related to NTRI, use the hardware monitor component of the NetView program to display informational screens about the alerts. For information on the network management vector transport (NMVT) data areas and alerts, see *Systems Network Architecture Formats.*

See the *NCP and EP Reference Summary and Data Areas, Volume 2* for detailed alert information.

Step 5. Need BER Listing for Alerts or Alarms

In addition to the information listed in the operating guide or problem determination book, gather a listing of the BER file from MOSS for all alerts or alarms, including those for the CSP.

Step 6. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Documentation Error Procedure

An NCP, SSP, or EP documentation problem is caused by incorrect, missing, or ambiguously stated information in an NCP, SSP, or EP book. The following symptoms indicate a documentation problem:

- Book contains wrong or ambiguous information.
- Book is missing information.
- Books contradict each other.
- NCP does not operate as described in a book.

Report a documentation error to your IBM Support Center representative only if it seriously interferes with program operation. For any other comments or suggestions on content, use the reader's comment form in the back of each book.

Documentation Checklist

If the problem results from a documentation error, use the procedure in Figure 8 on page 52 to diagnose the problem. During the diagnostic procedure, you may need to collect the following information:

- Publication that contains the error
- Location of the error in the publication
- Description of the problem that the error caused.

Diagnostic Procedure

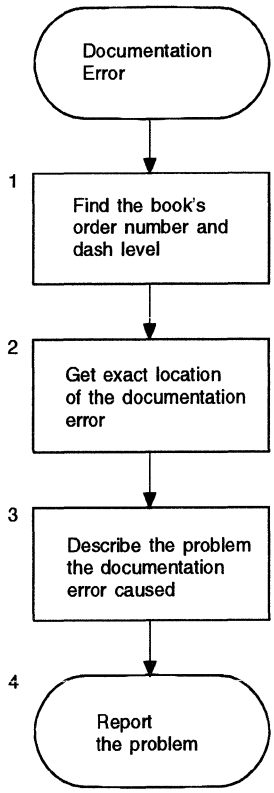


Figure 8. Overview of the Documentation Error Diagnostic Procedure

Step 1. What is Book's Order Number and dash level

Find the order number and dash level of the book that contains the documentation error. This information appears on the front cover and title page of a book in the following form:

```
xxxx-xxxx-nn
```

where xxxx-xxxx is the order number and nn is the dash level.

Step 2. Location of Error

The exact location of the error in the book is needed.

Step 3. Describe Problem the Documentation Error Caused

Located at the back of every IBM book is a reader's comments form. Use this form to describe any technical or editorial errors you found in the book, and return it to the IBM address listed on the back of the form (business reply postage is paid by IBM).

Step 4. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

NCP Generation Error Procedure

Generation problems occur during NCP generation using the NCP/EP definition facility (NDF), which is part of SSP. NDF runs in the host processor and provides error messages when problems are encountered. See Chapter 12 for a description of the NDF error messages and diagnostic facilities.

The following symptom indicates an NCP generation problem: Abnormal condition occurs during NCP generation.

Documentation Checklist

If your system experiences NCP generation problems, use the procedure in Figure 9 on page 54 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- Description of the operation you were performing
- Description of the results expected
- Description of the results received
- An input source listing
- NCP dump and abend information
- SYSLIST generation listing (VSE)
- NDF Summary Report (Print DD).

Diagnostic Procedure

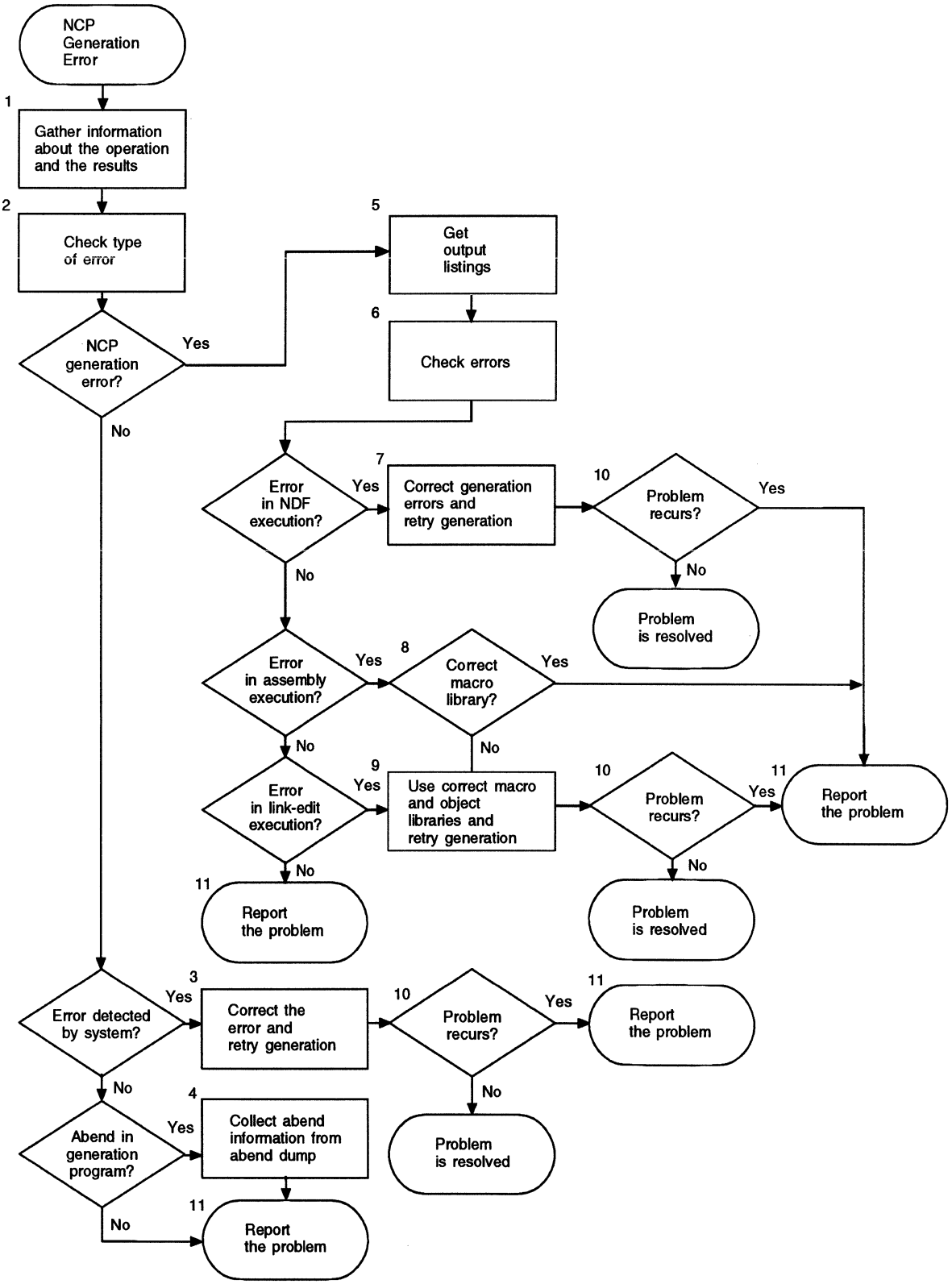


Figure 9. Overview of the NCP Generation Error Diagnostic Procedure

Step 1. Gather Information

Gather information on the operation you were performing, the results you expected, and the results you received.

You can get most of this information from your input source listing.

Step 2. Check Type of Error

1. If the problem is an NCP generation error, go to "Step 5. Get Output Listings" otherwise, continue.
2. If the error was detected by the system, go to "Step 3. Correct Error" ; otherwise, continue.
3. If the error is an abend in the generation program, go to "Step 4. Collect Abend Information From Abend Dump" ; otherwise, go to "Step 11. Report Problem."

Step 3. Correct Error

Correct the system error and retry the generation. Go to "Step 10. Check if Problem Recurs."

Step 4. Collect Abend Information From Abend Dump

The information you need to describe abend problems are:

- Program status word (PSW)
- Failing module and maintenance level of that module
- Failing instruction and offset of that instruction.

In addition to finding this information, you should check the following:

- The NDF output listing for any diagnostic messages issued by the NCP generation program
- The job-output-for-system messages that provide additional information.

Once you have collected the abend information, go to "Step 11. Report Problem."

Step 5. Get Output Listings

Get the following output listings:

- SYSLIST generation listing (VSE)
- NDF Summary Report (Print DD); in this report, find the listing for the failed step:
  - SYSPRINT for NDF
  - TBL1LIST for table 1 assembly
  - TBL2LIST for table 2 assembly
- MVS and VM link-edit listing.

Step 6. Check Errors

Use the output listing to determine where the error occurred.

1. If the error is in the NDF execution, go to "Step 7. Correct Generation Errors" otherwise, continue.

2. If the error is in the assembly execution, go to "Step 8. Check if Correct Macro Library is Used" ; otherwise, continue.
3. If the error is in the link-edit execution, go to "Step 9. Use Correct Macro and Object Libraries" ; otherwise, go to "Step 11. Report Problem."

Step 7. Correct Generation Errors

NCP generation step errors are normally straightforward and involve correcting conflicts in the generation input. For more information, see *NCP, SSP, and EP Messages and Codes*.

Go to "Step 10. Check if Problem Recurs."

Step 8. Check if Correct Macro Library is Used

Many assembly errors are caused by a mismatch between the version coded and the level of macros used. Ensure the version coded matches your library. Also, check the following:

- The MODEL, TYPGEN, and TYPSYS keywords on the BUILD definition statement. Incorrect coding of these keywords can cause assembly errors.
- Maintenance mismatches between NCP and SSP. Any mismatch can cause assembly errors. If you have the error message and the macro it is issued in, you can search the RETAIN database to help you identify the mismatch.

If the correct macro library is used, go to "Step 11. Report Problem" ; otherwise, go to "Step 9. Use Correct Macro and Object Libraries."

Step 9. Use Correct Macro and Object Libraries

Collect link-edit messages. Link-edit errors can occur because:

- The wrong object code libraries were used for link edit
- Mismatches have occurred in NCP and SSP maintenance. If you have the error message and the macro it was issued in, you can search the RETAIN database to help you identify the mismatch.

Correct the macro libraries specified and retry the generation.

Go to "Step 10. Check if Problem Recurs."

Step 10. Check if Problem Recurs

If the problem recurs, go to "Step 11. Report Problem" ; otherwise, the problem has been resolved.

Step 11. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Hung Session or Hung Resource Procedure

A hung session occurs when traffic between the application program and the terminal stops and does not resume. The following symptoms indicate a hung session or resource:

- Busy condition occurs at a user terminal.
- Pacing is withheld by NCP.
- Traffic between an application program and a terminal stops.
- Virtual routes on a transmission group are held.
- Virtual route pacing response does not occur.

A hung session is different from a hung resource. During a hung session, resources can be deactivated; whereas a hung resource does not respond to any command.

Apply the hung session or hung resource diagnostic procedure to any of the following resources:

- A line or a link
- A physical unit
- A logical unit
- A cluster controller
- A terminal.

The usual symptom of a hung session or resource is a complaint from a user who cannot get a response from a terminal or has a busy condition that has lasted abnormally long. Many times, you can alleviate a hung session or resource by issuing a DEACTIVATE, FORCE command to the line that contains the hung resource or session. This command forces VTAM and NCP to clean up all sessions using resources on this line. Usually, after the DEACTIVATE, FORCE completes its function, the devices on the line can be reactivated and sessions reestablished.

If the problem recurs after you issue the DEACTIVATE, FORCE command, or if you do not wish to issue DEACTIVATE, FORCE, use the following procedure to isolate the cause of your hung condition.

This diagnostic procedure provides you with some areas to investigate. If you still cannot resolve the problem, you will have at least eliminated many of the possible causes of the problem.

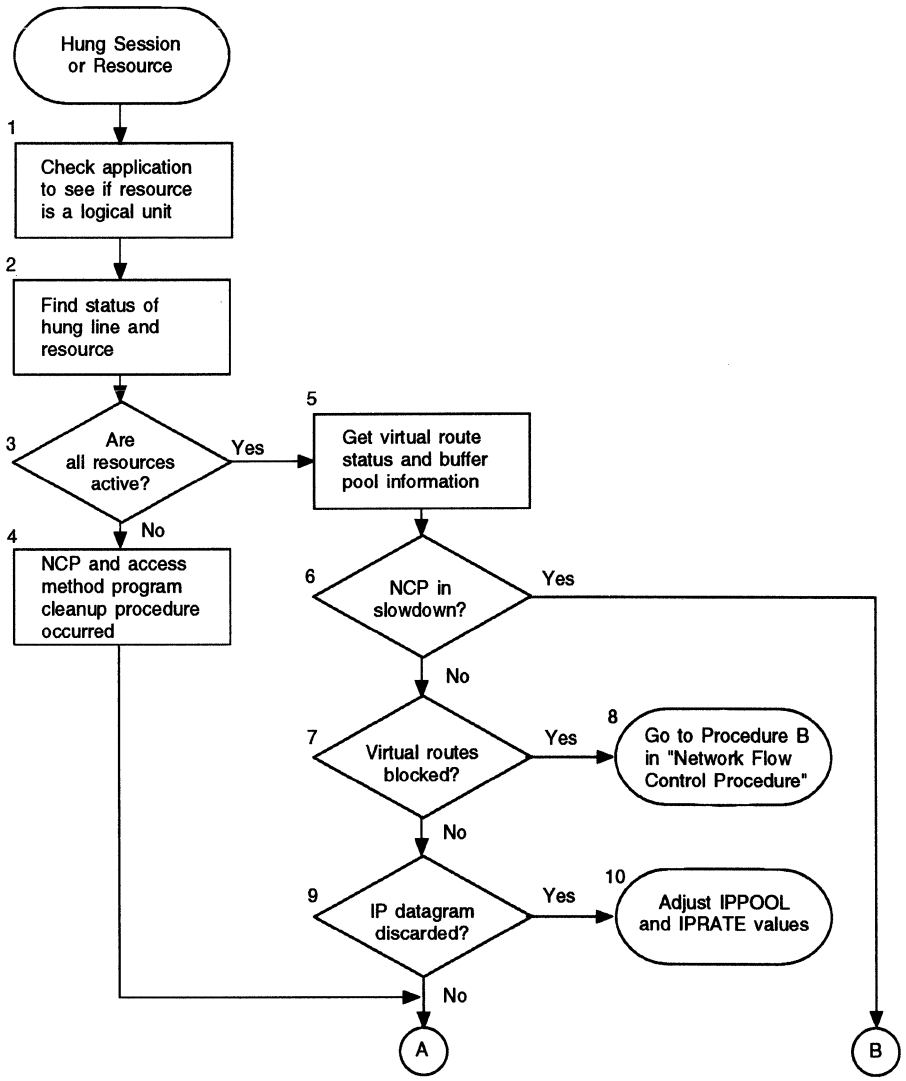
Documentation Checklist

If your system experiences a hung session or resource, use the procedure in Figure 10 on page 58 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- Access method trace
- Channel adapter IOH trace
- Channel control word (CCW) trace
- Connectivity subsystem line trace
- CRP reports
- GPT
- Line trace (level 2 and level 3) for EP

- NCP line trace
- PIU trace
- SIT
- Snap trace
- TIC internal trace
- VTAM buffer trace or TCAM PIU trace
- VTAM I/O trace or TCAM channel I/O interrupt trace.

Diagnostic Procedure



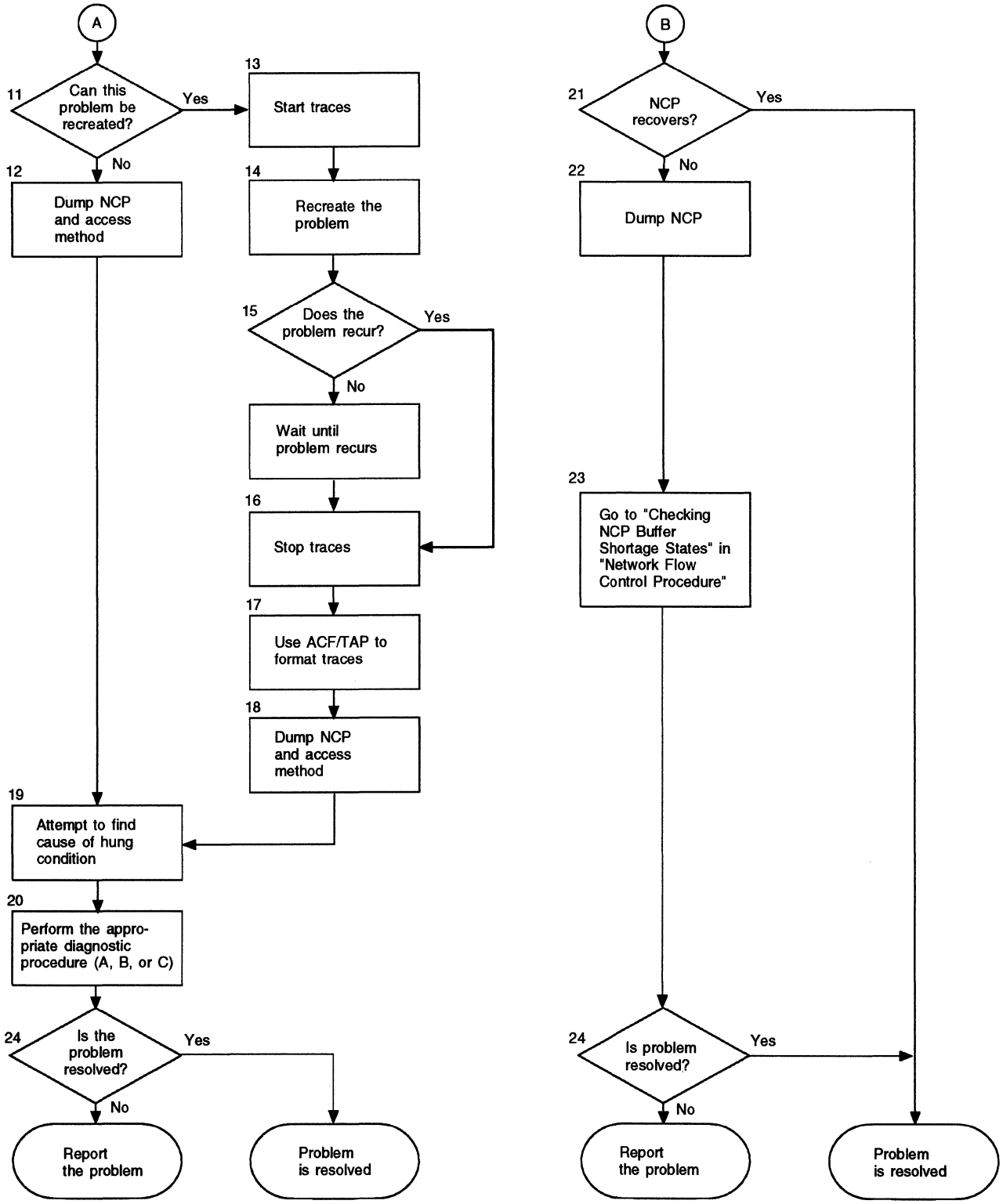


Figure 10 (Part 2 of 2). Overview of the Hung Session or Hung Resource Diagnostic Procedure

Step 1. Is Resource an LU

Use VTAM to display the status of the application.

Step 2. Find Status of Hung Line and Resources

Display the status of the hung line and devices. For information on displaying status, see *VTAM Operation.*

Step 3. Are Resources Active

If all the resources are active, go to "Step 5. Get VR Status and Buffer Pool Information" ; otherwise, go to "Step 4. Cleanup Procedure Occurred."

Step 4. Cleanup Procedure Occurred

The NCP and access method program cleanup procedure occurred. All the resources were active at one time, or the session could not have started. When a resource becomes inoperative, NCP and the access method initiate automatic cleanup procedures that take the session down. Because the session is hung, these procedures did not work.

Go to "Step 11. Can Problem be Re-created."

Step 5. Get VR Status and Buffer Pool Information

If the resources are active and the session is still hung, you may have a virtual route or buffer shortage problem. To determine this shortage, you need virtual route status and buffer pool information. To get this information, see "Obtaining Network Flow Control Information" on page 115; then go to "Step 6. Check if NCP is in Slowdown."

Step 6. Check if NCP is in Slowdown

If NCP is in slowdown, go to "Step 21. Check if NCP Recovers" ; otherwise, go to "Step 7. Are Virtual Routes Blocked."

Step 7. Are Virtual Routes Blocked

Directions for finding information on virtual routes can be found in "Obtaining Network Flow Control Information" on page 115.

1. Find the virtual routes for all sessions having problems.
2. Find the physical paths taken by these virtual routes. Answer each of the following questions:
   - Do all affected sessions reside within the same network?
   - Do all affected sessions use the same virtual route in any network?
   - Do all affected sessions traverse the same network?
   - Do all affected sessions use the same gateway NCP?
   - Do all affected sessions share the same virtual route end point?
   - Do all affected sessions use the same transmission priority?
3. Determine which sessions are hung.
4. Determine which sessions are experiencing slow response time.

See "Interpreting Blocked VR Alerts" on page 130 for an example of a blocked VR alert message received on NetView.

If virtual routes are blocked, go to "Step 8. See Procedure B in the " ; otherwise, go to "Step 9. Check if IP Datagrams are Discarded."

Step 8. See Procedure B in the

"Network Flow Control Error Procedure"

See "Procedure B: Hung Session and Resources for SNA (NCP V4R3.1, V5R3 (VSE), V5R4 and Later)" on page 68 for detailed instructions on diagnosing problems with virtual routes.

Step 9. Check if IP Datagrams are Discarded

This section applies to NCP V6R1 and later.

If an excessive number of IP datagrams is being lost, the problem could be that either:

- The Internet line is congested.
- IP datagrams are coming in faster than NCP allows.

To determine if NCP is causing IP datagrams to be lost, locate the Internet flow control information in NCP storage. For information on locating these control variables, see "Obtaining Network Flow Control Information" on page 115.

If IP datagrams are discarded, go to "Step 10. Adjust IPPOOL and IPRATE" ; otherwise, go to "Step 11. Can Problem be Re-created."

Step 10. Adjust IPPOOL and IPRATE

This section applies to NCP V6R1 and later.

The IPPOOL and IPRATE values in your NCP generation definition limit the IP datagram traffic arriving over the token-ring or Ethernet-type LAN. If NCP is discarding IP datagrams because the value coded for IPPOOL is being exceeded, increase the IPPOOL keyword value on the BUILD definition statement. Increasing this value allows more Internet Protocol traffic; however, be careful not to increase it too much since this could cause Internet Protocol traffic to monopolize the NCP buffer pool.

If NCP is discarding IP datagrams because the rate at which datagrams are being passed over the token-ring or Ethernet-type LAN is greater than the value specified for the IPRATE keyword on the BUILD definition statement, you can also increase this value. Again, be careful not to receive IP datagrams too quickly. You can omit the IPRATE keyword, but then NCP will depend only on the IPPOOL value when restricting Internet Protocol traffic.

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the IPPOOL and IPRATE keywords.

Step 11. Can Problem be Re-created

If the problem can be re-created, go to "Step 13. Start Traces" ; otherwise, go to "Step 12. Dump NCP and Access Method."

Step 12. Dump NCP and Access Method

Dump the following:

- The NCP that owns the failing resource. For information on how to do this, see the following:
  - For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
  - For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
  - For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

  NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.
- The access method that communicates between the host application program and the failing resource. For information on dumping VTAM, see *VTAM Diagnosis*. For TCAM, see *TCAM Diagnosis Guide*.

Go to "Step 19. Attempt to Find Cause of Hung Condition."

Step 13. Start Traces

From the following list, select the traces applicable to your network and access method: For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- Generalized PIU trace (GPT): Run the trace for NCP that has the problem.
- VTAM buffer trace or the TCAM PIU trace: Run trace for failing physical or logical unit. Start the trace from the specific node the physical unit or logical unit communicates with.

  To see the NMVT alerts generated by NCP, trace the SSCP-PU session. For more information on the blocked virtual route alert function, see *NCP and EP Reference*.

  See the *NCP and EP Reference Summary and Data Areas, Volume 2* for detailed alert information.
- VTAM I/O trace or TCAM channel I/O interrupt trace.
- Channel adapter IOH trace: If it is not already running.
- NCP line trace.

  If you activate an NCP line trace against a line attached to NTRI, the data is returned from a NTRI line trace and an IOH trace, instead of from an NCP line trace.
- EP line
- **NCP V6R2 and Later:** Connectivity subsystem line trace. For information on starting this trace, see the MOSS-E user guidance available online.

- Scanner interface trace (SIT): For the IBM 3720, 3725, or 3745 Communication Controllers.

  If you activate SIT against an address in an IBM 3720, 3725, or 3745 Communication Controller that has a TIC installed at that address rather than an IBM 3725 scanner, the data is returned from a TIC internal trace instead of from SIT.

- Transmission group trace

  Start this trace only if the NCP that owns the devices is not channel-attached to the application host and if you suspect that session data may not be crossing the subarea links between the NCPs.

- Snap trace, see "NTRI Snap Trace" on page 162.

Step 14. Re-create Problem

Attempt to re-create the problem.

Step 15. Does the Problem Recur

If problem recurs, go to "Step 16. Stop Traces" ; otherwise, wait until problem recurs, and then go to "Step 16. Stop Traces."

Step 16. Stop Traces

When the failure recurs, stop the traces that are running. For information on stopping traces, see the references given in "Step 13. Start Traces" and choose the correct option to stop each trace.

Step 17. Use ACF/TAP to Format Traces

Use ACF/TAP to format and interpret traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using the ACF/TAP program, see the *NCP, SSP, and EP Trace Analysis Handbook*. The channel adapter IOH trace prints in the NCP dump.

Step 18. Dump NCP and Access Method

Dump the following:

- The NCP that owns the failing resource. For information on how to do this, see the following:
  - For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
  - For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
  - For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

  NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

- The access method that communicates between the host application program and the failing resource. For information on dumping VTAM, see *VTAM Diagnosis*. For TCAM, see *TCAM Diagnosis Guide*.

Step 19. Attempt to Find Cause of Hung Condition

If you have the NetView program installed in your system, use NetView to find the virtual route that is supporting the failing session.

You can also look at the NCP dump to find the probable cause of your hung condition. Determine whether the cause is a BSC or a start-stop line, cluster, or terminal. For system network architecture (SNA), the resource may be an SDLC link, physical unit, or logical unit. To determine this cause, look at your NCP generation definition or the output of the CRP.

Obtain the element or network address from the reports printed by the CRP. The device page report lists the name of the device and either its element address or its network address. See Chapter 13 for information on CRP reports. If you cannot find copies of these CRP reports, obtain the network or element address of the failing resource from VTAM's resource definition table (RDT) control blocks.

Use a formatted dump of VTAM to find the resource definition table entry (RDTE) control blocks. The first 8 bytes of RDTE contain the resource name. The element address of the resource is at offset X'16' in RDTE. See *VTAM Diagnosis* for instructions about dumping VTAM. For information on RDT, see *VTAM Data Areas*. The network, subarea, and element addresses are located in the RPRE data area (part of RDT).

To verify the bit settings of the status bytes, use *NCP and EP Reference Summary and Data Areas, Volume 1*, to check control block fields. This is especially helpful when the procedure does not tell you what to look for in a byte. Each step in the procedure includes directions for finding the NCP required control blocks.

Go to "Step 20. Perform Diagnostic Procedure."

Step 20. Perform Diagnostic Procedure

Choose the correct diagnostic procedure from the following list:

- **NCP V4R1 (VSE) and NCP V4R2:** If the hung resource is an SNA resource (SDLC line, physical unit, or logical unit), use "Procedure A: Hung Session and Resources for SNA (NCP V4R1(VSE), NCP V4R2)" on page 65.
- **NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later** If the hung resource is an SNA resource (SDLC line, physical unit, logical unit, or scanner), use "Procedure B: Hung Session and Resources for SNA (NCP V4R3.1, V5R3 (VSE), V5R4 and Later)" on page 68.
- If the hung resource is a BSC or start-stop resource (line, cluster, or terminal), use "Procedure C: Hung Session and Resources for BSC or Start-Stop Line Control" on page 71.

To find all the notes cited in Procedures A, B, and C, see "Notes for Procedures A, B, and C" on page 74.

Go to "Step 24. Has Problem Resolved."

Step 21. Check if NCP Recovers

When NCP is in slowdown, you may want to wait to see if NCP recovers on its own. If NCP recovers, the problem has been resolved; otherwise, go to "Step 22. Dump NCP."

Step 22. Dump NCP

Since NCP did not recover, dump the NCP that owns the failing resource. For information on how to do this, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 23. Check for Buffer Shortage State

See "Checking NCP Buffer Shortage States" on page 139 under the heading "Obtaining Network Flow Control Information" for instructions on obtaining buffer shortage state information. You may then be able to modify your NCP generation definition to alleviate the problem. See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on using NCP buffer management keywords.

Go to "Step 24. Has Problem Resolved."

Step 24. Has Problem Resolved

If the problem cannot be resolved, collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center. Otherwise, the problem has been resolved.

Procedure A: Hung Session and Resources for SNA (NCP V4R1(VSE), NCP V4R2)

The following list directs you to the proper step:

- If your hung device is a logical unit, go to "Step 1."
- If your hung device is a physical unit, go to "Step 2."
- If your hung device is a line, go to "Step 3."
- If your hung device is a scanner, go to "Step 4."

Step 1: Do other logical units connected to the same physical unit as the failing logical unit work?

YES	NO
Check other possible problems: • Task is not in ready state. (LUB + X'0C' or X'28' contains B'...1 ....') • BATCH=YES specified on the LU definition statement (LUB + X'10' or X'2C' contains B'000. ....') • Awaiting pacing response from logical unit. (LUB + X'48' contains B'.... 1...') • Pending ACTLU/DEACTLU/BIND/UNBIND. (See Note 4 on page 74.) • Virtual route congested. (See Note 1 on page 74.)	Go to "Step 2."

Find a logical unit control block (LUB) with the network address (printed in hexadecimal beside it) that matches the network address of the failing logical unit. This LUB is in the formatted section of the NCP dump. The code that follows this LUB is the contents of the control block. The offsets in the chart are in hexadecimal and are determined from the beginning of the control block.

To find the virtual route control block (VRB) for a logical unit, look in the resource connection block (RCB) for the virtual route vector table (VVT) index. Find the RCB formatted after the LUB. The VVT index is at RCB + X'16'. Use this number to index the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

The physical unit control block for your logical unit is a common physical unit block (CUB), and it is formatted before the LUB. You will need this information if you go to "Step 2"

Step 2: Do other physical units on the link work?

YES	NO
Check other possible problems: • Pending contact or discontact, ACTPU or DEACTPU. (See Note 3 on page 74.) • Not responding or sending bad data. RETRIES, TEXTTO or REPLYTO set high. (See Note 2 on page 74 and Note 7 on page 75.) • Responding with receive-not-ready (RNR). (See Note 3 on page 74.) • Virtual route congested. (See Note 1 on page 74.)	Go to "Step 3."

Find a CUB with the network address (printed in hexadecimal beside it) that matches the network address of the failing physical unit. This CUB is in the formatted section of the NCP dump. The code that follows this CUB is the control

block contents. The offsets in the chart are in hexadecimal and are determined from the beginning of the control block.

To find the VRB for a physical unit, look in the RCB for the VVT index. Find the RCB formatted after the CUB. The VVT index is at RCB + X'16'. Use this number to index the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

Two control blocks relating to the line precede the CUB: the line group table (LGT) and ACB.

Step 3: Do other links on the scanner work or do the same types of resources work?

YES	NO
Check other possible problems: • Virtual route congested. (See Note 1 on page 74.) • RETRIES, TEXTTO/REPLYTO set too high or none specified. (See Note 2 on page 74 and Note 7 on page 75.) • Line status (ACB + X'04' or X'38' or X'3A').	Go to "Step 4."

Find a link control block (LKB) with the network address (printed in hexadecimal beside it) that matches the network address of the failing link. This is in the formatted section of the NCP dump. The code that follows this LKB is the control block contents. The offsets given in the chart are in hexadecimal and are determined from the beginning of the control block.

No particular VRB is associated with the line because lines do not have sessions. To check for virtual route congestion, find the VRBs for the logical units on this line.

To find the VRB for a logical unit, look in the RCB for the VVT index. Find the RCB that is formatted after the LUB. The VVT index is at RCB + X'16'. Use this number to index the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

Two control blocks relating to the line follow LKB: LGT and ACB.

Step 4: Do other scanners on the communication controller work? If only one scanner is attached, the problem may be listed in either column.

YES	NO
Check other possible problems: • Scanner disabled: (IBM 3725 and 3720) L1B + X'74'= pointer to AST. AST + X'10' is nonzero. • (IBM 3725 and 3720) BER type 11XX. • Generation errors (check the generation output for error messages)	Branch as follows: • NCP abended. See "NCP or EP Abend Procedure" on page 25. • NCP is in slowdown. See "Network Flow Control Error Procedure" on page 115. • NCP is in a loop. See "NCP or EP Loop Error Procedure" on page 91. • NCP has gone through auto network shutdown (ANS). Contact your network operator about your network's status.

For information on BER codes, see *Operator's Guide* or *Problem Determination and Extended Services* for your controller.

If you have not resolved the problem, you should now have enough documentation and information on the problem to call the IBM Support Center.

Procedure B: Hung Session and Resources for SNA (NCP V4R3.1, V5R3 (VSE), V5R4 and Later)

The following list directs you to the proper step:

- If your hung device is a logical unit, go to "Step 1."
- If your hung device is a physical unit, go to "Step 2."
- If your hung device is a line, go to "Step 3."
- If your hung device is a scanner, go to "Step 4."

Step 1: Do other logical units connected to the same physical unit as the failing logical unit work?

YES	NO
Check other possible problems: • Task is not in ready state. (BSB + X'0C' contains B'...1 ....') • REX is in batch mode. (BXI + X'3D' contains B'.... 1...') • REX held for REX transmit pace. (BXI + X'3C' contains B'.1.. ....') • Pending ACTLU or DEACTLU, BIND or UNBIND. (See Note 4 on page 74.) • Virtual route congested. (See Note 1 on page 74.)	Go to "Step 2."

If you are using SSP CLISTs, use IFWINAU to display the control blocks. Enter the network address for a logical unit to display the control blocks for Steps 1, 2, and 3.

Find a logical unit address control block (LRB) with the network address (printed in hexadecimal beside it) that matches the network address of the failing logical unit. This is in the formatted section of the NCP dump. Following this LRB are several other formatted control blocks. Among these control blocks are a boundary session block (BSB) and a boundary session block extension (BXI) control block for each session in which this logical unit is involved. To find the correct BSB and BXIs, look in each BXI for the name of this logical unit's session partner. The code that follows the BSB and BXI is the control block contents. The offsets in the chart are in hexadecimal and are determined from the beginning of the control block.

To find the VRB for the logical unit, look in RCB for the VVT index. The RCB is formatted above the BXI. The VVT index is at RCB + X'18'. Use this number to index the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

The physical unit control block for your logical unit is a CUB, and it is formatted before the LUB. You will need this information in "Step 2."

Step 2: Do other physical units on the link work

YES	NO
Check other possible problems: • Pending contact or discontact, ACTPU or DEACTPU. (See Note 3 on page 74.) • Not responding or sending bad data RETRIES, TEXTTO or REPLYTO set high. (See Note 2 on page 74 and Note 7 on page 75.) • Responding with RNR. (See Note 3 on page 74.) • Virtual route congested. (See Note 1 on page 74.)	Go to "Step 3."

If you are using SSP CLISTs, use IFWINAU to display the control blocks. Enter the network address for a physical unit to display the control blocks for "Step 2" and "Step 3."

Find a CUB with the network address (printed in hexadecimal beside it) that matches the network address of the failing physical unit. This CUB is in the formatted section of the NCP dump. The code that follows this CUB is the control block contents. The offsets in the chart are in hexadecimal and are determined from the beginning of the control block.

To find the VRB for the physical unit, look in the RCB for the VVT index. Find the RCB that is formatted a few control blocks past the CUB. The VVT index is at RCB + X'18'. Use this number to index into the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

Two control blocks relating to the line precede CUB: LGT and ACB.

Step 3: Do other links on the scanner work or do the same types of resources work?

YES	NO
Check other possible problems: • Virtual route congested. (See Note 1 on page 74.) • RETRIES, TEXTTO or REPLYTO set too high or none specified. (See Note 2 on page 74 and Note 7 on page 75.) • Line status (ACB + X'04' or X'38' or X'3A').	Go to "Step 4."

If you are using SSP CLISTs, use IFWINAU to display the control blocks. Enter the network address for a link to display the control blocks for "Step 3."

Find an LKB with the network address (printed in hexadecimal beside it) that matches the network address of the failing link in the formatted section of the NCP dump. The code that follows this LKB is the control block contents. The offsets given in the chart are in hexadecimal and are determined from the beginning of the control block.

No particular VRB is associated with a line because lines do not have sessions. To check for virtual route congestion, find the VRB for one of the logical units on this line.

To find the VRB for a logical unit, look in the RCB for the VVT index. Find the RCB by searching the LUBs following this LKB for the name of the logical unit. Following this LUB are BXIs. Find the BXI that contains the name of the session partner of this logical unit. The control block above that BXI is the RCB. The VVT index is at RCB + X'18'. Use this number to index into the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

Two control blocks relating to the line follow LKB: LGT and ACB.

Step 4: Do other scanners on the communication controller work? If only one scanner is attached, the problem may be listed in either column.

YES	NO
Check other possible problems: • Scanner disabled;[1] (3725 and 3720) L1B + X'74'= pointer to AST. AST + X'10' is nonzero. (IBM 3745) XDA + X'40'= pointer to L1B. L1B + X'70'= pointer to L1X. L1X + X'00'= pointer to AIT. AIT + X'10' is nonzero. • BER type 11XX.[2] • Generation errors (check the generation output for error messages).	Branch as follows: • NCP abended. See "NCP or EP Abend Procedure" on page 25. • NCP is in slowdown. See "Network Flow Control Error Procedure" on page 115. • NCP is in a loop. See "NCP or EP Loop Error Procedure" on page 91. • NCP has gone through ANS. Contact your network operator about your network's status.

[1] You can use SSP CLISTs IFWICA and IFWIERP to display relevant control block information.

[2] For information on BER codes, see *Operator's Guide* or *Problem Determination and Extended Services* for your controller.

If you have not resolved the problem, you should now have enough documentation and information on the problem to call the IBM Support Center.

Procedure C: Hung Session and Resources for BSC or Start-Stop Line Control

The following list directs you to the proper step:

- If your hung device is a terminal, go to "Step 1."
- If your hung device is a cluster, go to "Step 2."
- If your hung device is a line, go to "Step 3."

Step 1: Do other terminals on the cluster controller work?

YES	NO
Check other possible problems: • Device error lock set. (See Note 5 on page 75.) • Not in session. (See Note 5 on page 75.) • Print in progress—printer only. (See Note 5 on page 75.) • Task is not in ready state. (DVB + X'1C' contains B'...1 ....') • No command pending—contact. (See Note 5 on page 75.) • Virtual route congested. (See Note 1 on page 74.)	Go to "Step 2."

If you are using SSP CLISTs, use IFWINAU to display the control blocks. Enter the network address for a terminal to display the control blocks for "Step 1," "Step 2," and "Step 3."

Find a device base control block (DVB) with the network address (printed in hexadecimal beside it) that matches the network address of the failing terminal. This DVB is in the formatted section of the NCP dump. The code that follows this DVB is the control block contents. The offsets in the chart are in hexadecimal and are determined from the beginning of the control block.

To find the VRB for the terminal, look in the RCB for the VVT index. Find the RCB formatted after the DVB. For NCP V4R1 (VSE) and NCP V4R2, the VVT index is located at RCB + X'16'. For NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later, it is located at RCB + X'18'. Use this number to index the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

The cluster control block (CCB) for your terminal is also a DVB. To find the DVB for the cluster, return to RDTE. Look up the cluster name to get the network address of the cluster. (Information about RDTE can be found in Step 19 on page 64.) The cluster's DVB is formatted before the terminal's DVB. You will need this information in "Step 2."

Step 2: Do other cluster controllers on the line work?

YES	NO
Check other possible problems: • No command pending (invite). (See Note 5 on page 75.) • Error lock set. (See Note 5 on page 75.) • Task is not in ready state. (DVB + X'1C' contains B'...1 ....') • Virtual route congested. (See Note 1 on page 74.)	Go to "Step 3."

If you are using SSP CLISTs, use IFWINAU to display the control blocks. Enter the network address for a cluster to display the control blocks for "Step 2" and "Step 3."

Find a DVB with the network address (printed in hexadecimal beside it) that matches the network address of the failing cluster. This DVB is in the formatted section of the NCP dump. The code that follows this DVB is the control block contents. The offsets in the chart are in hexadecimal and are determined from the beginning of the control block.

To find the VRB for the cluster, look in the RCB for the VVT index. Find the RCB formatted after the DVB. For NCP V4R1 (VSE) and NCP V4R2, the VVT index is located at RCB + X'16'. For NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later, it is located at RCB + X'18'. Use this number to index the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

The line control block associated with the cluster is LCB, and it is formatted before the cluster's DVB. You will need this information in "Step 3" on page 73.

Step 3: Do other lines on the scanner work?

YES	NO
Check other possible problems: • Transmit limit set high (See Note 6 on page 75.) • Virtual route congested (See Note 1 on page 74.) • Session limit set too high. (See Note 6 on page 75.) • Line status. (ACB + X'04'or X'38'or X'3A') • RETRIES, TEXTO or REPLYTO set too high or none specified. (See Note 7 on page 75 and Note 8 on page 75.) • Work scheduler idle. (LCB + X'3C' contains B'...1 ....').	Go to Procedure A, "Step 4" on page 68, for SNA.

If you are using SSP CLISTs, use IFWINAU to display the control blocks. Enter the network address for a line to display the control blocks for "Step 3."

Find an LCB with the network address (printed in hexadecimal beside it) that matches the network address of the failing line. This LCB is in the formatted section of the NCP dump. The code that follows this LCB is the control block contents. The offsets given in the chart are in hexadecimal and are determined from the beginning of the control block.

No particular VRB is associated with a line because lines do not have sessions. To check for virtual route congestion, find the VRB for one of the terminals on this line.

To find the VRB for the terminal, look in the RCB for the VVT index. Find the RCB formatted after the DVB. For NCP V4R1 (VSE) and NCP V4R2, the VVT index is located at RCB + X'16'. For NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later, it is located at RCB + X'18'. Use this number to index into the VVT formatted near the end of the formatted section of the dump. The indexed field should contain the address of the VRB that matches one of the VRBs formatted after the VVT.

Two control blocks relating to the line follow LCB: LGT and ACB.

If you have not resolved the problem, you should now have enough information to call the IBM Support Center.

Notes for Procedures A, B, and C

Note 1 VRB + X'14': Hold state (the host owes NCP a virtual route pacing response):

- The pacing response is withheld because the virtual route threshold has been reached.
- The system is out of buffers.

VRB + X'54': Virtual route threshold limit

VRB + X'56': Virtual route threshold count

VRB + X'16': Buffers allocated from the BPOOL keyword for this virtual route

VRB + X'1A': PIUs on the virtual route transmit queue for this virtual route

V-pacing specified in VTAM too high for the application or not specified

Note 2 ACB + X'4E': Retry limit (set by RETRIES=*m*)

CUB + X'40': Second-level retries (set by RETRIES=(,,*n*))

CUB + X'45': Second-level ERP time delay (set by RETRIES=(,*t*,))

Error recovery time RETRIES=(*m*,*t*,*n*) is equal to:
$m \times (\text{REPLYTO} + \text{TEXTTO} + t) \times n$

Note 3 CUB + X'2E': Service-seeking and contact poll commands (2 bytes)

CUB + X'31': RNR received (device has a problem)

CUB + X'68': ACTPU/DEACTPU pending (device not responding or response lost)

CUB + X'74': ACTPU/DEACTPU pending (**NCP V4R2:** Device not responding or response lost)

CUB + X'75': ACTPU/DEACTPU pending (**NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later:** Device not responding or response lost)

Note 4 **NCP V4R1 (VSE) and NCP V4R2**:

LUB + X'3E': Processing ACTLU/DEACTLU (device not responding or response lost)

LUB + X'40': Processing BIND/UNBIND (device not responding or response lost)

LUB + X'48': Awaiting pacing from device (device not responding or response lost)

NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later:

BSB + X'28': Processing ACTLU/DEACTLU (device not responding or response lost for an system services control point (SSCP)-LU BSB)

BSB + X'28': Processing BIND/UNBIND (device not responding or response lost for an LU-LU BSB)

BXI + X'3C': Awaiting pacing from device (device not responding or response lost)

Note 5 DVB + X'50': In session (DVBSTAT contains B'.... 1...'

DVB + X'4B': Print in progress (DVBSTAT2 contains B'..1. ....')

(Printer is printing or hardware error)

Note 6 DVB + X'5C': Transmission or block limit generated (number of blocks NCP sends or receives from device before suspending the session)

LCB + X'76': Sessions allowed (should be equal to or greater than the number of devices on line)

The number of devices are at LCB + X'7A' or LCB + X'72'

Note 7 LGT + X'08': REPLYTO=*parm* on the GROUP definition statement (the time NCP waits in response to poll/text). Use the time value select table (TVS) control block to determine the amount of time.

LGT + X'09': TEXTTO=*parm* on the GROUP definition statement (the time NCP waits between text characters before retrying)

Note 8 ACB + X'4E': Retry limit (set by RETRIES=*m*)

LCB + X'4E': Second-level retries (set by RETRIES=(,,*n*))

LCB + X'50': Second-level ERP time delay (set by RETRIES=(,*t*,))

Error recovery time RETRIES=(*m*,*t*,*n*) is equal to:
m × (REPLYTO + *t*) × *n*.

Link Problem Determination Aid Error Procedure

Link problem determination aid (LPDA) tests are broadly classified into two groups, solicited (performed by the host) and unsolicited (performed by NCP). The following symptoms indicate an LPDA problem:

- Invalid response to an LPDA test occurs.
- LPDA unsolicited test error occurs.
- Negative response to an LPDA test occurs.
- No response to an LPDA test.

For solicited LPDA tests, the host operator requests tests for 386x and 586x modems using the NetView program. For solicited LPDA-1, the host sends a request for maintenance statistics (REQMS) from NCP. If NCP can accept the request, NCP responds positively to the REQMS. NCP then requests the modem to run the test. NCP packages and returns the test results in a record formatted maintenance statistics (RECFMS) PIU.

For unsolicited LPDA tests, NCP performs a test whenever NCP builds a RECMS PIU on a line that supports LPDA. NCP builds a RECMS to record line or station errors or to indicate a station counter overflow.

The basic concept for LPDA-2 is the same as for LPDA-1 except that NMVT PIUs are used instead of the REQMS/RECFMS mechanism. When the host operator request a solicited or NCP requests a unsolicited LPDA-2 test for the first segment of an LPDA data multiplex mode (DMPX) non-port-A line, the LPDA test is issued on the line connected to port A of the same modem.

NCP V5R4 and later:

1. You can code LPDATS=LPDA2 for a line and run LPDA-2 tests for the primary (MODE=PRI) or secondary (MODE=SEC) side of a subarea link. However, multiple errors may result if you initiate an LPDA-2 test from both sides of a subarea link at the same time. You can prevent these errors by coding LPDATS=LPDA-2 on either the primary or the secondary side of a subarea link, but not on both sides at the same time. NCP does not test for this error condition.
2. When you run LPDA-2 tests from the secondary side, first issue a SET LINK ATTRIBUTES command to the primary side of the link to stop its tests (if they are currently permitted); then issue a SET LINK ATTRIBUTES command to the secondary side of the subarea link to allow the tests.
3. To originate LPDA-2 tests from either the primary or secondary side of a link, you must configure the modem that is local to that side as primary.

Because NTRI lines are physically attached to communication controllers, the following traces are not supported for LPDA:

- NTRI line trace
- IOH trace
- TIC internal trace.

For more information on LPDA, see *NetView Problem Determination and Diagnosis*.

The following sections list symptoms and responses for both the solicited and unsolicited test failures.

Documentation Checklist

If the problem results in an LPDA solicited test error, use the procedure shown in Figure 11 on page 78. If the problem results in an LPDA unsolicited test error, use the procedure shown in Figure 12 on page 82. In either case, you may need to collect the following documentation:

- Access method dump
- NCP line trace
- NCP dump
- SIT
- VTAM buffer trace.

LPDA Solicited Test Error Diagnostic Procedure

There are three types of responses you can receive from an LPDA request:

- No response to the test request.

  This occurs when the NetView program's hardware monitor receives neither a positive nor a negative response to its test request. The problem appears as a hung NetView program console. If you do not receive a response to the test request, start at "Step 1. Start VTAM Buffer Trace" on page 79 to guide you through the LPDA solicited test error diagnostic procedure.

- Negative response to the test request.

  The NetView program's hardware monitor presents the negative response and its meaning on the NetView program's console. A negative response can appear as either a FUNCTION NOT SUPPORTED message or as an intermittent message, such as RESOURCE NOT AVAILABLE or FUNCTION ACTIVE. If you receive a test request that is negative, start at "Step 8. Receive FUNCTION NOT SUPPORTED Message?" on page 79 to guide you through the LPDA solicited test error diagnostic procedure.

- Test results received are invalid.

  This response occurs when there is a positive response to the test request, but the test results have a problem. This could be a problem with NCP or the communication facility. The NetView program's hardware monitor presents one of three statuses if there is a problem:

  – Test not executed
  – Bad data received
  – No data received.

  If you receive test results that are invalid, start at "Step 16. Start Traces" on page 80 to guide you through the LPDA solicited test error diagnostic procedure.

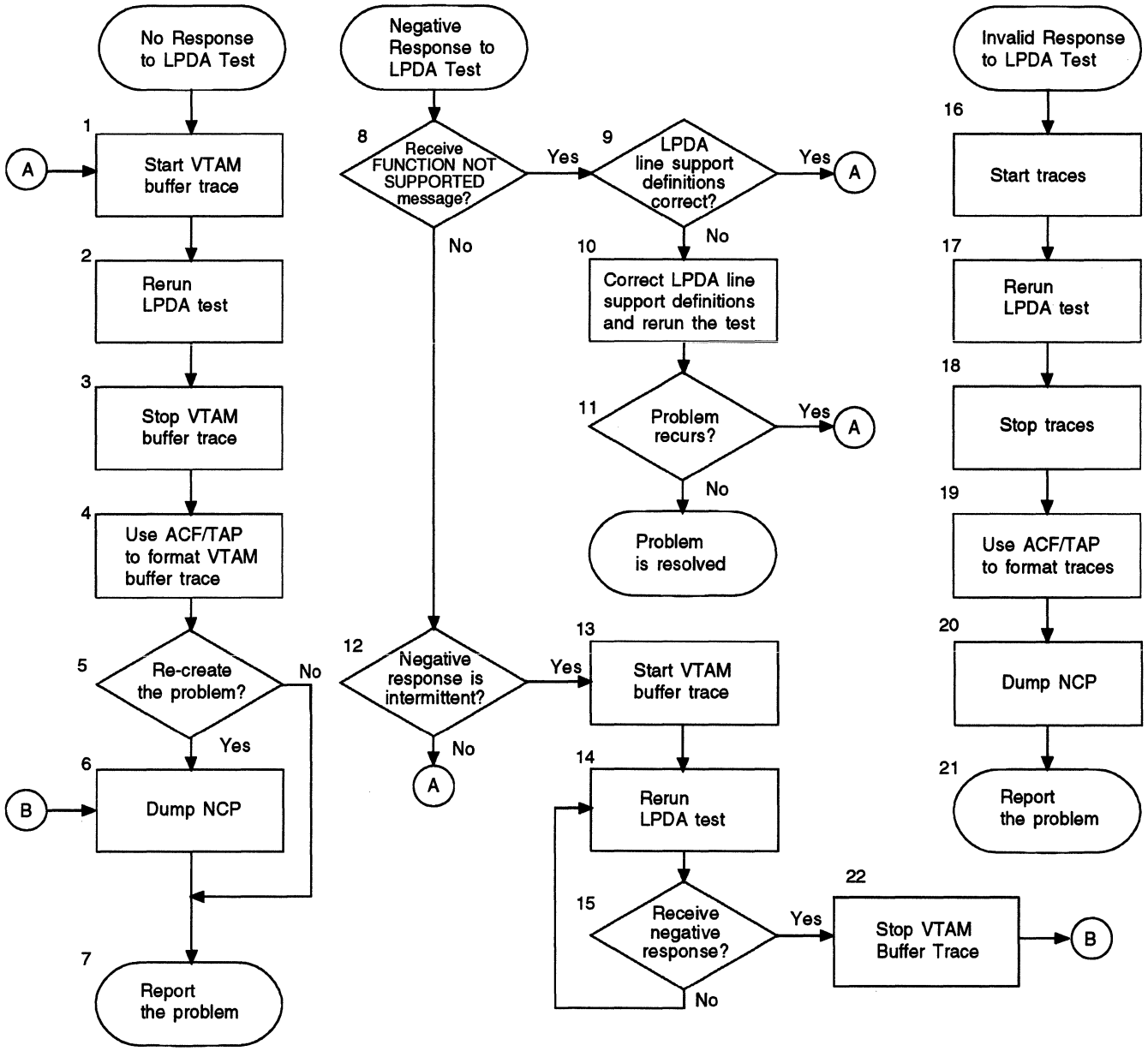


Figure 11. Overview of the LPDA Solicited Test Error Diagnostic Procedure

Step 1. Start VTAM Buffer Trace

Start the VTAM buffer trace from the specific node that the physical unit or logical unit communicates with. For information about running this trace, see "Starting and Stopping the VTAM Buffer Trace" in the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 2. Rerun LPDA Test

Rerun the LPDA test.

Step 3. Stop VTAM Buffer Trace

When the failure recurs, stop the trace that is running.

Step 4. Format VTAM Buffer Trace with ACF/TAP

Use ACF/TAP to format the VTAM buffer trace. To find out which reports to format for this trace data set, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 5. Re-create Problem?

If the problem can be re-created, go to "Step 6. Dump NCP" ; otherwise, go to "Step 7. Report Problem."

Step 6. Dump NCP

Dump the NCP that did not return an LPDA response. For information on dumping NCP, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 7. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Step 8. Receive FUNCTION NOT SUPPORTED Message?

A FUNCTION NOT SUPPORTED message could indicate:

- The line has not been generated with LPDA support (LPDATS keyword on the LINE definition statement).
- LPDA=BLOCK has been specified for a physical unit on the line.

If you received a FUNCTION NOT SUPPORTED message, go to "Step 9. Check LPDA Line Support Definitions" ; otherwise, go to "Step 12. Intermittent Negative Response."

Step 9. Check LPDA Line Support Definitions

Check the LPDA line support definitions. See *NCP, SSP, and EP Resource Definition Reference* for an explanation of how to define LPDA support for a line and the LPDA keyword on the PU definition statement. To verify these items, check the output of your generation definition.

If the LPDA line support definitions are correct, go to "Step 1. Start VTAM Buffer Trace" ; otherwise, go to "Step 10. Correct LPDA Definitions."

Step 10. Correct LPDA Definitions

Correct LPDA line support definitions, regenerate and reload, and rerun the test.

Step 11. Check if Problem Recurs

If the problem recurs, go to "Step 1. Start VTAM Buffer Trace" ; otherwise, the problem has been resolved.

Step 12. Intermittent Negative Response

If the reason for the negative response appears to be intermittent, such as RESOURCE NOT AVAILABLE or FUNCTION ACTIVE messages, go to "Step 13. Start VTAM Buffer Trace" ; otherwise, go to "Step 1. Start VTAM Buffer Trace."

Step 13. Start VTAM Buffer Trace

Start the VTAM buffer trace from the specific node that the physical unit or logical unit communicates with.

Step 14. Rerun LPDA Test

Rerun the LPDA test.

You are attempting to recreate an intermittent problem. Continue to run the LPDA test until you receive a negative response. If you do not receive a negative response you could consider the problem resolved.

Step 15. Receive a Negative Response?

If you received a negative response, go to "Step 22. Stop VTAM Buffer Trace" ; otherwise, go to "Step 14. Rerun LPDA Test."

Step 16. Start Traces

From the following list, select the traces applicable to your network and access method.

For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- NCP line trace.

  If you activate an NCP line trace against a line attached to NTRI, the data is returned from a NTRI line trace and an IOH trace, instead of from an NCP line trace.

- Scanner interface trace (SIT): To use this trace, the line to be traced must be active.

  If you activate SIT against an address that has a TIC installed at that address, the data is returned from a TIC internal trace instead of from SIT.

- VTAM buffer trace: For a failing physical or logical unit. Start them from the specific node the physical or logical unit communicates with.

Step 17. Rerun LPDA Test

Rerun the LPDA test.

Step 18. Stop Traces

Stop NCP line trace, SIT, and the VTAM buffer trace.

Step 19. Format Traces with ACF/TAP

Use ACF/TAP to format traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 20. Dump NCP

Dump the NCP that returned the invalid LPDA response. For information on dumping NCP, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 21. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Step 22. Stop VTAM Buffer Trace

When the failure recurs, stop the trace that is running.

Go to "Step 6. Dump NCP."

LPDA Unsolicited Test Error Diagnostic Procedure

One possible problem with unsolicited tests can be invalid test results. Because the tests result from events that are difficult to predict or control, these problems are more difficult to re-create.

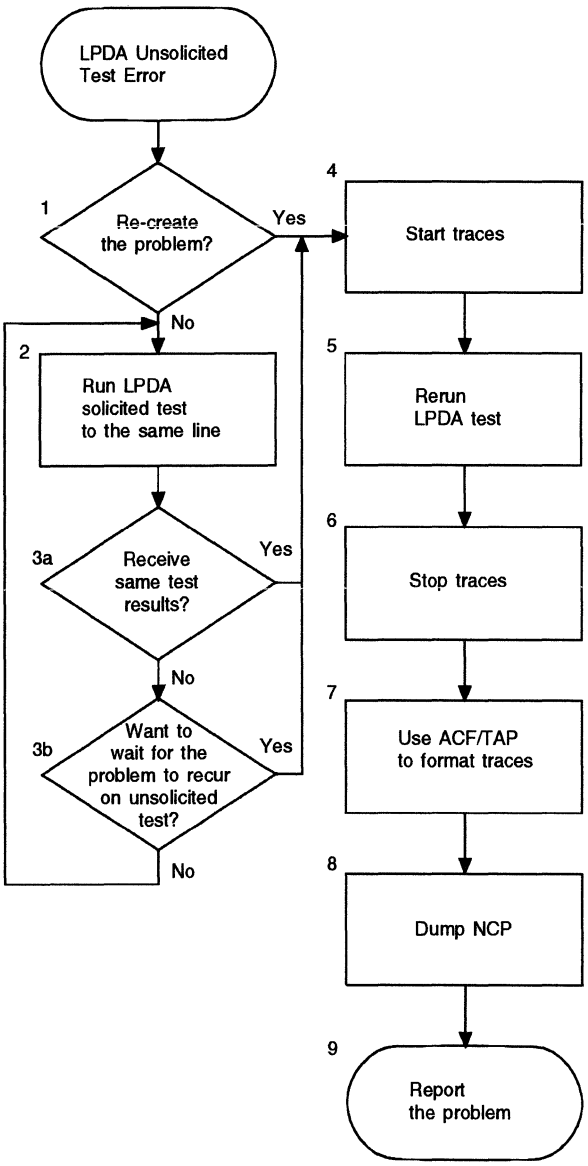


Figure 12. Overview of the LPDA Unsolicited Test Error Diagnostic Procedure

Step 1. Re-create Problem

Because the tests result from events that are difficult to predict or control, these problems are more difficult to re-create. If you cannot re-create the problem, go to "Step 2. Run LPDA Test" ; otherwise, go to "Step 4. Start Traces."

Step 2. Run LPDA Test

Run an LPDA solicited test to the same line.

Step 3. Check Test Results

1. You should receive the same results for a solicited test as you received for an unsolicited test. If you receive the same results, go to "Step 4. Start Traces" ; otherwise, continue.
2. If you do not receive the same results, the problem may be intermittent. If you want to wait for the problem to recur on an unsolicited test, go to "Step 4. Start Traces" ; otherwise, you can return to "Step 2. Run LPDA Test" and continue attempting to re-create the problem with a solicited test.

Step 4. Start Traces

From the following list, select the traces applicable to your network and access method.

For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- NCP line trace.

  If you activate an NCP line trace against a line attached to NTRI, the data is returned from a NTRI line trace and an IOH trace, instead of from an NCP line trace.

- Scanner interface trace (SIT): To use this trace, the line to be traced must be active.

  If you activate SIT against an address that has a TIC installed at that address, the data is returned from a TIC internal trace instead of from SIT.

- VTAM buffer trace: For a failing physical or logical unit. Start them from the specific node the physical or logical unit communicates with.

Step 5. Rerun LPDA Test

If you were able to re-create the problem using a solicited LPDA test, rerun the solicited LPDA test; otherwise, you must wait for the unsolicited LPDA test error to recur.

Step 6. Stop Traces

Stop NCP line trace, SIT, and the VTAM buffer trace.

Step 7. Format Traces with ACF/TAP

Use ACF/TAP to format traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 8. Dump NCP

Dump the NCP that passed the invalid LPDA unsolicited test results. For information on how to do this, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."

- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 9. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Message Error Procedure

The following symptoms indicate if you have an NCP or SSP message problem:

- Message indicates an error in the message itself.
- Message is issued under inappropriate conditions.
- Message is wrong or formatted incorrectly.
- Message is not documented in *NCP, SSP, and EP Messages and Codes.*
- Message text does not explain condition.

Documentation Checklist

if the problem occurs because of a message error, use the procedure in Figure 13 on page 85 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

For the SSP loader utility or dumper utility message problems:

- Console log
- Job output listing
- NDF generation definition
- Host region (MVS and VM) or partitioned (VSE) dump (optional)
- Host CCW trace (optional)
- Channel adapter IOH trace (optional)
- NCP stand-alone dump (optional).

For assembler message problems:

- Input to the assembler and output listing
- Console log (optional)
- Host region (MVS and VM) or partitioned (VSE) dump (optional).

For ACF/TAP message problems:

- Console log
- Job output listing
- Trace data set (COMWRITE, GTF, DOS) (optional)
- Host region (MVS and VM) or partitioned (VSE) dump (optional).

For NDF message problems:

- NDF generation definition report
- Generation definition.

For CRP message problems:

- Console log
- Job output listing
- NCP generation definition.

Diagnostic Procedure

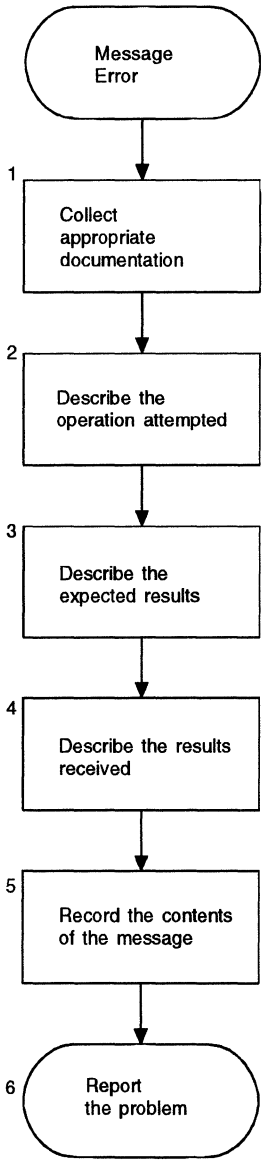


Figure 13. Overview of the Message Error Diagnostic Procedure

Step 1. Collect Documentation

To collect the documentation appropriate to the problem, see "Documentation Checklist" on page 84.

Step 2. Describe the Operation You Attempted

Step 3. Describe the Results You Expected

Step 4. Describe the Results You Received

Step 5. Record Content of Message

Record the complete content of the message, including the message identifier. For example:

```
ICN111I SEQUENCE ERROR, PREVIOUS GROUP HAS NO LINES
```

Step 6. Gather Information

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

NCP Load and Initialize Error Procedure

This section applies to SSP V3R6 and later releases.

This procedure helps you determine exactly where a failure occurred during the load, initialization, or activation of NCP in a channel- attached communication controller. The following symptoms indicate an NCP load, initialize, or activate problem:

- Initialize failure of NCP occurs.
- Load failure of NCP occurs.

If a communication controller channel error occurs while loading NCP, the SSP loader utility produces a trace table containing information on the channel programs executed by the utility. If the stand-alone SSP loader utility is invoked, the trace table is written to SYSPRINT.

If the SSP loader utility is invoked by VTAM, you must define a data set or file for the trace table.

MVS: To allocate the data set, use the sample JCL in Figure 14; then to define the data set, include the sample JCL in Figure 15 on page 87 in your VTAM startup job.

```
//ddname   DD DSN=(output-data-set-name),DISP=(NEW,CATLG),
//            UNIT=device-number,VOLSER=serial-number,
//            SPACE=(TRK,(1,5)),DCB=(DSORG=PS,RECFM=FA,
//                   BLKSIZE=121,LRECL=121)
```

Figure 14. JCL for Allocating a Data Set before Starting VTAM

```
//LDRIOTAB DD DSN=(output-data-set-name),DISP=(SHR,PASS,KEEP)
//*
```

Figure 15. JCL for Defining a Trace Table Data Set at VTAM Startup

VM: Include the following sample FILEDEF in your VTAM startup job to define the data file.

```
FILEDEF LDRIOTAB DISK fn ft fm
```

VSE: Include the following sample JCL in your VTAM startup job to define the data file.

```
// ASSGN SYSLST,cua
```

The trace table for a load describes the last 15 channel programs executed; each channel program is represented by one entry in the table. Each table entry contains the following information:

- The command channel words (CCWs) that compose the channel program (there may be up to three CCWs)
- The channel status word (CSW) for the channel program
- The first 20 bytes of the channel data transfer buffer immediately after execution of the channel program.

Figure 16 on page 88 illustrates some of the normal channel commands used during the load, initialization, and activation sequence for loading an NCP load module into a communication controller. The command sequence has been abbreviated for clarity.

The diagnostic procedure in "Diagnostic Procedure" on page 89 refers to Figure 16 on page 88. This procedure and Figure 16 do not discuss disk loading functions of the various communication controllers.

Note: The numbered callouts in Figure 16 on page 88 correspond to diagnostic steps discussed in the NCP load, initialize, or activate error diagnostic procedure on page 89 .

Documentation Checklist

If the problem occurs because of an NCP load, initialize, or activate error, use the procedure in Figure 17 on page 89 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- CCW/CSW traces with data
- NCP dump.

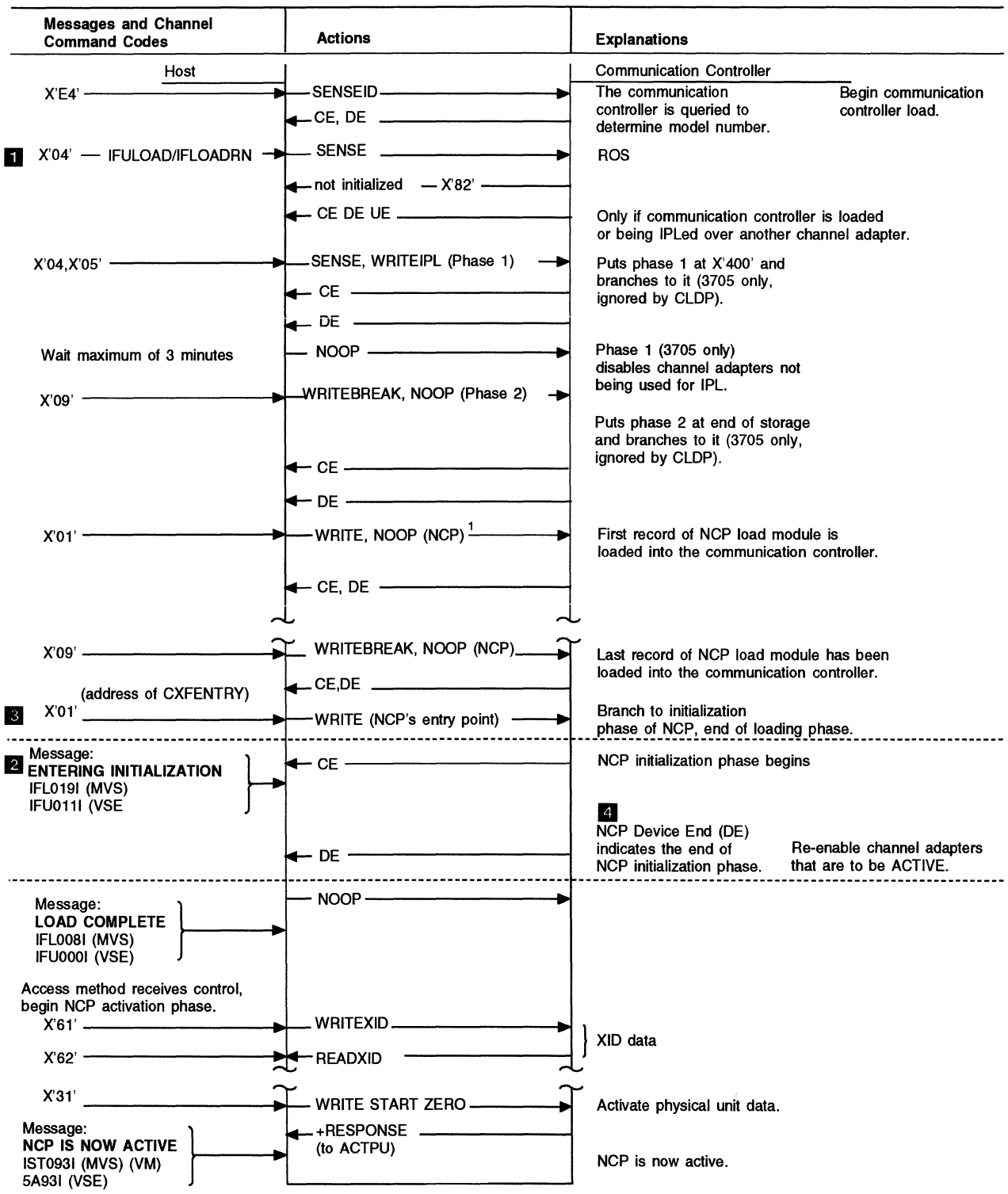


Figure 16. Overview of the SSP Loader Utility and Host or Communication Controller Interaction

[1]This WRITE may be chained to WRITESTART. For example:

```
WRITESTART,WRITE,NOOP(NCP)
```

Diagnostic Procedure

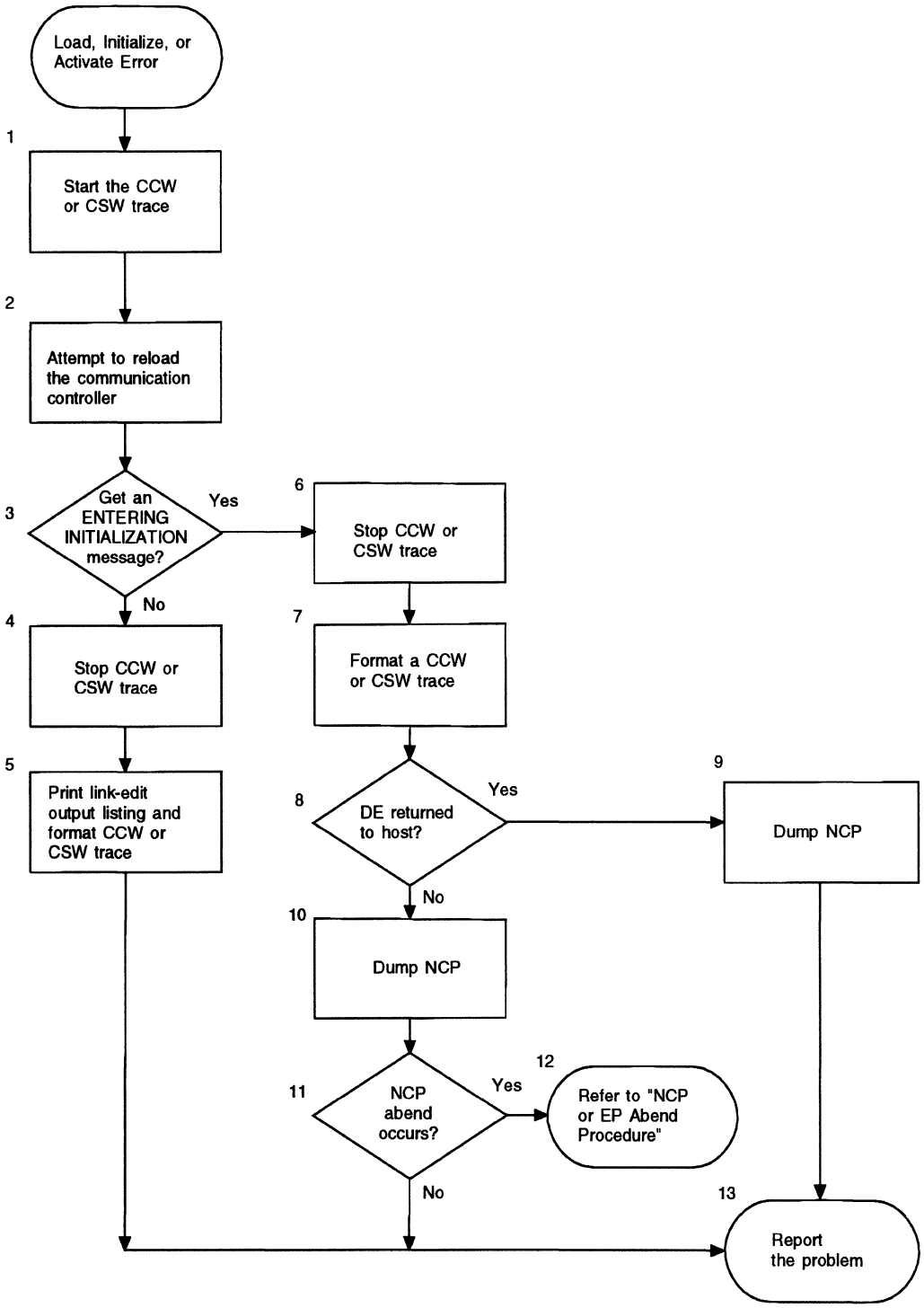


Figure 17. Overview of the NCP Load and Initialize Error Procedure

Step 1. Start CCW/CSW Trace

Start the CCW/CSW trace. If you use the internal CCW trace, you may not need to start host traces and re-create the problem. For information on starting these traces, see the service aids for your operating system.

Step 2. Reload Communication Controller

Attempt to reload the communication controller experiencing the problem. You must use the SSP loader utility to load NCP into your channel-attached communication controller. Do not use the access method to perform this task. If you do not use the SSP loader utility, this procedure and Figure 16 on page 88 will not be valid. Use the IFLOADRN command for MVS and VM; use the IFULOAD command for VSE. See Item 1 in Figure 16 on page 88.

Step 3. Check Console Messages

Did either of the following messages display at the console?

```
IFL019I  ENTERING INITIALIZATION
IFU011I  ENTERING INITIALIZATION
```

Note: See Item 2 in Figure 16 on page 88.

If one of the above messages was displayed, keep a record of the message for reporting the problem.

Step 4. Stop CCW/CSW Trace

For information on stopping these traces, see the service aids for your operating system.

Step 5. Print Link-edit Output and Format Trace

If the communication controller did not finish loading, print the link-edit output listing and format the CCW/CSW trace.

Step 6. Stop CCW/CSW Trace

For information on stopping these traces, see the service aids for your operating system.

Step 7. Format CCW/CSW Trace

For information on formatting these traces, see the service aids for your operating system.

Step 8. Check Device End in CCW/CSW Trace

Check the CCW/CSW trace to determine whether the device end (DE) was returned to the host after the CXFENTRY address (CXFSTART, if NCP V3 is being loaded) was sent to NCP. See Items 3 and 4 in Figure 16 on page 88. If the IFL008I or IFU000I message appeared at the console (which means the DE was returned), keep a record of the message.

Step 9. Dump NCP

Dump the NCP that failed. For information on how to do this, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."

- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 10 Dump NCP

Dump the NCP that failed. For information on how to do this, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 11. Check for NCP Abend

If you received an NCP abend when the failure occurred, go to "Step 12. Gather Information on NCP Abend" ; otherwise, go to "Step 13. Report Problem."

Step 12. Gather Information on NCP Abend

The NCP has abended during the initialization phase. To gather information on the NCP abend, see "NCP or EP Abend Procedure" on page 25.

Step 13. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center. If the problem is a hardware-related failure, contact your local IBM branch office for support.

NCP or EP Loop Error Procedure

An NCP or EP loop problem exists when NCP or EP seems to repeat an operation endlessly. The following symptoms indicate a loop problem:

- NCP or EP does not respond to commands entered on the console.
- Printers stop.
- NCP or EP functions stop.
- Tapes stop.
- Wait light on IBM 3725 panel is off (IBM 3720 and 3745 panels do not have a wait light).

For the IBM 3725, the wait light can be off, making NCP or EP appear to be in a loop when it actually is not. This may occur if the PAUSE keyword on the LINE definition statement for active lines is 0, causing loop symptoms to appear if there is heavy traffic on the lines. Level 2 and level 3 use all central control unit (CCU) cycles while trying to service the lines, which leaves level 4 and level 5 little time to run.

Documentation Checklist

If you suspect that NCP or EP is in a loop, use the diagnostic procedure in Figure 18 to diagnose the problem. During the diagnostic procedure, you may need to collect the following documentation:

- Branch trace
- Link-edit map
- NCP or EP stand-alone dump.

Diagnostic Procedure

To solve a loop problem, the IBM Support Center representative must know the instruction addresses in the loop. Use the branch trace to find these addresses. The loop error diagnostic procedure must be executed while NCP or EP is still looping.

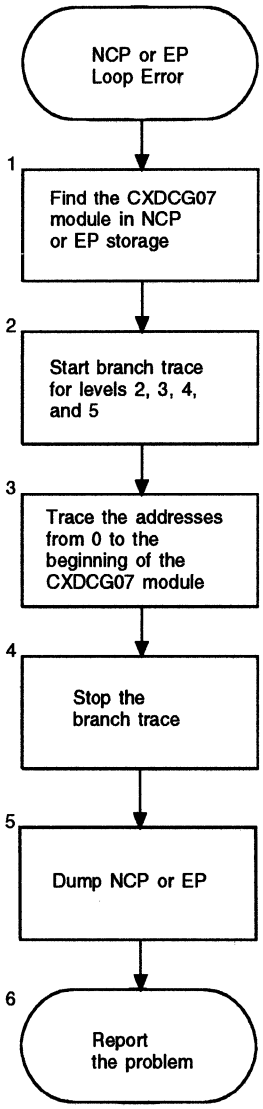


Figure 18. Overview of the NCP or EP Loop Error Diagnostic Procedure

Step 1. Find CXDCG07 Module in NCP or EP Storage

You can find the location of the CXDCG07 module in NCP or EP storage in two ways:

- Obtain the link-edit map for your NCP or EP. This map is output from the link-edit step when your NCP or EP was generated. Find the module named CXDCG07 in the alphabetical listing. Note the starting address of this module.
- Dump, format, and print NCP or EP. For information on dumping NCP, see the following:
  - For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
  - For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
  - For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

This CXDCG07 module contains the 100-millisecond timer code. Do not trace this code with the branch trace because this causes the trace table to fill with timer-code entries.

For a formatted dump, a load map is located immediately before the hexadecimal section. Search the list of modules for CXDCG07. Note the starting address of this module.

For an unformatted dump, find CXDCG07 in the interpreted section of the hexadecimal section of the dump. The module name is at the end of the module. Note the address of the next fullword following the name of the module that precedes the CXDCG07 module in the unformatted dump. This is the start of the CXDCG07 module.

If you dump NCP or EP, you must re-create the problem.

Step 2. Start Branch Trace

While NCP or EP is looping, start the branch trace for levels 2, 3, 4, and 5. For information on using the branch trace, see "Branch Trace" on page 160.

Step 3. Trace Addresses to Beginning of CXDCG07

Trace the range of the addresses starting at address 0 and ending at the beginning address of the CXDCG07 module.

Step 4. Stop Branch Trace

After the branch trace has run for a few minutes, stop the trace. For information on stopping the branch trace, see "Branch Trace" on page 160.

Step 5. Dump NCP or EP

Dump the NCP or EP that was looping. For information on dumping NCP, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" on page 201 and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM" on page 219.
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE" on page 227.

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 6. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

NCP Performance Error Procedure

An NCP performance problem is usually characterized by slow response time. The following symptoms indicate an NCP performance error:

- BSC lines are not being polled.
- Performance is degraded after a network outage.
- Response does not occur.
- Response is slow.
- SDLC physical units are RNR polled.
- Virtual routes attached to NCP are held.

Performance problems are hard to pinpoint and difficult to define. When you suspect a performance problem, gather as much information as possible about your operating environment before and during poor performance times. Performance can often be improved by simply tuning the environment (changing the NCP or host system generation parameters). Since overuse of dynamic resources can degrade NCP performance, define all the resources required for normal processing in your generation definition and use the dynamic allocation function to handle unexpected demand. See NCP, SSP, and EP Resource Definition Guide for more information about dynamic resource allocation.

Documentation Checklist

If your system is experiencing a performance problem, use the procedure in Figure 19 on page 95 to collect the following documentation:

- NDF generation definition report
- NCP line trace
- NCP stand-alone dump
- NTRI line trace
- NetView program route test output
- SIT
- TIC internal trace
- VTAM I/O trace or TCAM channel I/O interrupt trace
- VTAM or TCAM buffer trace.

Diagnostic Procedure

Poor performance can occur with the host application, the access method, NCP, or its attached resources. This procedure helps only with performance problems in NCP or its attached resources.

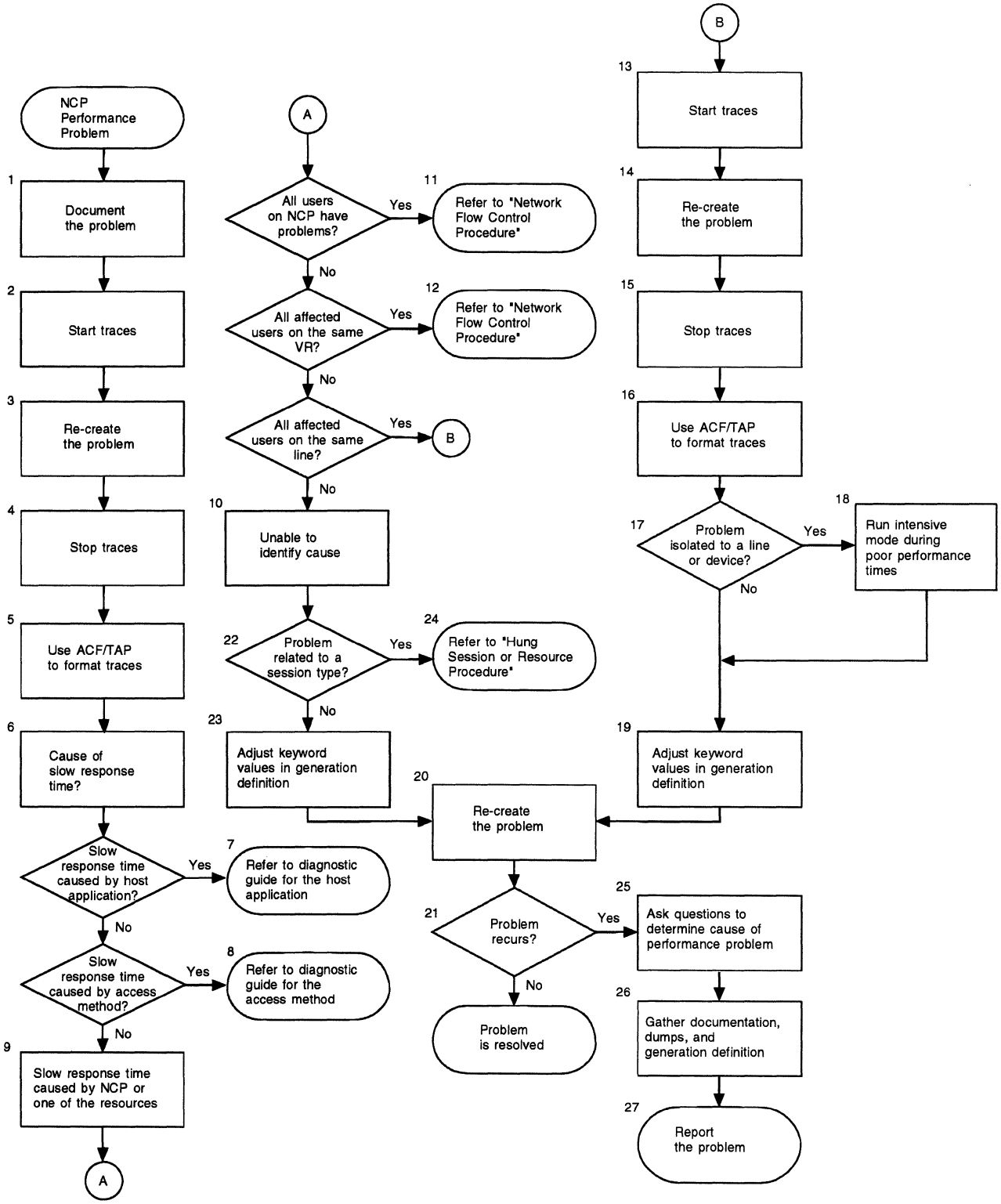


Figure 19. Overview of the NCP Performance Error Diagnostic Procedure

Step 1. Document Problem

Prepare a description of the following items to report to the IBM Support Center:

- The operation you were performing
- The results you expected
- The results you received.

Step 2. Start Traces

From the following list, select the traces applicable to your access method:

For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- VTAM buffer trace or the TCAM PIU trace: For a failing physical or logical unit. Start them from the specific node the physical unit or logical unit communicates with.
- VTAM I/O trace or the TCAM channel I/O interrupt traces.

Step 3. Re-create Problem

To determine the origin of a performance problem, use the resources that are having performance problems during the poor performance times. Run the traces long enough to catch the data flow between the host application and the user.

Step 4. Stop Traces

From the following list, select the traces applicable to your access method:

- VTAM buffer trace or the TCAM PIU trace: For a failing physical or logical unit. Stop them from the specific node the physical unit or logical unit communicates with.
- VTAM I/O trace or the TCAM channel I/O interrupt traces.

Step 5. Format Traces with ACF/TAP

Use ACF/TAP to format traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on how to use ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 6. Determine Cause of Slow Response Time

1. Use the time stamp printed with each trace entry to determine if the host application caused the slow response time. If so, go to "Step 7. See the Diagnosis Guide of Host Application" ; otherwise, continue.
2. Use the time stamp printed with each trace entry to determine if the access method caused the slow response time. If so, go to "Step 8. See the Diagnosis Guide of Access Method" ; otherwise, go to "Step 9. Caused by NCP or Other Resources."

Step 7. See the Diagnosis Guide of Host Application

See the diagnosis guide of the host application.

Step 8. See the Diagnosis Guide of Access Method

See the diagnosis guide of the access method.

Step 9. Caused by NCP or Other Resources

If the slow response time was not caused by the host application or by the access method, the problem must be with either NCP or one of its resources.

For information on NCP system slowdown, see *NCP and EP Reference*.

Your answers to the following questions determine the next step:

1. Are all users attached to this NCP experiencing the performance problem? If so, this may indicate a buffer shortage problem. If NCP has buffer shortage problems, the users may not be receiving any responses. In this case, go to "Step 11. Buffer Shortage Data Information" ; otherwise, continue.
2. Are all the users who are experiencing the performance problem using the same virtual route or a selected group of virtual routes? If you do not know, use either Network Logical Data Manager (NLDM) or the NetView program to determine to which virtual route a particular user is attached. See *NLDM Installation and Operations* or *NetView Operation* for information on using these products. If all users are using the same virtual route, you may have a virtual route problem. Go to "Step 12. Virtual Route Data" ; otherwise, continue.
3. If all users are experiencing the performance problem using the same line or the same line type, go to "Step 13. Start NCP Line Trace and SIT on Failing Line" for line problems (or terminal problems); otherwise, go to "Step 10. Unable to Identify Cause?."

Step 10. Unable to Identify Cause?

If none of these descriptions match your performance problem and you cannot pinpoint the cause of your performance degradation, go to "Step 22. Problem Related to Particular Session Type?."

Step 11. Buffer Shortage Data Information

See "Network Flow Control Error Procedure" on page 115 for a description of buffer shortage data.

Step 12. Virtual Route Data

See "Network Flow Control Error Procedure" on page 115 for a description of virtual route data.

Step 13. Start NCP Line Trace and SIT on Failing Line

Many times you can improve poor performance for lines and devices by tuning NCP generation parameters. If your performance problem seems to be line dependent, start an NCP line trace and SIT for the failing line. However, using these traces may worsen performance. You cannot start these traces if NCP is in slowdown.

If you activate an NCP line trace against a line attached to NTRI, the data is returned from a NTRI line trace and an IOH trace instead of from an NCP line trace.

If you activate SIT against an address with TIC rather than a line scanner installed at that address, the data is returned from a TIC internal trace and not from SIT.

For NCP line trace and SIT start and stop information, see the *NCP, SSP, and EP Trace Analysis Handbook*

Step 14. Re-create Problem

Attempt to re-create the problem.

Step 15. Stop Traces

Stop the NCP line trace, and SIT (IBM 3720, 3725, and 3745).

Step 16. Format Traces with ACF/TAP

Use ACF/TAP to format traces. To find out which report to format for the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 17. Problem Isolated to Line or Device?

Check if the problem is isolated to a line or device. If the problem is related to a particular device or line (or group of devices or lines), go to "Step 18. Run in Intensive Mode" ; otherwise, monitor and record the RECMS records in LOGREC.

Step 18. Run in Intensive Mode

See *VTAM Operation* or *TCAM Operation* for information on how to run in intensive mode during the poor performance times.

Step 19. Adjust Keyword Values

Adjust the keyword values specified in your generation definition.

The following table shows some of the keywords on NCP definition statements that may impact the performance of NCP lines, physical units, and terminals. Check the values for these keywords specified in your generation definition and correct them as appropriate. See *NCP, SSP, and EP Resource Definition Reference* and *NCP, SSP, and EP Resource Definition Guide* for a description of the meaning of these keywords.

Table 7. NCP Keywords That May Affect NCP Performance

Definition Statement	SDLC	BSC and Start-Stop	SDLC, BSC, and Start-Stop	Channel Links	Internet Protocol	Frame Relay
BUILD		ITEXTTO	DIALTO DSABLTO ENABLTO TRANSFR DELAY TIMEOUT		IPPOOL IPRATE CNLSQMAX CNLSQTIM	
LINE	HDXSP SERVLIM	CUTOFF NEGPOLP POLIMIT POLLTO SERVPRI SESSION	AVGPB PAUSE REDIAL RETRIES TRANSFR	ADDRESS CA CASDL DELAY DYNADMP ETRATIO INBFRS HICHAN LOCHAN NCPCA NCPCOLL TIMEOUT TRANSFR	INTFACE	LOCALTO MAXFRAME T2TIMER MAXOUT MODULO
PU	AVGPB DATMODE IRETRY MAXDATA MAXOUT PASSLIM RETRIES					MAXOUT MODULO
GROUP	ACTIVTO RETRYTO LNCTL	CRETRY DELAY TEXTTO TTDCNT WACKCNT WAKDLAY LNCTL	REPLYTO LNCTL	LNCTL=CA		T2TIMER MAXOUT MODULO
SERVICE			ORDER= (PU1,PU2, PU3,...)			
LU	BATCH PACING					
TERMINAL		BFRDLAY CRDLAY				

Step 20. Re-create Problem

Attempt to re-create the problem after tuning the parameters.

Step 21. Check if Problem Recurs

If the problem recurs, go to "Step 25. More Questions" ; otherwise, the problem has been resolved.

Step 22. Problem Related to Particular Session Type?

If the problem is related to a particular session type, go to "Step 24. Hung Sessions and Resources" ; otherwise, go to "Step 23. Adjust Keyword Values."

Step 23. Adjust Keyword Values

Adjust the keyword values specified in your generation definition.

Table 7 on page 99 shows some of the keywords on NCP definition statements that may impact the performance of NCP channel links. Check the values for these keywords specified in your generation definition and correct them as appropriate. For a description of the meaning of the keywords, see *NCP, SSP, and EP Resource Definition Reference* and *NCP, SSP, and EP Resource Definition Guide*.

For the IBM 3720 Communication Controller, 370 I/O channel attachments can also be defined as channel links on either the GROUP or LINE definition statement.

Go to "Step 20. Re-create Problem."

Step 24. Hung Sessions and Resources

See "Hung Session or Hung Resource Procedure" on page 57 for a description of hung sessions and resources.

Step 25. More Questions

Ask a few more questions to determine the cause of your performance problem.

- Is there a particular time of day when poor performance occurs?
- Are there any unique applications running at that time, such as a batch transfer operation?
- Have any recent modifications been made to NCP generation parameters?
- Have any user modifications been made to TCAM, VTAM, or NCP?

Step 26. Gather All Documentation

Gather all documentation, together with a copy of any NCP dumps taken during this procedure and a copy of the NCP generation input definition.

Step 27. Report Problem

Collect all documentation collected during the diagnostic procedure and report the problem to the IBM Support Center.

Ethernet-Type LAN or Internet Protocal Error Procedure

This section applies to NCP V6R1, V6R2, and V6R3.

An internet route error occurs when IP datagrams do not reach their requested destinations. Problems can be related to NCST logical unit sessions, Ethernet-type LAN lines, or internet routing. The following symptoms indicate an NCP internet function error:

- An NCST session does not activate.
- No Ethernet-type LAN or internet traffic is flowing through NCP.
- Performance is poor for internet traffic and Ethernet-type LANs.

Documentation Checklist

If your system experiences an internet function error, use the diagnostic checklist to diagnose the problem. After using the diagnostic checklist, collect the required documentation and then report the problem to the IBM Support Center.

For an NCST logical unit problem you may need to collect:

- A VTAM buffer trace
- A channel control word (CCW) trace with SNALINK DEBUG on
- An NCP dump.

For an Ethernet-type LAN problem you may need to collect:

- A line trace
- A SIT
- An NCP dump.

For an internet routing problem you may need to collect:

- A VTAM buffer trace
- A line trace
- An NCP dump.

Diagnostic Procedure

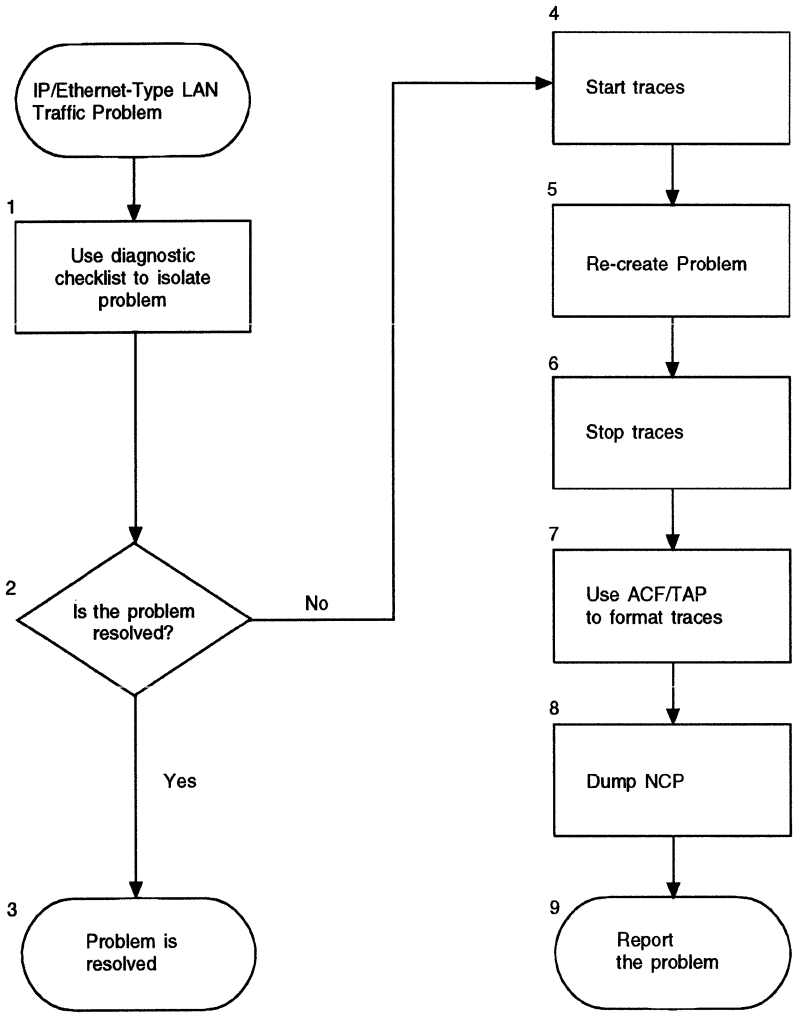


Figure 20. Overview of the Ethernet-Type LAN or Internet Protocol Diagnostic Procedure

Step 1. Isolate Problem with Diagnostic Checklist

Use the following diagnostic checklist to verify possible Ethernet-type LAN or internet routing problems related to your generation definition before you call the IBM Support Center.

1. For a problem related to NCST logical unit sessions:

   If traffic is not flowing:

   __ • Are the necessary NCST logical unit sessions active?

   __ • Is the NCST logical unit in session with the desired remote logical unit?

   If the NCST session does not activate:

   __ • Are all necessary subarea links active?

   __ • For NCST-NCST sessions, does each logical unit have the other specified as the remote logical unit?

- ___ • For NCST-SNALINK sessions, is the SNALINK logical unit specified as the remote logical unit on the NCP generation?
- ___ • Does an SNA path exist between the NCST logical unit and its session partner (remote logical unit)?
- ___ • In a multiple host environment, are the VTAM cross-domain resource managers (CDRMs) active and the proper VTAM cross-domain resource (CDRSC) major nodes defined?
- ___ • For NCST-SNALINK sessions, is the SNALINK application logical unit properly defined to the VTAM application major node?
- ___ • For NCST-SNALINK sessions, are the host TCP/IP and SNALINK applications active?

2. For a problem related to Ethernet-type LAN lines:
   - ___ • Are the necessary Ethernet-type LAN lines active?
   - ___ • Is the Ethernet-type LAN line internet address in the same network or subnetwork as its devices?
   - ___ • Is the correct Ethernet-type LAN frame format (Ethernet V2 or IEEE 802.3) being used?
   - ___ • Are the proper physical Ethernet-type LAN connections made?
   - ___ • Is the Ethernet-type LAN device set up for the correct physical medium (thin or thick net)?
   - ___ • Is the IPRATE keyword on the BUILD definition statement coded to allow the desired amount of Ethernet-type LAN line traffic?
3. For a problem related to internet routing:
   - ___ • Does an internet route exist to the desired destination network or subnetwork?
   - ___ • Are there two or more hosts in the same internet network; is subnetting required?
   - ___ • Is the TCP/IP PING command effective when you try to contact intermediate nodes or interfaces?
   - ___ • Is a default or backup route unintentionally being used?
   - ___ • Is an over-congested subarea link causing IP datagrams to be discarded?
   - ___ • Is the IPPOOL keyword on the BUILD definition statement coded to allow enough buffers for internet traffic?
   - ___ • Are the CNLSQMAX and CNLSQTIM keywords on the BUILD definition statement coded so that PIUs are not being unnecessarily discarded?
   - ___ • Has NCP gone into slowdown mode?

Step 2. Is Problem Resolved?

If the checklist resolved the problem, there is no need to continue; otherwise, go to "Step 4. Start Traces."

Step 3. Problem Is Resolved

Step 4. Start Traces

From the following list, select the traces applicable to the problem. For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- NCP line trace.
- Scanner interface trace.
- VTAM buffer trace: For a failing physical or logical unit. Start this trace from the specific node the physical unit or logical unit communicates with.
- CCW trace with SNALINK DEBUG on: For information about how to start the CCW trace for problems related to NCST logical units, see *MVS/ESA Service Aids* and *TCP/IP Installation and Maintenance* for your operating system.

Step 5. Re-Create Problem

Attempt to re-create the problem.

Step 6. Stop Traces

Stop the NCP line trace, SIT, VTAM buffer trace, and CCW trace.

Step 7. Format Traces Using ACF/TAP

Use ACF/TAP to format traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 8. Dump NCP

For information on dumping NCP, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 9. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Internet Route Error Procedure (NCP V7R1 or Later)

An internet route error occurs when IP datagrams do not reach their requested destinations. Problems can be related to NCST logical unit sessions, token-ring or Ethernet-type LAN lines, or Internet routing. The following symptoms indicate an NCP internet function error:

- An NCST session does not activate
- Internet traffic does not flow through NCP
- Performance is poor for internet traffic and the Ethernet-type LANs or token-ring LANs that carry it
- Dynamic routes are not recognized by NCP
- Communications are not established with the NCPROUTE program and you receive alert flooding.

Documentation Checklist

If your system experiences an internet function error, use the diagnostic checklist to diagnose the problem. After using the diagnostic checklist, collect the required documentation and then report the problem to the IBM Support Center.

For an NCST logical unit problem you may need to collect:

- A VTAM buffer trace
- A channel control word (CCW) trace with SNALINK DEBUG on
- An NCP dump.

For a LAN problem you may need to collect:

- A line trace
- A SIT
- An NCP dump.

For an internet routing problem you may need to collect:

- A VTAM buffer trace
- A line trace
- An NCP dump.

Diagnostic Procedure

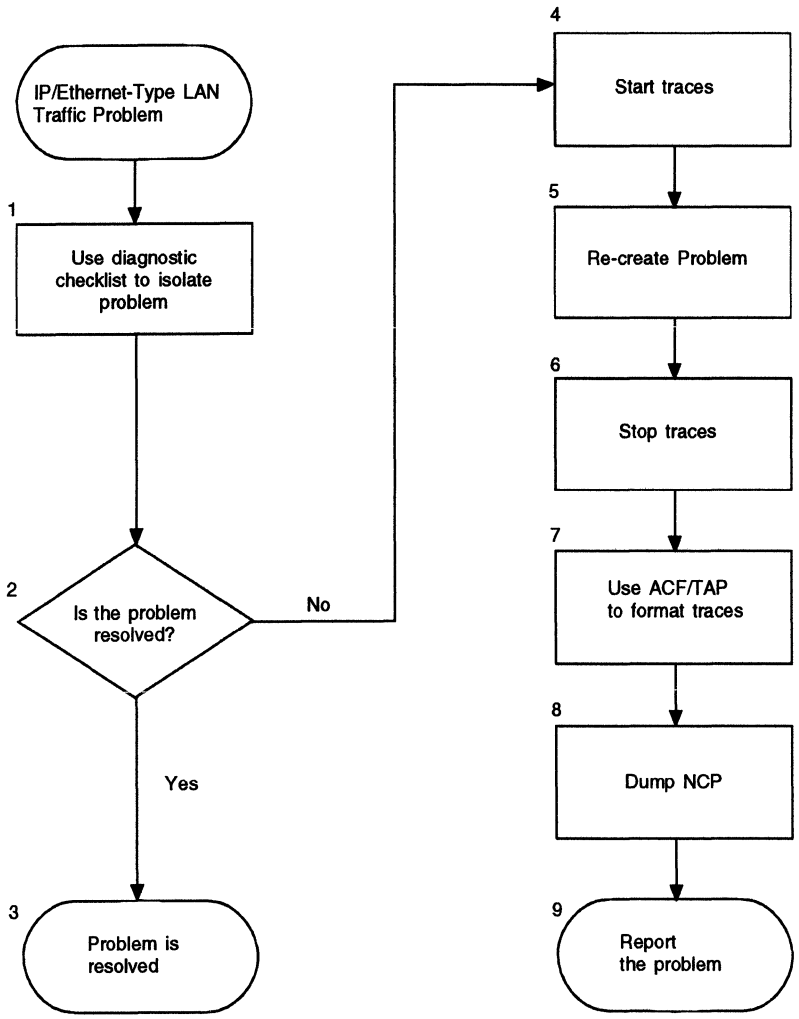


Figure 21. Overview of the Internet Route Diagnostic Procedure

Step 1. Use Diagnostic Checklist

Use the following diagnostic checklist to verify possible Ethernet-type LAN or internet routing problems related to your generation definition before you call the IBM Support Center.

1. For a problem related to NCST logical unit sessions:

   If traffic is not flowing:

   __ • Are the necessary NCST logical unit sessions active?

   __ • Is the NCST logical unit in session with the desired remote logical unit?

   If the NCST session does not activate:

   __ • Are all necessary subarea links active?

   __ • For NCST-NCST sessions, does each logical unit have the other specified as the remote logical unit?

- ___ • For NCST-SNALINK sessions, is the SNALINK logical unit specified as the remote logical unit on the NCP generation?
- ___ • Does an SNA path exist between the NCST logical unit and its session partner (remote logical unit)?
- ___ • In a multiple host environment, are the VTAM cross-domain resource managers (CDRMs) active and the proper VTAM cross-domain resource (CDRSC) major nodes defined?
- ___ • For NCST-SNALINK sessions, is the SNALINK application logical unit properly defined to the VTAM application major node?
- ___ • For NCST-SNALINK sessions, are the host TCP/IP and SNALINK applications active?

2. For a problem related to Ethernet-type LAN lines:
   - ___ • Are the necessary Ethernet-type LAN lines active and are the physical units contacted?
   - ___ • Is the Ethernet-type LAN line internet address in the same network or subnetwork as its devices?
   - ___ • Is the correct Ethernet-type LAN frame format (Ethernet V2 or IEEE 802.3) being used?
   - ___ • Are the proper physical Ethernet-type LAN connections made?
   - ___ • Is the Ethernet-type LAN device set up for the correct physical medium (thin or thick net)?
   - ___ • Is the IPRATE keyword on the BUILD definition statement coded to allow the desired amount of Ethernet-type LAN line traffic?
   - ___ • Is the newest level of microcode for the adapter installed?
3. For a problem related to token-ring LAN lines:
   - ___ • Are the necessary token-ring LAN lines active and are the physical units contacted?
   - ___ • Is the token-ring LAN line internet address in the same network or subnetwork as its devices?
   - ___ • Are the proper physical token-ring LAN connections made?
   - ___ • Is the IPRATE keyword on the BUILD definition statement coded to allow the desired amount of token-ring LAN line traffic?
   - ___ • Does the PASSLIM value allow enough internet traffic to flow?
4. For a problem related to internet routing:
   - ___ • Is the NCPROUTE program running?
   - ___ • Is the session to NCPROUTE running?
   - ___ • Does an internet route exist to the desired destination network or subnetwork?
   - ___ • Are there two or more hosts in the same internet network; is subnetting required?
   - ___ • Is the TCP/IP PING command effective when you try to contact intermediate nodes or interfaces?

- __ • Is a default or backup route unintentionally being used?
- __ • Is an over-congested subarea link causing IP datagrams to be discarded?
- __ • Is the IPPOOL keyword on the BUILD definition statement coded to allow enough buffers for internet traffic?
- __ • Are the CNLSQMAX and CNLSQTIM keywords on the BUILD definition statement coded so that PIUs are not being unnecessarily discarded?
- __ • Has NCP gone into slowdown mode?
- __ • Is the internal route RIP managed? If the route interface is not defined as RIP managed, then the route using that interface will not be RIP managed.
- __ • Are there enough routing table entries for any new routes that may be added dynamically? Check the NUMROUTE keyword on the IPOWNER statement.
- __ • Check the ordering of routes and metric assignments on the DESTADDR keyword on the IPROUTE definition statement. If more than one route exists to an IP destination, the route with the lowest metric value whose interface is active must be selected.
- __ • If communication with the owning TCP/IP host is not established and you are not receiving alerts, it could be that no NCP sessions have been activated.

5. Communications not established with NCPROUTE?
   - __ • Is the NCPROUTE program up?
   - __ • Is the routing information table (RIT) available on the owning TCP/IP host?
   - __ • Is the session to the owning TCP/IP host up?
   - __ • Is there a small value for the MAXHELLO keyword on the IPOWNER statement. A small value can create alert flooding.
   - __ • Are NCPROUTE and NCP using the same UDP port number? They must be the same.

Step 2. Problem Resolved?

If the checklist resolved the problem, there is no need to continue; otherwise, go to "Step 4. Start Traces."

Step 3. Problem is Resolved

Step 4. Start Traces

From the following list, select the traces applicable to the problem. For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- NCP line trace.
- Scanner interface trace.

- VTAM buffer trace: For a failing physical or logical unit. Start this trace from the specific node the physical unit or logical unit communicates with.
- CCW trace with SNALINK DEBUG on: For information about how to start the CCW trace for problems related to NCST logical units, see *MVS/ESA Service Aids* and *TCP/IP Installation and Maintenance* for your operating system.

Step 5. Re-create Problem

Attempt to re-create the problem.

Step 6. Stop Traces

Stop the NCP line trace, SIT, VTAM buffer trace, and CCW trace.

Step 7. Format Traces with ACF/TAP

Use ACF/TAP to format traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 8. Dump NCP

For information on dumping NCP, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.

Step 9. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

NCP 3745 Frame-Relay Link Error Procedure

This section applies to NCP V6R1 and later.

Frame-relay link problems occur when attempts to activate logical links are unsuccessful. The most common symptom for this problem is a frame-relay link station hang.

Documentation Checklist

If your system experiences a frame-relay link problem, use the procedure in Figure 22 on page 111 to diagnose the problem. Before you begin the diagnosis procedure, get an input source listing that contains the frame-relay network definition.

During the diagnostic procedure, you may need to collect the following documentation:

- Description of the operation you were performing
- Description of the results expected
- Description of the results received.

Diagnostic Procedure

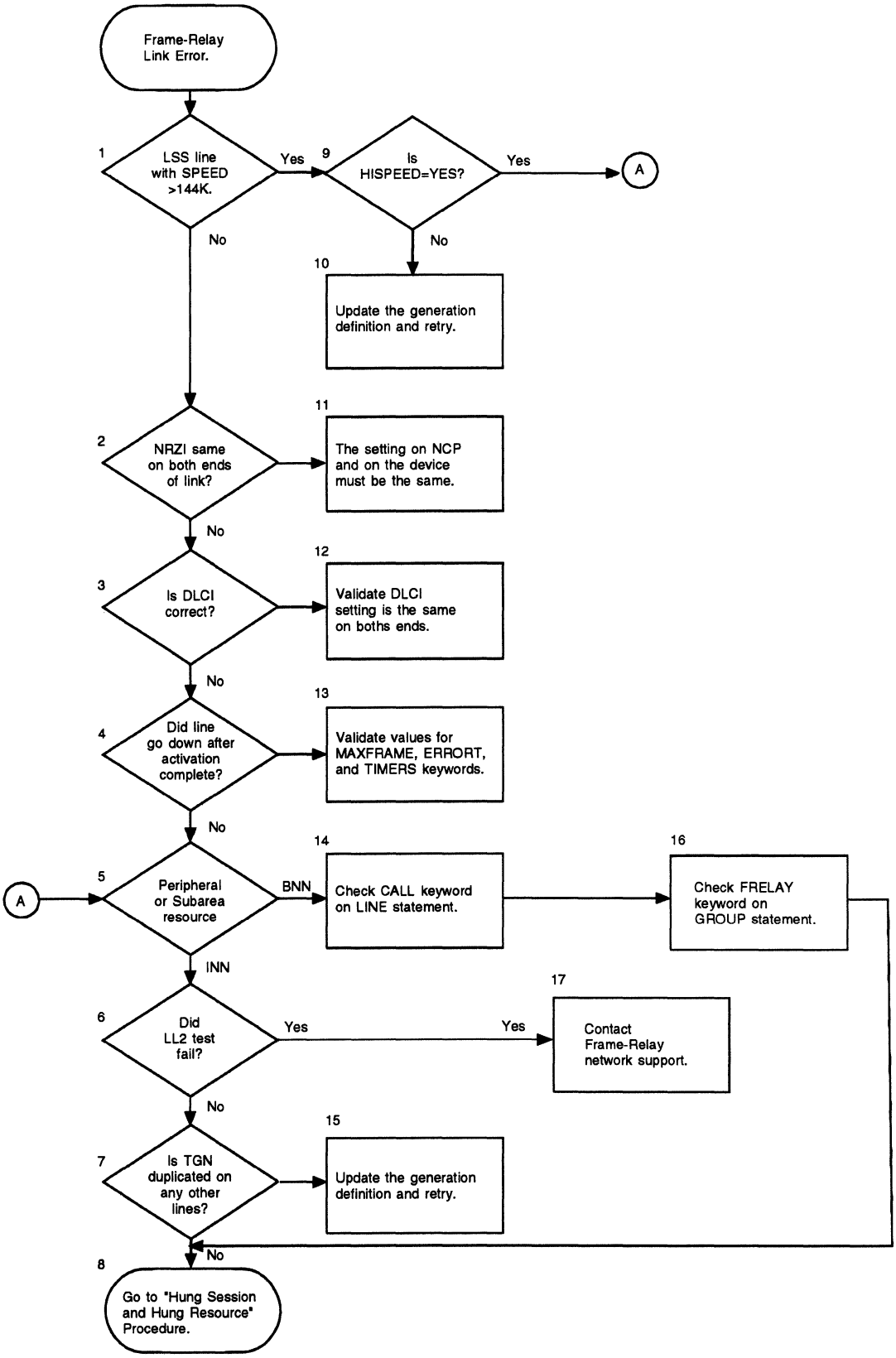


Figure 22. Overview of the NCP Frame-Relay Link Diagnostic Procedure

Step 1. Line Speed?

Low speed scanner line speed? Check the low speed scanner (LSS) line speed.

Check the LINE definition statements for the SPEED keyword. If the value of SPEED is greater than 144 000, go to "Step 8. Go to Hung Resource" ; otherwise, go to Step 2. NRZI=YES?

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the SPEED keyword.

Step 2. NRZI=YES?

Check the value coded for the NRZI keyword on the LINE definition statement.

You should code NRZI=NO on the LINE definition statement for the frame-relay physical line. If NRZI=YES, go to "Step 11. Change NRZI" ; otherwise, go to Step 3. DLCI Correct?.

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the NRZI keyword.

Step 3. DLCI Correct?

Check the assigned value of the DLCI. The DLCI values are obtained from the public frame-relay service provider. If the value is correct and you have tried all the steps in this procedure, go to "Step 4. Line Goes Down?" ; otherwise, go to "Step 12. Update DLCI"

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the ADDR keyword.

Step 4. Line Goes Down?

If the line goes down after activation complete, go to "Step 13. MAXFRAME, ERRORT, TIMERS ?" ; otherwise, go to "Step 5. Peripheral or Subarea Network."

Step 5. Peripheral or Subarea Network

If the failing resource is peripheral, go to "Step 14. Check CALL Keyword." If the failing resource is subarea, go to "Step 6. LL2 Test Fail?."

Step 6. LL2 Test Fail?

Check the number of link level 2 (LL2) test messages.

Use VTAM to perform the link level 2 test. VTAM should return the same number of messages you send. If you do not receive the same number of messages, the problem may be with your frame-relay network connections. Go to "Step 17. Contact Support."

For more information on the LL2 test, see the *VTAM Operation* book.

Step 7. TGN Duplicated?

Check the value coded for the TGN keyword on the PU definition statement for the logical line.

NCP V6R2 and Later: TGN values do not need to be unique if TGCONF=MULTI on the PU definition statement. Go to "Step 8. Go to Hung Resource"

Check the PU definition statement for unique TGN values. You should have a different TGN value for each logical line between any two subareas.

If the TGN values are unique, go to "Step 8. Go to Hung Resource" ; otherwise, go to "Step 15. Update Generation Definition."

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the TGN keyword.

Step 8. Go to Hung Resource

If you have gone through all of the steps and the problem is not resolved, then the problem may be a hung resource or hung session. For detailed diagnostic procedures see "Hung Session or Hung Resource Procedure" on page 57.

Step 9. HISPEED=YES?

Check the value coded for HISPEED on the LINE definition statement.

You must code HISPEED=YES for low speed scanner lines with speeds greater than 144 000. If HISPEED=YES, go to "Step 2. NRZI=YES?" ; otherwise, go to "Step 10. Change HISPEED"

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the HISPEED keyword.

Step 10. Change HISPEED

Update the generation definition. Change the HISPEED keyword on the LINE definition statement to HISPEED=YES. Retry the generation and try to activate the link station again.

If the logical links become active, the problem is resolved; otherwise, go to "Step 2. NRZI=YES?."

Step 11. Change NRZI

Update the generation definition.

Verify that the setting for NRZI keyword on the LINE definition statement in NCP and on the adjacent device is the same. Retry the generation and try to activate the link again.

If the logical links become active, the problem is resolved; otherwise, go to "Step 3. DLCI Correct?."

Step 12. Update DLCI

Update the generation definition. Verify that the DLCI value used by NCP and the adjacent device is the same. For subarea lines, the value must be coded in hexadecimal, on the ADDR keyword. For peripheral lines, the DLCI must be specified on the peripheral device, but not in NCP.

If the logical links become active, the problem is resolved; otherwise, go to "Step 4. Line Goes Down?."

Step 13. MAXFRAME, ERRORT, TIMERS ?

Validate values for MAXFRAME, ERRORT, and TIMERS keywords and retry.

The values for these keywords must be the same across connections. Retry the generation and try to activate the link again.

If the logical links become active, the problem is resolved; otherwise, report the problem.

Step 14. Check CALL Keyword

Check the CALL keyword on the LINE statement. The peripheral device may be trying to call in, but if all lines were coded as CALL=OUT, no logical lines are available. To call in and out you should code CALL=INOUT.

If the logical links become active, the problem is resolved; otherwise, go to "Step 16. Validate FRELAY Keyword."

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the CALL keyword.

Step 15. Update Generation Definition

Change the TGN keyword on the PU definition statement for the logical line. For frame relay, the value of TGN should be unique for each logical line between any two subareas. Retry the generation and try to activate the link again.

If the logical links become active, the problem is resolved; otherwise, go to "Step 8. Go to Hung Resource."

Step 16. Validate FRELAY Keyword

If subarea connections are active but peripherals are hung, the FRELAY keyword may be miscoded.

Subarea connections are active but the peripheral connections are not active when FRELAY is coded FRELAY=(PHYSICAL,ANY).

Verify that the microcode level supports receiving both types of frames concurrently. Intensive mode should be run if the NCP resource supports it.

Go to "Step 5. Peripheral or Subarea Network."

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the FRELAY keyword.

Step 17. Contact Support

Contact your frame-relay network support person.

Since the connection was established, the problem is with the frame-relay network and not with the frame-relay definitions. Contact your frame-relay network support person.

Network Flow Control Error Procedure

The following symptoms indicate a network flow control problem:

- Slow response time
- No response for network users.
- Blocked virtual route generic alert was received

Most network flow control problems can be alleviated by tuning the environment: for example, changing NCP or host system generation parameters. Sometimes, hardware or software failures cause flow control problems. This procedure is not specifically designed to help you tune your system, but it does include some tuning suggestions.

The settings you select for transmission group flow control thresholds and virtual route window sizes can significantly affect the performance of your network. The correct value for these settings is determined by your network's configuration and data flow. Use Network Traffic Analysis (NTA) to:

- Optimize your network data flows by identifying SNA traffic congestion problems
- Calculate correct virtual route parameter settings by recommending actions that tune virtual route performance.

For additional detailed discussions of network flow control problems, see the following technical bulletins:

- *"Held VR" Symptom, Problem or Normal Operation*
- *ACF Network Flow Control*
- *VR Performance and Window Size Tuning.*

This procedure helps you diagnose network flow control problems related to NCP. The primary purpose of flow control is to regulate the amount of data entering the network and flowing between network users. Network flow control prevents congestion by managing traffic that is either already in the network or entering the network.

Obtaining Network Flow Control Information

In order to diagnose network flow control problems, you must first know how to obtain network flow control information. This section discusses the 14 ways to collect this information:

- "Locating NCP Flow Control Variables" on page 129
- "Finding a Virtual Route Number for a Session" on page 130
- "Finding Element Addresses for a Resource" on page 130
- "Finding the Physical Path for a Virtual Route" on page 133
- "Checking Traces for Congestion Indicators" on page 134

- "Locating NCP Virtual Route Status" on page 135
- "Determining Whether a Transmission Group Is Hung" on page 136
- "Checking NCP for Transmission Group Problems" on page 136
- "Checking NCP Virtual Route End Points for BPOOL Problems" on page 138
- "Checking NCP Virtual Route End Points for Virtual Route PIU Pool Problems" on page 138
- "Checking NCP Buffer Shortage States" on page 139
- "Locating VTAM Virtual Route Status" on page 142
- "Checking for VTAM Buffer Shortage Problems" on page 142
- "Obtaining Additional Network Flow Control Diagnostic Tools" on page 143.

Documentation Checklist

If the problem results in an NCP flow control failure, use the procedure in Figure 23 on page 117 to collect the following documentation:

- NCP dump
- VTAM I/O trace or TCAM channel I/O interrupt trace
- NCP transmission group trace.

Diagnostic Procedure

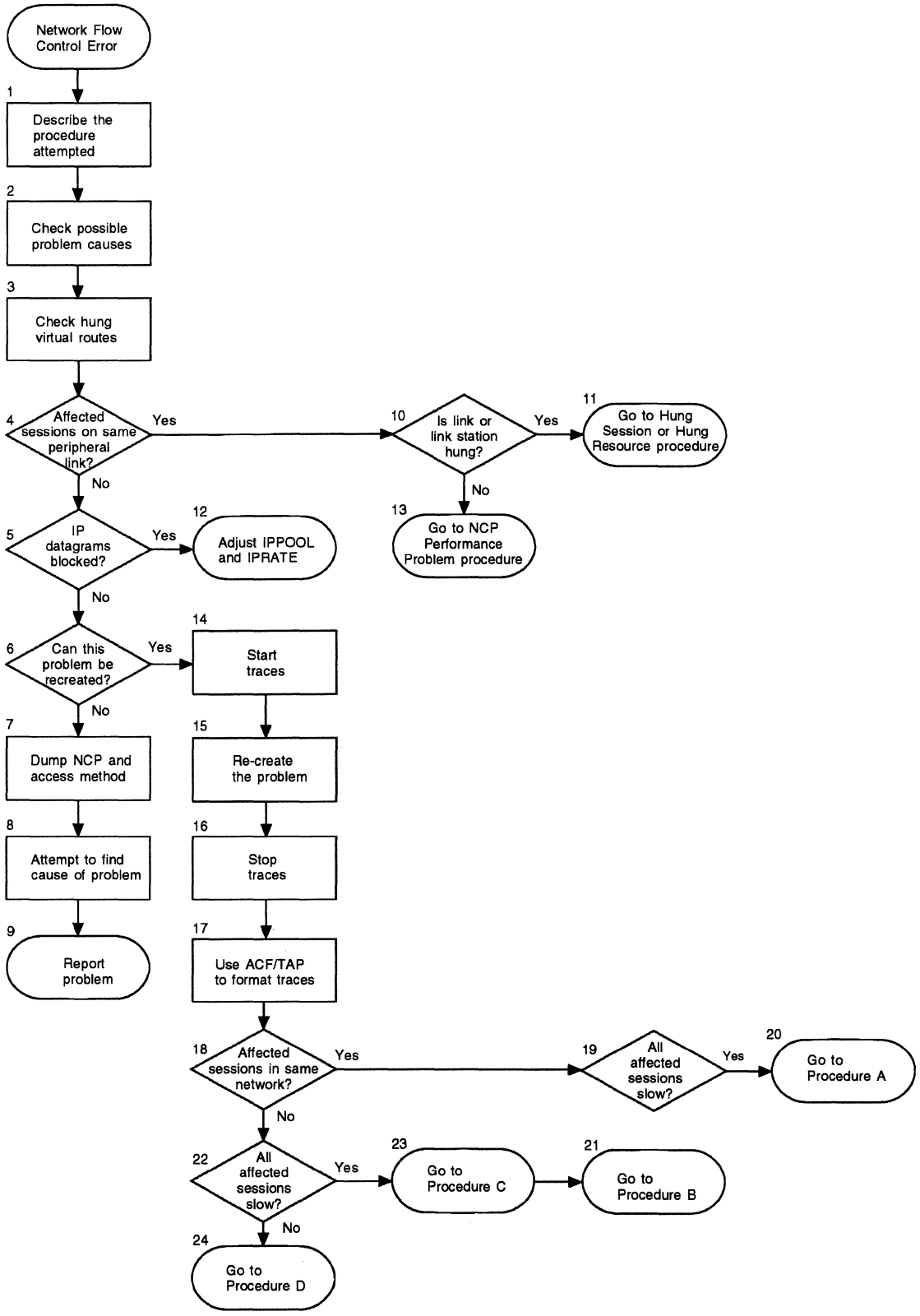


Figure 23. Overview of the Network Flow Control Diagnostic Procedure

Step 1. Describe Procedure Attempted

- Describe the operation you were trying to perform.
- Describe the results you expected.
- Describe the results you received.

Step 2. Check Possible Problem Causes

Answer the following questions:

- Does poor performance occur at a particular time?
- Are there any unique applications running at the time of the problem, such as a batch transfer operation?
- Have you made any recent modifications to NCP generation parameters?
- Have you made any user modifications to TCAM, VTAM, or NCP?

Make a note if any of these questions are relevant.

Step 3. Check Hung Virtual Routes

Information on obtaining virtual route status can be found in "Locating NCP Flow Control Variables" on page 129 and "Locating NCP Virtual Route Status" on page 135.

1. Find the virtual routes for all sessions having problems.

   If a blocked VR generic alert was received, the generic alert identifies the problem VR. See "Interpreting Blocked VR Alerts" on page 130.

2. Find the physical paths taken by these virtual routes. Answer each of the following questions:
   - Do all affected sessions reside within the same network?
   - Do all affected sessions use the same virtual route in any network?
   - Do all affected sessions traverse the same network?
   - Do all affected sessions use the same gateway NCP?
   - Do all affected sessions share the same virtual route end point?
   - Do all affected sessions use the same transmission priority?
3. Determine which sessions are hung.
4. Determine which sessions are experiencing slow response time.

Step 4. Check Physical Link

If all affected sessions are on the same peripheral link, go to "Step 10. Determine if Link is Hung" ; otherwise, go to "Step 5. Check For Discarded IP Datagrams."

Step 5. Check For Discarded IP Datagrams

This section applies to NCP V6R1 and later.

If Internet Protocol (IP) datagrams are not being received across an Ethernet-type LAN, the problem could be either:

- The internet line is congested.
- IP datagrams are coming in faster than NCP allows.

To determine if NCP is causing IP datagrams to be lost, locate the internet congestion information in NCP storage. For information on locating this congestion information, see "NCP IPPOOL and IPRATE Mechanism" on page 350.

If NCP is discarding IP datagrams, go to "Step 12. Adjust IPPOOL and IPRATE Values" ; otherwise, go to "Step 6. Can Problem Be Re-created?."

Step 6. Can Problem Be Re-created?

If the problem can be re-created, go to "Step 14. Start Traces" ; otherwise, go to "Step 7. Dump NCP and Access Method."

Step 7. Dump NCP and Access Method

Dump the following:

- The NCP that owns the problem resource. For information on how to do this, see the following:
  - For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
  - For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
  - For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

  NCP V6R2 and Later: You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. For more information, see the MOSS-E online help.
- The access method that communicates between the host application program and the problem resource. For information on dumping VTAM, see *VTAM Diagnosis*. For TCAM, see *TCAM Diagnosis Guide*.

Step 8. Find Cause of Problem

Look at the formatted NCP dump to find the probable cause of the problem. If you have the NetView program installed in your system, use NetView to find the virtual route that is supporting the failing session.

You can also look at the formatted NCP dump to find the probable cause of your hung condition. Determine whether the cause is a BSC or a start-stop line, cluster, or terminal. For SNA, the resource may be an SDLC link, physical unit, or logical unit. To determine this cause, look at your NCP generation definition or the output of the CRP.

Obtain the element or network address from the reports printed by the CRP. The device page report lists the name of the device and either its element address or its network address. See Chapter 13 for information on CRP reports. If you cannot find copies of these CRP reports, obtain the network or element address of the failing resource from the VTAM RDT control blocks.

Use a VTAM formatted dump to find the RDTE control blocks. The first 8 bytes of RDTE contain the resource name. The element address of the resource is at offset X'16' in RDTE. See *VTAM Diagnosis* for instructions about dumping VTAM. For information on RDT, see the following:

- For MVS, see *VTAM Data Areas for MVS*.
- For VM, see *VTAM Data Areas for VM*.
- For VSE, see *VTAM Data Areas for VSE*.

The network, subarea, and element addresses are located in the RPRE data area (part of RDT).

To verify the bit settings of the status bytes, use *NCP and EP Reference Summary and Data Areas, Volume 1*, to check control block fields. This is especially helpful when the procedure does not tell you what to look for in a byte. Each step in the procedure includes directions for finding the NCP required control blocks.

Step 9. Report Problem

Collect all the information gathered during the diagnostic procedure and report the problem to the IBM Support Center.

Step 10. Determine if Link is Hung

If the link or link station is hung, go to "Step 11. Hung Session or Hung Resource" ; otherwise, go to "Step 13. NCP Performance Problem."

Step 11. Hung Session or Hung Resource

If all affected sessions use the same peripheral link in the NCP virtual route end point and the link or link station is hung, start your investigation with "Hung Session or Hung Resource Procedure" on page 57.

Step 12. Adjust IPPOOL and IPRATE Values

This section applies to NCP V6R1 and later.

The IPPOOL and IPRATE values in your NCP generation definition limit the IP datagram traffic arriving over the token-ring or Ethernet-type LAN. If NCP is discarding IP datagrams because the value coded for IPPOOL is being exceeded, increase the IPPOOL keyword value on the BUILD definition statement. Increasing this value allows more IP traffic; however, be careful not to increase it too much since this could cause IP traffic to monopolize the NCP buffer pool.

If NCP is discarding IP datagrams because the rate at which datagrams are being passed over the token-ring or Ethernet-type LAN is greater than the value specified for the IPRATE keyword on the BUILD definition statement, you can also increase this value. Again, be careful not to receive IP datagrams too quickly. You can omit the IPRATE keyword, but then NCP will depend only on the IPPOOL value when restricting IP traffic.

See *NCP, SSP, and EP Resource Definition Guide* and *NCP, SSP, and EP Resource Definition Reference* for more information on coding the IPPOOL and IPRATE keywords.

Step 13. NCP Performance Problem

If all affected sessions use the same peripheral link in the NCP virtual route end point, but the link or link station is not hung, start your investigation with "NCP Performance Error Procedure" on page 94.

Step 14. Start Traces

From the following list, select the traces applicable to your network and access method: For trace start and stop procedures see the applicable trace information in the *NCP, SSP, and EP Trace Analysis Handbook*.

- VTAM I/O trace or the TCAM I/O interrupt trace: For each virtual route between a host and the NCP that is experiencing problems. Trace the access method as a physical unit (ID=ISTPUS) and trace all of NCP (ID=NCP,E).
- Transmission group trace: At one of the transmission group end points for all transmission groups between NCPs along the virtual route.

Step 15. Re-create Problem

Attempt to re-create the problem.

Step 16. Stop Traces

Run the traces long enough to catch several trips of data flow between both ends of the session then stop the trace.

Step 17. Use ACF/TAP to Format Traces

Use ACF/TAP to format the traces. To find out which reports to format for each of the trace data sets, see "Using Trace Reports to Gather Information" on page 17. For information on using ACF/TAP, see the *NCP, SSP, and EP Trace Analysis Handbook*.

Step 18. Affected Sessions in Same Network?

If all affected sessions are in the same network, go to "Step 19. Are All Sessions Slow?" ; otherwise, go to "Step 22. Are All Sessions Slow?."

Step 19. Are All Sessions Slow?

If all sessions are slow, go to "Step 20. Go to Procedure A" ; otherwise, go to "Step 21. Go to Procedure B."

Step 20. Go to Procedure A

If the affected sessions are experiencing slow response time, go to "Procedure A, Slow Response in Same Network" on page 122.

Step 21. Go to Procedure B

If the affected sessions are hung, go to "Procedure B, Hung Session in Same Network" on page 124.

Step 22. Are All Sessions Slow?

If all sessions are slow, go to "Step 23. Go to Procedure C" ; otherwise, go to "Step 24. Go to Procedure D."

Step 23. Go to Procedure C

If the affected sessions are experiencing slow response time, go to "Procedure C, Slow Sessions Across Networks" on page 126.

Step 24. Go to Procedure D

If the affected sessions are hung, go to "Procedure D, Hung Sessions Across Networks" on page 127

Procedure A, Slow Response in Same Network

A response-time problem indicates that data flow is not completely shut off. The sessions are not hung. If sessions are hung, first investigate the hung session by going to "Procedure B, Hung Session in Same Network" on page 124.

Step 1 Do all affected sessions use the same virtual route? If not, more than one virtual route must be affected, go to Step 4; otherwise, go to Step 2.

Step 2 Are other virtual routes with the same or lower transmission priorities still running problem free to both of the virtual route end points? If not, go to Step 3.

If they are running problem free, there may be congestion because a transmission group is congested along the route that the virtual route uses.

Check traces for congestion indicators. Check for transmission group problems in NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 3 If an NCP is a virtual route end point, start a session using the same or lower priority virtual route ending in that NCP. This can eliminate or confirm the boundary pool (BPOOL) as the problem area. If that virtual route runs correctly, congestion may occur because a transmission group is congested along the route that the virtual route uses.

Check traces for congestion indicators. Check for transmission group problems in NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

If another same or lower priority virtual route does not run smoothly, the slow response time is probably occurring because:

- A transmission group along the route used by the problem virtual route is congested.
- BPOOL thresholds are exceeded in the NCP virtual route end point.

Check traces for congestion indicators. Check for transmission group problems in NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 4 Do all affected sessions end or start at the same virtual route end point? If not, go to Step 8. If so, and the shared virtual route end point is an NCP, go to Step 5. If so and the shared virtual route end point is a host, go to Step 7.

Step 5 Are other virtual routes with the same or lower transmission priority using this NCP as an end point running problem-free? If not or if you are not sure, go to Step 6.

If so, a BPOOL threshold has not been exceeded. Since multiple virtual routes are affected, the problem is probably not a virtual route PIU pool problem unless the virtual routes all feed the same congested peripheral link in NCP. Congestion is probably occurring because the same transmission group along the virtual route being used is congested. Check

traces for congestion indicators. Check for transmission group problems in the NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 6 Because multiple virtual routes are affected, the problem is probably not a virtual route PIU pool problem unless the virtual routes all feed the same congested link at the peripheral node. Start a session using the same or lower priority virtual routes having this NCP as an end point to eliminate or confirm BPOOL as the problem area.

If that virtual route runs correctly, congestion may occur because a transmission group used by all the virtual routes is congested. Check traces for congestion indicators. Check for transmission group problems in the NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

If another same or lower priority virtual route does not run smoothly, the slow response time is probably occurring because:

- A transmission group used by all the virtual routes is congested.
- BPOOL thresholds are exceeded in the NCP virtual route end point.
- NCP has buffer shortage problems.

Check for buffer shortage problems and BPOOL problems in NCP virtual route end point. Check traces for congestion indicators. Check for transmission group problems in common NCPs along the routes. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 7 Since the shared virtual route end point is a host, the response- time problem could be occurring because:

- VTAM has buffer shortage problems.
- VTAM has virtual route problems.
- A transmission group used by all the virtual routes is congested.

Check VTAM for buffer shortages and virtual route status. Check traces for congestion indicators. Check for transmission group problems in common NCPs along the routes. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 8 Do all sessions with response time problems have the same transmission priority? If not, go to Step 9.

If so, a shared transmission group along the routes has congestion. Check traces for congestion indicators. Check for transmission group problems in the common NCPs along the routes. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 9 Do all sessions with the response time problem share the same network node? If not, go to Step 10.

If so, investigate all shared network nodes.

If the network node is an NCP, the response time problem could be occurring because:

- NCP has buffer shortage problems.

- NCP's transmission groups used by all the virtual routes are congested.

Check for buffer shortage problems and transmission group problems in NCP. Check traces for congestion indicators. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

If the network node is a host, the response time problem can occur because:

- VTAM has buffer shortage problems.
- VTAM has virtual route problems.
- A transmission group used by all the virtual routes is congested.

Check VTAM for buffer shortages and virtual route status. Check traces for congestion indicators. Check for transmission group problems in common NCPs along the routes. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 10 If you experience multiple network location failures:

- Check traces for congestion indicators.
- Check all network nodes that are used by many of the virtual routes.

For shared NCP nodes, check for:

- Transmission group congestion problems
- Virtual route PIU pool problems, if the NCP is a virtual route end point
- NCP buffer shortage problems
- NCP BPOOL problems, if the NCP is a virtual route end point.

For shared host nodes, check for:

- VTAM buffer shortage problems
- VTAM virtual route problems.

Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Procedure B, Hung Session in Same Network

Use this procedure if you have a hung session, which means the sessions have stopped entirely. This can occur because of a flow control mechanism failure or a deadlocked network node.

Throughout this procedure, *congestion indicators* are mentioned. One way to check congestion indicators is the NCP blocked virtual routes alert function. NCP starts monitoring virtual routes for congestion if the following conditions occur:

- The virtual route is held.
- NCP withholds virtual-route pacing responses because the virtual-route PIU pool is exhausted.

NCP V7R2: NCP issues a Virtual Route Out-Of-Sequence alert when it detects that PIUs have been received out-of-sequence.

For more information on blocked virtual route alerts, see *NCP and EP Reference.*

Step 1 Do all the hung sessions use the same virtual route? If not, more than one virtual route must be affected. Go to Step 4; otherwise, go to Step 2.

Step 2 Do both virtual route end points have other virtual routes running with sessions that are not hung? If not, go to Step 3.

If so, the hung session problem may occur because there is a hung transmission group along the virtual route.

Check the virtual route status at both virtual route end points. Check traces for congestion indicators. Check for transmission group problems in NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 3 If one virtual route end point has no other virtual routes ending there, you can start a session using a different virtual route ending in that node. If the new session runs smoothly, the hung session problem may occur because there is a hung transmission group along the virtual route.

Check the virtual route status at both virtual route end points. Check traces for congestion indicators. Check for transmission group problems in the NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

If the new session does not run correctly, the hung session problem may occur because:

- A hung transmission group exists along the virtual route.
- A buffer shortage problem exists in the virtual route end point.

Check for buffer shortage problems in the virtual route end point. Check traces for congestion indicators. Check for hung transmission groups in the NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 4 Do all the hung sessions run on virtual routes that share the same virtual route end point? If not, go to Step 7; otherwise, go to Step 5.

Step 5 Is another virtual route to the virtual route end point still running? If not, go to Step 6.

If so, the sessions are probably hung because of a shared hung transmission group along the virtual route. Check the virtual route status at both virtual route end points for all virtual routes. Check traces for congestion indicators. Check for hung transmission groups in the NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 6 The virtual route end point is probably congested due to buffer shortage problems. A shared hung transmission group can also cause the hung session. Check the virtual route status in both virtual route end points for all virtual routes. Check the virtual route end point for buffer shortage problems. Check traces for congestion indicators. Check for hung transmission groups in the NCPs along the route. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 7 Do the hung sessions share the same network nodes? If not, go to Step 8.

If so, investigate all shared network nodes.

If the network node is an NCP, the hung session problem may occur because:

- NCP has buffer shortage problems.
- NCP's transmission groups used by the virtual routes are hung.
- There is a shared hung transmission group.

Check the virtual route status in both virtual route end points for all virtual routes. Check for buffer shortage problems and transmission group problems in NCP. Check traces for congestion indicators. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

If the network node is a host, the hung session problem may occur because:

- VTAM has buffer shortage problems.
- A transmission group used by all the virtual routes is hung.

Check the virtual route status in both virtual route end points for all virtual routes. Check VTAM for performance problems. Check traces for congestion indicators. Check for transmission group problems in the common NCPs along the routes. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 8 You are experiencing multiple network location failures. Sessions are stopped because virtual routes are stopped. Investigate problems on each virtual route separately. Examine virtual route control blocks at both virtual route end points and resolve hung virtual route occurrences as separate problems. Check traces for congestion indicators. Check all network nodes that are used by many of the virtual routes.

For shared NCP nodes, check for:

- Transmission group congestion problems
- Virtual route PIU pool problems if the NCP is a virtual route end point
- NCP buffer shortage problems.

For shared host nodes, check for VTAM buffer shortage problems. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Procedure C, Slow Sessions Across Networks

Use this procedure if all the affected sessions are not in the same network, you have a response-time problem, and the sessions are not hung. If sessions are hung, investigate the hung session problem first by going to "Procedure D, Hung Sessions Across Networks" on page 127.

Step 1 Do all sessions with the response-time problem share the same virtual route in any network? If not, more than one virtual route must be affected. Go to Step 2.

If so, investigate the path of the shared virtual route for problems. Isolate single network problems to investigate the virtual route. Go to "Procedure A, Slow Response in Same Network" on page 122.

Step 2 Each cross-network session uses at least two virtual routes, one in each network through which the session traffic travels. Do all of the affected sessions traverse the same network or share the same set of networks? If not, go to Step 4.

If so, treat the response-time problems of the cross-network sessions as single network problems. If the only shared network node among the affected sessions is the gateway NCP, go to Step 3. If there are not any shared network nodes, go to Step 5. Otherwise, treat the response time problem as a single network problem. Go to Step 4 of "Procedure A, Slow Response in Same Network" on page 122.

Step 3 The slow response time is probably occurring because the gateway NCP has buffer shortage problems or virtual route PIU pool problems. Check for buffer shortage problems in the gateway NCP. Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Step 4 Do all the affected sessions share the same gateway NCP? If not, go to Step 5; otherwise, go to Step 3.

Step 5 If you are experiencing multiple multi-network location failures, investigate the affected routes individually. Check traces for congestion indicators. Check NCP nodes for:

- Transmission group congestion problems
- Virtual route PIU pool problems if NCP is a virtual route end point
- NCP buffer shortage problems
- NCP BPOOL problems if NCP is a virtual route end point.

Check host nodes for:

- VTAM performance problems
- VTAM virtual route problems
- Transmission group congestion problems.

Go to "Procedure E, Locating Information" on page 128 for instructions on checking this information.

Procedure D, Hung Sessions Across Networks

Use this procedure if you have hung sessions and all the hung sessions are not in the same network. In this situation, all the sessions have stopped entirely. Hung sessions can occur because of a flow control mechanism failure or a deadlocked network node.

Step 1 Do all sessions with the response time problem share the same virtual route in any network? If not, more than one virtual route must be affected. Go to Step 2.

If so, investigate the path of the shared virtual route for problems. Isolate single network problems to investigate the virtual route. Go to "Procedure B, Hung Session in Same Network" on page 124.

Step 2 Each cross-network session uses at least two virtual routes, one in each network through which the session traffic travels. Do all of the affected sessions traverse the same network or share the same set of networks? If not, go to Step 4.

If so, treat the problems of the hung cross-network sessions as single network problems. If the only shared network node among the affected sessions is the gateway NCP, go to Step 3. If there are not any shared network nodes, go to Step 5. Otherwise, treat the hung session problems as single network problems. Go to Step 4 of "Procedure B, Hung Session in Same Network" on page 124.

Step 3 The hung sessions are probably occurring because the gateway NCP is having buffer shortage problems, or virtual route PIU pool problems. Check for buffer shortage problems in the gateway NCP. Go to "Procedure E, Locating Information" for instructions on checking this information.

Step 4 Do all the affected sessions share the same gateway NCP? If not, continue to the next step, otherwise, go to Step 3.

Step 5 If you are experiencing multiple multi-network location failures, investigate the affected routes individually. Check traces for congestion indicators. Check NCP nodes for:

- Transmission group congestion problems
- Virtual route PIU pool problems if NCP is a virtual route end point
- NCP buffer shortage problems
- NCP BPOOL problems if NCP is a virtual route end point.

Check host nodes for:

- VTAM performance problems
- VTAM virtual route problems
- Transmission group congestion problems.

Go to "Procedure E, Locating Information" for instructions on checking this information.

Procedure E, Locating Information

The previous procedures requested various items of information in the nodes along the physical path of the virtual routes having difficulty. The procedures for finding this information are discussed in this section. See "Network Flow Control Variables" on page 363 for the location of the flow control variables. Read only the sections suggested by the previous procedure. When you finish reading the following sections, gather all the information. Diagnose the problem to the best of your ability.

Try to alleviate the performance problem by adding more virtual routes or by changing virtual route window sizes, transmission group thresholds, or retry and time-out values in the subarea links. If you still suspect an NCP code problem, call the IBM Support Center. Dump any NCPs in slowdown. For information on dumping NCP, consult the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" and Chapter 11, "Using SSP CLISTs in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

Locating NCP Flow Control Variables

To locate the NCP network flow control variables, you can:

- Use the NetView program to obtain the formatted output from the virtual route status test
- Use the display storage function to check NCP control block fields from the network operator's console
- Use a formatted NCP dump to check NCP control block fields
- Use SSP CLISTs to check control block fields.

Using the NetView Program: This section applies to VTAM V3R2 and later releases and NCP V4R2, NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later.

The virtual route status test in the NetView program allows the collection of congestion data for selected virtual routes; this data is then sent to the NetView program for formatting. Using the NetView program, you can request to collect two types of congestion data:

1. Explicit route congestion data: Collected from each NCP along the virtual route and returned in ER-test-reply and ER-tested PIUs.

   Included in the vector (CV X'20') are:

   NCP's total buffer count
   Number of committed buffers
   Number of free buffers
   Slowdown entry threshold
   Slowdown exit threshold
   CWALL entry threshold.

2. Virtual route congestion data: Collected from the virtual route end points and returned in the route-test response.

   Included in the vector (CV X'3B') are:

   Maximum pacing window size
   Minimum pacing window size
   Current pacing window size
   Next virtual route sequence number to be sent
   Next virtual route sequence number to be received
   Virtual route held indicator
   Virtual route status bytes.

The virtual route status test not only pinpoints the nodes with buffer or virtual route problems but also monitors the status of a specific virtual route. Run the virtual route status test for every virtual route that is used by a session with performance problems. Record all virtual route and buffer information listed above for the selected virtual routes. For more information on the NetView program, see *NetView Operation*.

Using the Display Storage Function: Another way to locate network flow control variables is to use the display storage function from the network operator's console. This function allows you to look at the fields from NCP control blocks. To find the values in these fields, see *VTAM Operation*.

Using a Formatted NCP Dump: For information on dumping NCP, consult the following:

For information on how to locate NCP's flow control variables in an NCP dump, see Appendix A, "Supplementary Network Flow Control Information" on page 343.

Finding a Virtual Route Number for a Session

Besides locating NCP flow control variables, you can also obtain network flow control information by finding a virtual route number in session. You locate this route number from the COS TABLE for the resource having performance problems.

If you have NLDM or the NetView program, issue a request at the operator's console to find the virtual route number for a session. See *NLDM Installation and Operations Guide* or *NetView Operation* for information on finding this number.

Another method for finding the session's virtual route number is to locate the RCB for the NCP resource that owns the device. For information on this procedure, see "RCB—NCP Resource" on page 380. After you locate RCB, find the 2-byte field labeled RCBVVT. Use this to index into VVT to locate the VRB unique to the virtual route. To help locate the field in VRB that contains the virtual route number, see "VVT—NCP Virtual Route Vector Table" on page 368 and "VRB—NCP Virtual Route Block" on page 369.

An easier method for finding the session's virtual route number is to use a trace to locate a PIU for that session. The virtual route number is in the transmission header portion of the PIU. For the offset of this field, see "TH—Transmission Header" on page 364.

Finding Element Addresses for a Resource

Another way to gather network flow control information is by finding the element address for a resource from the reports printed by the CRP. See Chapter 13 for information on the CRP. The CRP utility generates and prints CRP reports. For resources that are dynamically created, the element address will not appear in the CRP.

The device page report lists the device name and element address.

You can also find the resource's element address by locating a PIU for that session in a trace. The element address is in the transmission header portion of the PIU. For the offset of this field, see "TH—Transmission Header" on page 364.

Interpreting Blocked VR Alerts

The VR timer function of **NCP V6R1 and later** can be used to warn the network administrator of potential network flow problems before they affect the user. It provides diagnostic information about virtual routes which are experiencing flow control problems at the same time the problem occurs. The VR timer function lets the network administrator decide what conditions should be considered *congestion*; NCP monitors for those conditions and sends diagnostic information to NetView in the form of 4 different types of blocked VR generic alerts.

1. VR held time limit reached
2. VR pacing withheld time limit reached
3. Held VR deactivation time limit reached
4. VR transmit queue overun

The VR timer function is activated by coding the VRTIMER*n* keyword in the NCP generation. If you do not code VRTIMER*n*, NCP will not send any generic alerts to NetView to report VR congestion problems. For more information about VRTIMER see the *NCP, SSP, and EP Resource Definition Guide* and the *NCP, SSP, and EP Resource Definition Reference*

Following is an example of a blocked VR alert message received on NetView.

```
DESCRIPTION: VR PACING WITHHELD TIME LIMIT REACHED
NPDA-45A        * RECOMMENDED ACTION FOR SELECTED EVENT *

ACTIONS - I008 - PERFORM PROBLEM DETERMINATION PROCEDURE FOR ACTI
          ROUTE E2C5E3C84040404000000000E000000010110
          I136 - CONTACT COMMUNICATIONS SYSTEM PROGRAMMER
          I141 - REPORT THE FOLLOWING STATUS CODE
            02500800001E6608000D000C0000000E
          I258 - REFER TO IBM ACF/NCP PRODUCT DOCUMENTATION FOR
           ADDITIONAL INFORMATION
```

Figure 24. Example of Alert received from NetView

The fields on the `ROUTE E2C5E3C84040404000000000E000000010110` line identify the virtual route which is experiencing congestion. See the following figure for a description of the fields.

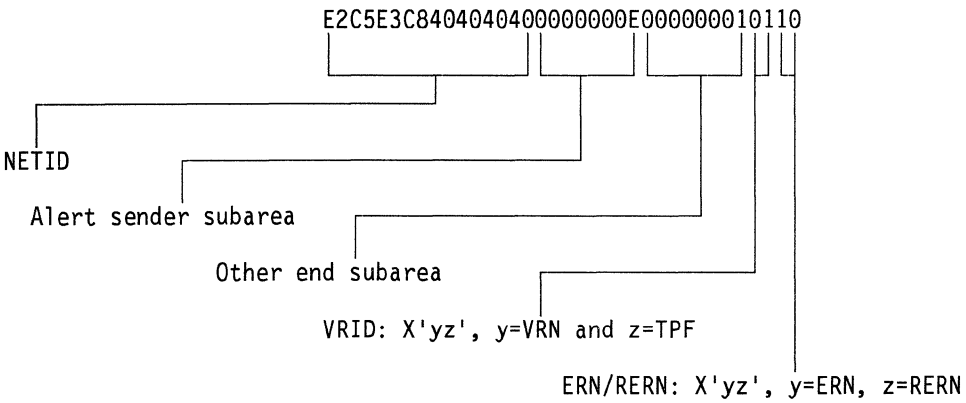


Figure 25. ROUTE Field Descriptions

The fields in the status code, `02500800001E6608000D000C0000000E`, provide flow control information about the virtual route at the time of congestion. This information is similar to the information returned in a route-test response (see "Locating NCP Flow Control Variables" on page 129). See the following figure for a description of the status code fields.

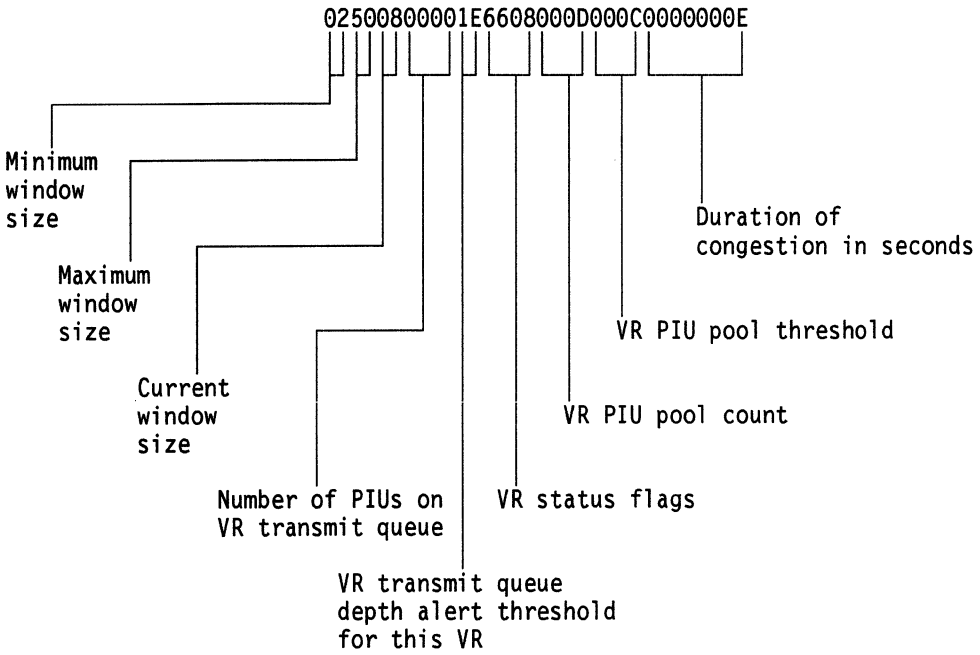
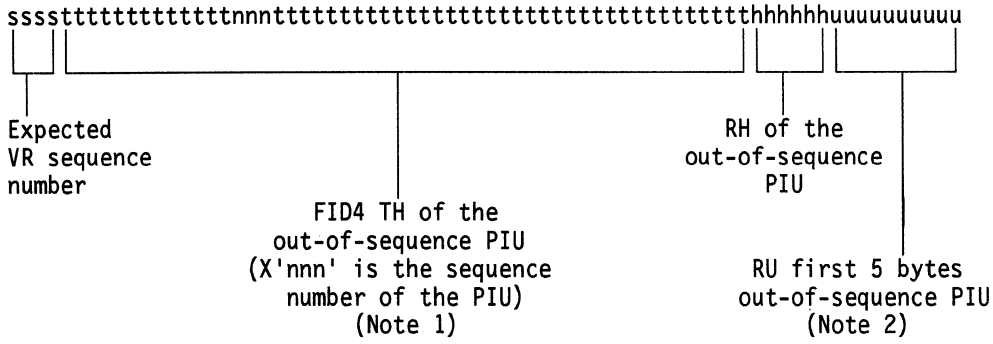


Figure 26. Status Code Field Descriptions

When you have the VR congestion information, continue with the diagnostic procedure to determine the cause of the congestion.

NCP V7R1 and later can also send a VR out-of-sequence alert to NetView. On the NetView screen the VR out-of-sequence alert appears like a VR congestion alert. The only difference is the hex data of the detailed status code. See the following figure for a description of the VR out-of-sequence status code.



Note 1: See *NCP Reference Summary and Data Areas Volume 1*, "PIU (FID4)" for more information.
Note 2: If the RU is less than 5 bytes, the entire RU is shown.

Figure 27. VR Out-of-Sequence Status Code Field Descriptions

When NCP sends a VR out-of-sequence alert indicating a network error occurred causing a PIU to be lost or corrupted, you must deactivate a subarea node or TG to force the VR to be cleaned up. There is no other procedure to recover from this error. If a VR out-of-sequence alert is received contact IBM service for assistance.

For more information on how to parse the entire generic alert see the *NCP and EP Reference Summary and Data Areas Volume 2*, "NMVT RU Formats"

Finding the Physical Path for a Virtual Route

The last way to collect network flow control information is to find the physical path for a virtual route. The physical path for a virtual route uses an explicit route number between the two virtual route end points. To use this method, you must have access to the PATH definition statements in all the subarea nodes along the path. Find the explicit route number from a PATH definition statement in the virtual route activator. Find the subarea of the other end of the virtual route in the DESTSA keyword on the PATH definition statements in the NCP generation definition for the virtual route activator. This is the PATH definition statement that contains the virtual route to explicit route mapping for your virtual route:

1. Find the VRx=y keywords, where x is the virtual route number, and y is the explicit route number for your virtual route.
2. Trace the virtual route's physical path, starting with this PATH definition statement, as follows:
   a. Find the ERy=(w,z) keywords in this PATH definition statement, where y is the explicit route number, and w is the subarea of the next node in the virtual route's physical path.
   b. Find the PATH definition statements in the generation definition for this subarea.
   c. Among those PATH definition statements, find the one that contains the subarea of the other end of the virtual route in the DESTSA keyword.
   d. In this statement, find the ERy=(w,z) keywords, where y is the explicit route number determined earlier, and w is the subarea of the next node in the virtual route's physical path.
   e. Repeat this process until w equals the subarea of the other end of the virtual route.

An example of how to find a virtual route's physical path for a three-hop virtual route, VR1, follows. The virtual route activator is in subarea 1, and the other end of the virtual route is in subarea 12. The PATH definition statement used in the generation definition for the virtual route activator follows.

```
PATH  DESTSA=12,
      ER0=(12,1),ER1=(12,1),ER2=(4,1),ER3=(5,1),
      VR0=1,VR1=2,VR2=3
```

In this definition, VR1 uses ER2. The next node in the physical path is subarea 4. Use the following PATH definition statement in the generation definition for subarea 4:

```
PATH  DESTSA=12,
      ER0=(1,1),ER1=(1,1),ER2=(5,1),ER3=(5,1),
      VR0=1,VR1=2,VR2=3
```

The next node in the physical path is subarea 5. Use the following PATH definition statement in the generation definition for subarea 5:

```
PATH  DESTSA=12,
      ER0=(4,1),ER1=(4,1),ER2=(12,1),ER3=(12,1),
      VR0=1,VR1=2,VR2=3
```

The next node in the physical path is subarea 12, which is the subarea at the other end of the virtual route. Thus, the physical path for this virtual route is:

```
SA1 - SA4 - SA5 - SA12
```

For more information on network flow control and its terminology, see Appendix A, "Supplementary Network Flow Control Information" on page 343.

Checking Traces for Congestion Indicators

Identify the affected session and the direction of each PIU that was traced from an affected session. Uniquely identify the PIUs with the destination and origin subarea and element address fields and the virtual route number and transmission priority fields in the transmission header of the PIU.

For each PIU flowing on the affected sessions, check the settings of these bits, and note the ones that have these bits on:

PCI	Program-controlled interrupt for CCU
CWI	Change window indicator
VRPRQ	Virtual route pacing request
VRPRS	Virtual route pacing response
CWRI	Change window reset indicator
RWI	Reset window indicator

If the PCI bit is on in the last PIU flowing in a particular direction, the virtual route is held in the origin subarea. Check the status of the virtual route in that subarea.

If the CWI bit is on, the transmission group counter for that priority virtual route exceeded its threshold in an NCP along the route. Isolate the transmission group having problems by finding the point at which the CWI bit was turned on for that PIU.

When the receiving virtual route end point receives the PIU with the CWI bit on, it sets the CWRI bit on in the next VRPRS bit to the sending virtual route end point. This instructs the virtual route end point to lower the window size by one. NCP also turns on the CWRI bit in the next VRPRS bit when it has either BPOOL or virtual route PIU pool problems. If the CWRI bit is on in a VRPRS bit and none of the previous PIUs flowing in the opposite direction had a CWI bit on, check the BPOOL and virtual route PIU pool for the virtual route in the VRPRS sender's subarea for problems.

Both VTAM and NCP can turn on the RWI bit in PIUs flowing in the direction opposite to the problem direction. The virtual route end point receiving a RWI sets its window size to the minimum. NCP virtual route end points turn on the RWI bit when it has BPOOL problems. If the composite transmission group counter exceeds its threshold in one of the NCPs along the virtual route's physical path, the RWI severe congestion indicator is set on in every PIU flowing in the opposite direction on this particular transmission group. When VTAM enters a buffer shortage state, the RWI bit is set on in PIUs for all virtual routes as soon as I/O buffers are available. If the RWI bit is on in a PIU, isolate the problem to either the origin virtual route end point or a congested transmission group along the way. If the PIU has the RWI bit on when it left the virtual route sender, the problem is a BPOOL problem if NCP is the virtual route sender, or a VTAM buffer shortage problem if VTAM is the virtual route sender.

For information on using the VRWS trace analysis program to troubleshoot virtual route problems, see the heading "Trouble Shooting Problems with Analysis Program" in the technical bulletin *VR Performance and Window Size Tuning.*

Locating NCP Virtual Route Status

The easiest way to get NCP virtual route status is to obtain the NetView program's formatted output from the virtual route status test function. See "Locating NCP Flow Control Variables" on page 129 for more detailed information.

You can also get a virtual route's status from VRB in NCP. Note the following fields when this information is requested:

VRBLNID	Local network ID (LNID)
VRBOSAF	Subarea on the other end of the virtual route
VRBTGBP	Pointer to the TGB for this virtual route
VRBFCFLG	Virtual route status flags Bit 0 on: Send VRPRS Bit 1 on: VRPRS received Bit 2 on: VRPRQ received Bit 3 on: Virtual route held Bit 4 on: Notify blocked tasks Bit 5 on: Set CWRI on next VRPRS Bit 6 on: Withholding VRPRSs Bit 7 on: Set RWI on next PIU sent
VRBFLAGS	Virtual route status flags Bit 0 on: Virtual route inoperative Bit 2 on: Session outage notification triggered Bit 3 on: Internal virtual route Bit 4 on: Virtual route deactivation responsibility Bit 6 on: Virtual route out of sequence (discarding PIUs)
VRBPIUCT	Number of buffers allocated to this virtual route
VRBVRID	VRID (virtual route number and transmission priority) Bits 0–3: Virtual route number Bits 6–7: Transmission priority
VRBXMTQC	Number of PIUs on virtual route transmit queue
VRBMWIND	Virtual route maximum window size
VRBWIND	Virtual route current window size
VRBWCNT	Virtual route window count
VRBVVTI	VVT index
VRBLWIND	Virtual route minimum window size
VRBFTHRS	Virtual route Inbound PIU threshold
VRBFCNT	Virtual route Inbound PIU count

Each VRB represents a unique virtual route and transmission priority to a given subarea in a given network. To find a particular VRB, use the RCB method outlined for finding the virtual route number of a session. See "Obtaining Network Flow Control Information" on page 115. Check each VRB matching virtual route number, subarea on the other side and LNID.

Determining Whether a Transmission Group Is Hung

If a transmission group along a virtual route is hung or broken, Route Test commands are not completed. If a transmission group is hung, all virtual routes appear as held. Other network virtual routes may also show as held. However, a hung virtual route cannot stop a route test because the route test, if issued correctly, runs at the explicit route level. A successful route test indicates the route's transmission groups are operational and all route elements at the physical level are working properly. A hung transmission group or network node can cause an unsuccessful route test. For information on the route test, see *NetView Operation*.

The Route Test PIU must be sent by VTAM to either VTAM's own physical unit or to NCP. This PIU does flow on a virtual route if sent to NCP. However, the Route Test PIU does not test the route; the route is tested by the Explicit Route Test PIUs that start their flow at the node receiving the Route Test PIU. The Explicit Route Test PIUs flow on the explicit route and stop at every node along the route.

If the route you wish to test starts at a VTAM node, instruct VTAM to send the Route Test to itself. If the route is between two NCPs, find a VTAM host that owns the NCP in the native network and has a SSCP-NCP session that does not ride on a held virtual route. In fact, it is highly recommended that all SSCP-NCP sessions use high- priority virtual routes that no other session uses. There can be eight high-priority virtual routes between any two subarea nodes.

If the Route Test is completed successfully, your transmission group is not hung. Any hung virtual routes result from a different flow control problem, such as virtual route PIU pool or buffer shortage. If the Route Test does not complete and the NCP to which the Route Test PIU was sent is not in slowdown, a transmission group along the virtual route is probably hung. Isolate the hung transmission group using traces and gather the information requested under the next procedure.

Checking NCP for Transmission Group Problems

If a transmission group is congested, the traces should show congestion indicators. Also, check fields in TGB, FLB, and SCB for signs of transmission group problems. If the byte count for each virtual route priority or the composite byte count is at or near its threshold, the transmission group is or will be congested. If the transmission group out of sequence bit is on and there are many PIUs on the FLB Resequence Queue, transmission group resequencing is either slowing down the traffic rate or can be causing the transmission group to hang, if there is a lost PIU.

If link error recovery occurs while the transmission group is in the sweep function, the transmission group may hang. This happens because the sweep cannot end until all individual link queues of the transmission group are empty. A link in error recovery does not have an empty queue until error recovery finishes. This problem can be compounded if the REPLYTO keyword on the GROUP definition statement or the RETRIES keyword on the SDLCST, MTALCST, LINE, or PU definition statement is specified too high for the link. The sweep function is invoked when:

- The sweep indicator is on in the FID4 transmission header for special PIUs.
- RNR is received on a link.
- The transmission group sequence number field is rolled over.

If you suspect that the transmission group is hung, check the FLB for an indication of the sweep function, rollover conditions, and out of sequence. Check the SCBs for link error recovery indications and RNR received.

For transmission group problems, check these fields in the TGB:

TGBDLCP	Pointer to the FLB
TGBTCNT	Total inbound byte count
TGBHCNT	High-priority inbound-byte count
TGBSTATE	Transmission group state definitions
TGBMCNT	Medium-priority inbound-byte count
TGBLCNT	Low-priority inbound-byte count
TGBTTHR	Total byte count threshold
TGBHTHR	High-priority byte-count threshold
TGBMTHR	Medium-priority byte-count threshold
TGBLTHR	Low-priority byte-count threshold

For transmission group problems, check these fields in the FLB:

FLBRQCB	Head pointer for resequence queue
FLBRQCB	Tail pointer for resequence queue
FLBXQCB	Head pointer for transmit queue
FLBXQCB	Tail pointer for transmit queue
FLBSOC	Station operative count
FLBSCBP	Pointer to the first SCB
FLBSTF	State flags Bit 2 on: Transmission group in sweep mode Bit 3 on: Special FIDF PIU expected
FLBNRO	Next sequence number for outbound PIUs
FLBNRI	Next expected sequence number from inbound PIUs
FLBSTFC	State flags Bit 0 on: Transmission group out of sequence

For transmission group problems, check the fields in the SCB:

SCBOCF	Station service seeking output control flags Bit 0 on: Output skip bit Bit 2 on: RNR received Bit 3 on: Second-level error recovery procedure (ERP) pause in progress Bit 6 on: RNR re-poll
SCBERS	First error encountered
SCBRTCNT	ERP retry counts
SCBSRTLR	Second-level retry limit
SCB2ERPT	Second-level ERP timeout value
SCBERPT	Second-level ERP pause
SCBTRTCT	Total retry counter
SCBSRTR	Total retries threshold value
SCBFLPF	Chain pointer to next SCB on FLB
SCBFLST	Status of multilink transmission group Bit 0 on: Station ready to send

The SCB chain starts in FLB, and the next-in-chain pointers are in the SCBs. First get TGB from VRB; then get FLB from TGB. The VVT points to VRB. Each VRB represents a unique virtual route and transmission priority to a given subarea in a given network. To find a particular VRB, you can use the RCB method outlined for finding the virtual route number of a session. See "Obtaining Network Flow Control Information" on page 115. You could also check each VRB's matching virtual route number, subarea on the other side and LNID.

Checking NCP Virtual Route End Points for BPOOL Problems

NCP BPOOL problems cause congestion indicators to be set in PIUs flowing to the other virtual route end point. Changing window sizes on virtual routes slows virtual route traffic ending in the NCP depending on the virtual route's priority and the level of buffers left in the BPOOL, as listed below:

- For virtual routes with TPN=0:

  Set the CWRI bit when BPOOL is at 62.5% threshold
  Set the RWI bit when BPOOL is at 75% threshold.

- For virtual routes with TPN=1:

  Set the CWRI bit when BPOOL is at 75% threshold
  Set the RWI bit when BPOOL is at 87.5% threshold.

- For virtual routes with TPN=2:

  Set the CWRI bit when BPOOL is at 87.5% threshold
  Set the RWI bit when BPOOL is full.

The BPOOL control block (BPB) maintains the BPOOL count. The virtual route receiver increments and decrements the count when a PIU is moved to the channel hold queue or to the link-outstanding queue or when a PIU is released. Get the number of buffers currently in the BPOOL and the threshold values from BPB when BPOOL problems are suspected.

Checking NCP Virtual Route End Points for Virtual Route PIU Pool Problems

The virtual route PIU pool operates by counting PIUs. NCP keeps count of the number of PIUs that arrived at an NCP over a given virtual route in VRB. This count is incremented only for PIUs whose destination is a SNA peripheral station, a virtual physical unit or logical unit, a GWNLB, or NCP itself. PIUs destined to SNA logical units or BSC or start-stop terminals are not included. The count is decremented when the PIU is moved to the channel-hold queue or to the link-outstanding queue, or the PIU is released. This count is compared to a threshold value kept in VRB for each virtual route.

The two possible actions that can be taken when the number of PIUs from a virtual route exceeds its threshold are:

- When virtual route PIU pool count is greater than the threshold, withhold the VRPRS bit.
- When virtual route PIU pool count is greater than the threshold + 6, withhold the VRPRS bit and set the CWRI bit on next the VRPRS bit sent.

Get the virtual route PIU pool count and the threshold value from VRB when you suspect virtual route PIU pool problems.

The VVT points to VRB. Each VRB represents a unique virtual route and transmission priority to a given subarea in a given network. To find a particular VRB, you can use the RCB method outlined for finding the virtual route number of a session. See "Obtaining Network Flow Control Information" on page 115. Alternately, check each VRB matching virtual route number, subarea on the other side and LNID.

See "Interpreting Blocked VR Alerts" on page 130 for an example of a blocked VR alert message received on NetView.

Checking NCP Buffer Shortage States

There are four ways to determine if NCP is in a buffer shortage state:

1. You will receive a message at the host console saying that NCP entered the slowdown state.
2. **NCP V4R2, NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later**: You can check the formatted output of the NetView program's virtual route status test function.
3. You can use the display storage function at the network operator's console to check NCP bit settings.
4. You can look at fields in a dump of NCP.

All methods of obtaining this information are discussed in "Obtaining Network Flow Control Information" on page 115. The location of the fields in the NCP control blocks are given in "Network Flow Control Variables" on page 363. The following fields should be noted:

SYSBUFCT—HWE + X'00'	Total number of buffers in the communication controller
SYSBUFCT—FAX + X'5C'	Total number of buffers in the communication controller (for NCP V6R2 and later)
SYSBPQBC—HWE + X'02'	Exit slowdown threshold
SYSBPQBC—FAX + X'60'	Exit slowdown threshold (for NCP V6R2 and later)
SYSBPCW—XDH + X'50'	CWALL entry threshold
SYSBPGCC—XDH + X'52'	Global committed buffers count
SYSBPGCC—XDA + X'08'	Global committed buffers count (for NCP V6R2 and later)
SYSBPCBC—XDH + X'54'	Current free buffer count
SYSBPCBC—XDA + X'14'	Current free buffer count (for NCP V6R2 and later)
SYSBPTBC—XDH + X'56'	Slowdown entry threshold
SYSBPTBC—XDA + X'18'	Slowdown entry threshold (for NCP V6R2 and later)
SYSIPCP—FAX + X'3C'	Current IPPOOL buffer counts Maximum number of buffers allowed in the IPPOOL is at IPC + X'00'. Current number of buffers allocated in the IPPOOL is at IPC + X'04'.
SYSPRELC—XDB + X'03'	System PRELEASE count
SYSDSPM—XDB + X'04'	System dispatch mask Bit 0 on: System in CWALL Bit 1 on: System in pseudo-slowdown
SYSBPSTS—XDB + X'09'	Buffer pool and network status Bit 0 on: System in slowdown Bit 3 on: SDLC RR/RNR polling control during slowdown Bit 4 on: SLOWDOWN ENTRY message required

When NCP buffer problems occur, your IBM Support Center may ask you to account for the current buffer usage, including their locations. Use a formatted dump or SSP CLIST to do this.

You can use the SSP CLIST IFWILSOW to calculate the current buffer usage. You will not need to count the number of buffers on the QCB as described in the next paragraph.

To locate all buffers that are not free (that is, buffers currently in use), you must first understand how the buffers are chained on an NCP queue. The queue, represented by a QCB, has a head and tail pointer. The head pointer is the address of the first buffer of the first PIU on the QCB. The tail pointer is the address of the first buffer of the last PIU on the QCB. The first buffer of each PIU contains a pointer to the next PIU on the QCB. Each buffer also has a pointer to the next buffer in the PIU. Using these buffer pointers, you can count the number of buffers on the QCB. These pointers are contained in fullword fields at the following locations:

QCB + X'00'	QCB head pointer
QCB + X'04'	QCB tail pointer
buffer + X'08'	Next PIU pointer
buffer + X'00'	Next buffer in the PIU pointer

You can find all the control blocks containing the queues in a formatted NCP dump. The layout of a formatted dump is given in "Formatted Dump Contents" on page 195. You should mainly be concerned with finding the QCBs containing long buffer chains. The following is a list of the QCBs that you can check:

- Active virtual routes:

VRB + X'1A'	VRB transmit queue PIU count (2 bytes)
VRB + X'20'	VRB transmit QCB

- Active channels:

CAB EXT + X'00'	Channel-intermediate queue
CAB EXT + X'0C'	Channel-hold queue

- Active subarea links and stations:

LKB + X'00'	Link-input queue
ACB + X'14'	Block-overrun queue head pointer
ACB + X'20'	Block-overrun queue tail pointer
SCB + X'00'	Link-inbound queue
SCB + X'18'	Link-outbound queue
SCB + X'20'	Link-outstanding queue

- Transmission groups:

TGB + X'00'	Transmission group inbound queue head pointer (no tail pointer)
FLB + X'00'	Multilink resequence QCB
FLB + X'18'	Multilink transmit QCB
FLB + X'32'	FLB status

  If these queues contain many buffers, the user should note the bit settings in this byte.

- Active peripheral SNA links, physical units, and logical units:

LKB + X'00'	Link input QCB
ACB + X'14'	Block-overrun queue head pointer
ACB + X'20'	Block-overrun queue tail pointer
CUB + X'00'	Link-inbound QCB
CUB + X'18'	Link-outbound queue
CUB + X'20'	Link-outstanding queue
CUB + X'78'	SSCP-PU CPM out process QCB (for NCP V4R1 (VSE) and NCP V4R2)
LUB + X'00'	SSCP-LU CPM out process QCB (for NCP V4R1 (VSE) and NCP V4R2)
BSB + X'00'	SSCP-LU CPM out process QCB (for NCP V5R3 (VSE), NCP V5R4 and later, this is the SSCP-LU BSB)
LUB + X'1C'	LU-LU CPM out process QCB (for NCP V4R1 (VSE) and NCP V4R2)
BSB + X'00'	LU-LU CPM out process QCB (for NCP V5R3 (VSE), NCP V5R4 and later, this is an LU-LU BSB)

- Active pre-SNA links and devices:

LCB + X'00'	Line input/output QCB
ACB + X'14'	Block-overrun queue head pointer
ACB + X'20'	Block-overrun queue tail pointer
DVB + X'00'	Device work QCB
DVB + X'10'	Device input QCB

- Active standard attachment facility resources:

NLB + X'00'	NLB QCB
NLX + X'00'	NLX QCB

- Active gateway resources:

NLB + X'00'	NLB QCB
NLX + X'00'	NLX QCB
RCB + X'08'	RCB VRL pointer

By checking these queues, you can locate most of the buffers. You can also investigate these additional areas:

- If there are many buffers on the virtual route transmit QCB, see if the virtual route is held (VRB + X'14' bit 3 on). Bit 3 on indicates a problem with the other end point of the virtual route. The subarea node on the other side of the virtual route owes this NCP a virtual route pacing response.
- If there are many buffers on an LU-LU CPM out-process QCB, check for a pacing response outstanding from the device LUB + X'48' bit 4 on (for NCP V4R1 (VSE) and NCP V4R2). This may indicate a terminal problem. Otherwise, you may need to specify V-pacing in the application because the application is flooding NCP with data to the device.
- If no outstanding pacing response from the terminal occurs, check the task dispatching priority of this QCB at LUB + X'2C' (for NCP V4R1 (VSE) and NCP V4R2). If the first 3 bits in this byte are 0's (B'000x xxxx'), BATCH=YES was specified on the logical unit definition statement in the NCP generation definition. This is the lowest priority. Therefore, this QCB is dispatched when no higher-priority tasks are pending. Also, there may be many PIUs on the

LUBAPQ queue in LUB if NCP received RNR from the physical unit (for NCP V4R1 (VSE) and NCP V4R2).

If you defined DYNPOOL on the BUILD statement, you are using dynamic control block, and you may have buffers allocatted to these control blocks. The count is locted in the GPB (GPB + X'20'). Also, the GPA for each pool will indicate the number being used for that pool. See the *NCP and EP Reference* for more information on the dynamic controls and thier buffers.

Locating VTAM Virtual Route Status

The easiest way to locate VTAM virtual route status is to obtain the NetView program's formatted output from the virtual route status test function. See "Locating NCP Flow Control Variables" on page 129 for more detailed information.

You can also find the virtual route status from the virtual route control block (VRBLK) in a formatted VTAM dump. Record the following fields when this information is requested:

VRBVRN	Virtual route number
VRBPACNT	Virtual route window count
VRBMINWS	Virtual route minimum window size
VRBMAXWS	Virtual route maximum window size
VR status	Virtual route status byte for TP=0
	Bit 1 on: VRPRQ (Virtual route pacing request received)
	Bit 2 on: VRPRS (Virtual route pacing response received)
	Bit 3 on: CWI (Change-window indicator received)
	Bit 4 on: CWRI (Change-window reset required)
	Bit 5 on: RWI (Reset window required)
	Bit 6 on: Virtual route held
	Bit 7 on: Some half-session queues must be checked for held sessions
VRBDSTSA	Subarea of the other end of the virtual route.

The virtual route number and the subarea on the other side of the virtual route can uniquely identify the VRBLKs.

Checking for VTAM Buffer Shortage Problems

VTAM has fewer local flow control mechanisms than NCP. VTAM's flow control mechanisms all center on the usage of the I/O buffer pool and CPU utilization. See "VTAM Buffer Management Mechanisms" on page 360 for a complete description of these mechanisms. *VTAM Customization* and *VTAM Network Implementation Guide* discuss how to tune these buffer pool parameters.

VTAM displays and traces can be used to identify VTAM buffer shortage problems. See *VTAM Diagnosis* for more information about diagnosing VTAM performance problems.

Obtaining Additional Network Flow Control Diagnostic Tools

There are two additional tools for diagnosing network flow control problems:

- The virtual route window size (VRWS) trace analysis program
- The upper bound window size (UBWS) program.

For a description of these tools and their uses, see the technical bulletin *Virtual Route Performance and Window Size Tuning*.

To obtain these tools, contact your IBM system engineer.

Part 2. Diagnostic Aids

Chapter 4. Gathering NCP-Collected Trace and Performance Data

In addition to using traces and performance data that are collected by the host to diagnose NCP errors, you can use traces that are collected and stored in NCP. These traces help you examine the data flow through your network and isolate and identify the source of network problems. If you determine the problem is in NCP, you can use these aids to gather information to help IBM Support Center representatives when they assist you in solving the problem.

This chapter describes how to diagnose the problem using the following NCP-collected traces:

- Channel adapter trace
- Channel adapter input/output (IOH) trace
- Address trace
- Dispatcher trace
- Supervisor call trace
- PERFORM trace
- Branch trace
- Conditional branch trace (IBM 3745-130, 3745-150, 3745-160, 3745-170, and 3745 17A)
- NTRI snap trace
- Connectivity subsystem snap trace
- IP snap trace
- Parameter status area (PSA) trace
- Adapter control block (ACB) trace
- Synchronous Data Link Control (SDLC) I/O level 3 trace.

In addition, this chapter documents other diagnostic aids, such as:

- Dynamic panel displays
- Line test
- Commands to request NCP information.

This chapter describes these diagnostic aids and tells you when and how to use them, start and stop them, and obtain them.

Channel Adapter Trace

The channel adapter trace is a maintenance and debugging tool that traces channel adapter interrupts. It stores the communication controller's external registers related to the channel adapter in a trace table. If you suspect a channel adapter hardware error, this trace can monitor the control and data interrupts at the channel interface. This trace can also monitor all channel external registers. You can record all interrupts or only certain types of interrupts.

NCP V6R2 and Later: Use the connectivity subsystem adapter trace to trace ESCON adapters. For more information, see the *NCP, SSP, and EP Trace Analysis Handbook*

Use the channel adapter trace when you have an NCP loop problem or when an abend suggests a channel adapter failure. You can also use the channel adapter trace to monitor channel STATUS/SENSE commands and to monitor path information units (PIUs) if no response is returned. The channel adapter trace is also useful for investigating problems with channel links.

Starting the Channel Adapter Trace (IBM 3720 and 3725)

If you are using NCP V5R3 (VSE) or NCP V5R4, this section applies to the IBM 3720 Communication Controller; if you are using NCP V4R1 (VSE), NCP V4R2, or NCP V4R3.1, this section applies to the IBM 3725 Communication Controller.

To include the channel adapter trace with NCP, specify CATRACE=(YES,*count*) on the BUILD definition statement. The *count* parameter indicates the number of entries you want in the trace table. Specify any number from 1 to 255. A minimum of 10 is recommended. For more information on the BUILD definition statement, see *NCP, SSP, and EP Resource Definition Reference*.

Start the channel adapter trace from the IBM 3720 or 3725 maintenance and operator subsystem (MOSS) operator keyboard. To start and stop the channel adapter trace:

1. Press the CCU FNCTN key on the MOSS keyboard. The screen displays the CCU options list. Enter 6 to specify the data exchange function; then press the SEND key.
2. If the IBM 3720 or 3725 is running NCP/PEP, put the communication controller in NCP mode by entering 7 in the FUNCTION field and C in the DATA field; then press the SEND key.
3. The screen displays the three fields: DATA, FUNCTION, and CCU LVL3. Enter xx06 in the DATA field, where xx is the channel adapter identification, and enter 1 in the FUNCTION field and Y in the CCU LVL3 field; then press the SEND key.

   Only the following bits are valid for channel adapter identification from X'01' to X'3F':

   ```
      ...1  CA1
      ..1.  CA2
      .1..  CA3
      1...  CA4
     1....  CA5
    1.....  CA6
   ```

   An IBM 3720 Communication Controller has two channel adapters; an IBM 3720 or 3725 that operates remotely has no channel adapters.
4. To deactivate the trace, enter 0006 in the DATA field, 1 in the FUNCTION field, and Y in the CCU LVL3 field; then press the SEND key.

Starting the Channel Adapter Trace (IBM 3745)

You can start or stop the channel adapter trace with the NCP line trace. No trace records are returned because the trace table is kept in NCP storage. Find the trace table in the formatted section of the NCP dump.

NCP V5R3 (VSE), NCP V5R4 and later: To include the channel adapter trace with NCP, specify CATRACE=(YES,*count*) on the BUILD definition statement. The *count* parameter indicates the number of entries you want in the trace table. Specify any number from 1 to 512. A minimum of 50 is recommended.

For additional information on starting and stopping the channel adapter trace for the IBM 3745 Communication Controller, see *Advanced Operations Guide* for the IBM 3745 Communication Controller.

Obtaining the Channel Adapter Trace

After the activate or deactivate channel adapter trace is complete and all processing for the session has ended, use a dump of the communication controller to analyze the channel adapter trace table for any channel activity. The trace table is contained in the dump. For directions on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

Identifier characters CTRC mark the beginning of the trace table in the dump. The pointer to the trace table can be found in the Extended Halfword Direct Addressable (HWE) control block. For more information on the channel adapter trace table and how to analyze its contents, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

Channel Adapter IOH Trace

The channel adapter input/output (IOH) trace is a maintenance and debugging tool that traces channel adapter IOHs. This trace allows service personnel to trace the sequence of IOHs issued to the channel adapters and determines the failure point of a channel operation.

NCP V6R2 and Later: Use the connectivity subsystem adapter trace to trace ESCON adapters. For more information, see the *NCP, SSP, and EP Trace Analysis Handbook*

Use the channel adapter IOH trace whenever you have an activate or deactivate problem, a hung resource or session problem, or a message problem. You may want to use the channel adapter IOH trace any time that you would also want to run a channel command word (CCW) trace.

Starting the Channel Adapter IOH Trace

The channel adapter IOH trace runs continually for the available channel adapters if you code CAIOTRC=YES on the BUILD definition statement. If you code CAIOTRC=NO on the BUILD definition statement, only the IOHs that travel on the less frequently used paths through the channel code are traced for all of the channel adapters.

Setting bit 0 on at offset X'2C' in the RTRCATRC field of XDB activates the channel adapter IOH trace in the level 3 router, but IOHs that travel on the most heavily used paths through the channel code are not traced. See Table 8 for details about the RTRCATRC field.

Table 8. RTRCATRC Field of XDB

Byte Expansion	Bit Name	Meaning
1...	RTRIOHT	Use the trace version (CXDNCPT, CXDPEPT, CXDNEOT) of the level 3 router. These routers trace their IOHs and decide if the IOHs for the current level 3 channel adapter interrupt will be traced. If set to 0, use the other level 3 routers (CXDNCP, CXDPEP, CXDNEO). These routers do not trace any of their IOHs and do not perform the selective channel adapter IOH trace.
.1..	CAIOHTR	Tells the IOH trace routine (CXCAIOHT) to trace this IOH. CXCAIOHT gets control only if the CAIO macro is coded with YES as its fifth parameter (default is YES).
..1.	RTRCAVL	The IOH trace is restricted to one channel adapter as specified in the low 4 bits of RTRCATRC.
...x	reserved	
.... xyyy		Channel adapter address of single channel adapter to trace. x = bus bit: 0 for IOC1 and 1 for IOC2, yyy = channel adapter select bits

To selectively trace IOHs for one channel adapter for either case (CAIOTRC=YES or CAIOTRC=NO), set this XDB field as follows:

```
1010 XYYY    where:  X = IOC bus      and   YYY = Channel adapter select
                     0 = IOC1                     bits (relative position
                     1 = IOC2                     of the channel adapter
                                                  on the bus, 0–7)
```

Run the channel adapter IOH trace against channel adapters selected from Table 9 on page 155.

Table 9. Channel Adapter Trace Selection

Communication Controller	Channel Adapter Position	XYYY
3745	1	X'8'
	2	X'9'
	3	X'A'
	4	X'B'
	5	X'0'
	6	X'1'
	7	X'2'
	8	X'3'
	9	X'C'
	10	X'D'
	11	X'E'
	12	X'F'
	13	X'4'
	14	X'5'
	15	X'6'
	16	X'7'
3725	1	X'0'
	2	X'1'
	3	X'2'
	4	X'3'
	5	X'4'
	6	X'5'
3720	1	X'0'
	2	X'1'

Obtaining the Channel Adapter IOH Trace

After the channel adapter IOH trace is complete and all processing for the session has ended, dump the communication controller to analyze the channel adapter trace table for any channel activity. The trace table is contained in the dump. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

  You can also use the SSP CLIST IFWITRAC to display the contents of the table online. See Chapter 11 for more information on SSP CLISTs.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

For more information on the channel adapter trace table and how to analyze its contents, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

Address Trace

The address trace lets you record the contents of selected areas of communication controller storage, general registers, and external registers at each successive interrupt. You can select any combination of up to four external registers, general registers, and storage fullwords, and record their contents each time data is loaded from or stored in a specific storage address at a designated program level. You can also specify a displacement to the register or address so that the contents of the areas at these displaced locations are also recorded. Transfer the recorded

data to the host through the dump program. Monitor suspected errors within NCP by recording external registers and changes to storage addresses. Because of the complexity of the address trace, you should use it only under the direction of the IBM Support Center representative.

Starting the Address Trace

To include the address trace with NCP, specify TRACE=(YES,*size*) on the BUILD definition statement. The *size* parameter indicates the number of entries allowed in the trace table. For more information on the BUILD definition statement, see *NCP, SSP, and EP Resource Definition Reference.*

NCP V5R3 (VSE), NCP V5R4 and later. For the IBM 3745, specify a number from 10 to 512.

Start the address trace from the communication controller's MOSS operator keyboard. To start and stop the address trace, use *Problem Determination and Extended Services* or *Advanced Operations Guide* for your IBM communication controller.

Obtaining the Address Trace

Display the address trace table using the display long function or show it as part of an NCP dump. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

For information on the display long function, see "Dynamic Display of Registers and Storage" on page 169.

To find the address trace table in an unformatted NCP dump, look for the SYSATBP field in the extended halfword direct addressable (HWE) control block. This field points to the address trace block (ATB) in the dump. The address of the address trace table is at location X'10' in ATB. For information on ATB and the address trace table, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

To find the address trace in a formatted NCP dump, see "Formatted Dump Contents" on page 195.

Dispatcher Trace

The dispatcher trace table contains a record of the control flow activity in NCP program level 5. This control flow activity includes the following items:

- The active queue control block (QCB) dispatched, including:

  The time it was dispatched
  The first element on the queue
  The task entry point.

- The address where each call is issued
- The address of the subtask branched to by the subtask sequencer
- The address of the subtask branched to by the control router

- The address where a supervisor call (SVC) is issued
- PERFORM trace information (see "PERFORM Trace (IBM 3720 and 3745)" on page 160).

Use the dispatcher trace when you have an NCP abend, loop, or performance problem.

Starting the Dispatcher Trace

The dispatcher trace starts automatically when you load NCP into the communication controller and stops if an abend occurs. You can also stop it by turning on bit 2 (X'20') in the RTRB17 field at offset X'36' in the byte direct addressable storage (XDB) control block or by setting a trap in the NCP code.

To do a selective dispatcher trace:

1. Choose the low and high physical storage addresses of the QCBs to be traced.
2. Use the superzap utility for your operating system to alter the load address instruction located at DSPX000 + X'04', with the low address determined in Step 1.
3. Use the superzap utility for your operating system to alter the load address instruction located at DSPX000 + X'0C', with the high address determined in Step 1.

Because of the complexity of a selective dispatcher trace, use it only under the direction of your IBM Support Center.

Obtaining the Dispatcher Trace

The NCP dump contains the dispatcher trace table. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

  You can use the SSP CLIST IFWITRAC to display the contents of the table online. See Chapter 11 for more information on SSP CLISTs.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

To find the trace table in an unformatted NCP dump, find entry DSPX000 in the link-edit map or in HWE at HWE + X'78'. This gives you the address of the table in the dump. Otherwise, scan the interpreted area of the dump for symbols CXDCG01 and CXDCG02. The identifier characters DISP and TEND are between these two symbols. DISP marks the beginning of the trace table in the dump; TEND marks the end. The fullword before DISP contains the address of the current entry in the table. The dispatcher trace table appears after the control blocks.

NCP V4R1 (VSE), NCP V4R2, NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later: To find the dispatcher trace in a formatted NCP dump, see "Formatted Dump Contents" on page 195.

For more information on the dispatcher trace table and how to analyze its contents, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

If the dispatcher trace was stopped by a trap in NCP code, view the trace output with the NCP dynamic storage display facility. See Chapter 1 for information on how to use the dynamic storage display facility.

Supervisor Call Trace

The supervisor call (SVC) trace records the data from level 5 registers for every supervisor call macro issued from program level 5. In a wrap mode, the trace table records the last 75 SVCs from level 5 registers 0, 3, 5, and 7. You can also trace level 5 registers 1, 2, 4, and 6 if you select the trace-all-registers option.

NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later: The SVC trace is part of the dispatcher trace.

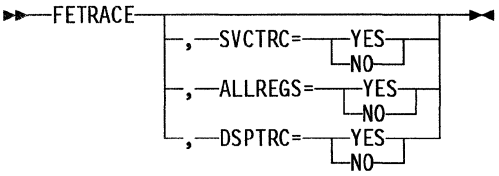
Use the SVC trace when you have an NCP abend, loop, or performance problem. Because of the complexity of an SVC trace, you should use it only under the direction of your IBM Support Center.

Starting the SVC Trace

The SVC trace is started by coding the FETRACE macro in your user-written communication controller code or turning on RTRSVCT bit 4 (X'08') in the RTRB17 field of the byte addressable area. Correlate the SVC trace entries and the dispatcher trace entries with the TIMTENTH field from XDH, which both traces use as a relative time. In order for the SVC trace to run, the dispatcher trace must be active.

For the selective SVC trace, the default addresses traced are X'00000' to X'FFFFF'. The default values immediately follow the SVCTBEND. Zap SYSCG001 to change the defaults.

To trace all level 5 registers (0, 3, 5, 7, 1, 2, 4, 6), change the beginning blank character (X'40') to X'00' or code the FETRACE macro. The FETRACE macro controls the SVC and dispatcher traces. Use the macro to turn the supervisor trace off or on, tracing only registers.



SVCTRC=YES
Specifies that the SVC trace is to be turned on. If SVCTRC equals YES, DSPTRC must also equal YES.

SVCTRC=NO
Specifies that the SVC trace is to be turned off. If SVCTRC equals NO, DSPTRC must also equal NO.

ALLREGS=YES
Specifies that all level 5 registers are to be traced in the SVC trace entries.

ALLREGS=NO
Specifies that only registers 0, 3, 5, and 7 are to be traced when the SVC trace is on.

DSPRTC=YES
Specifies that the dispatcher trace is to be turned on. If DSPTRC equals YES, SVCTRC must also equal YES.

DSPRTC=NO
Specifies that the dispatcher trace is to be turned off. If DSPTRC equals NO, SVCTRC must also equal NO.

You can also code these SVC macro bits directly as follows:

byte 0,1	Always set to 0070
byte 2	Always A9 (set to the SVC code)
byte 3	bit 0 1 = turn SVC trace on, 0 = turn SVC trace off
bit 1	1 = trace all registers, 0 = trace only 0,3,5,7
bit 5	1 = turn dispatcher trace on, 0 = undefined
bit 6	1 = turn dispatcher trace off, 0 = undefined

Examples:

- To turn SVC trace on, tracing all registers, code: 0070 A9C0.
- To turn SVC trace on, tracing only registers 0, 3, 5, and 7, code: 0070 A984.
- To turn SVC trace off, code: 0070 A900.
- For a snapshot of all registers, code: 0070 A904 0070 A900.
- To turn dispatcher trace on, code: 0070 A904.
- To turn dispatcher trace off, code: 0070 A902.

Obtaining the SVC Trace

The NCP dump contains the SVC trace table. For information on obtaining an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

To find the trace table in the dump, look for the SVC in the interpreted portion of the dump. The current entry is in the fullword preceding the SVC. The current entry represents the next entry to be used by the SVC trace. Identify the end of the trace with the SVCTBEND. You can also find the SVC trace table by locating the CXASVCTR entry in the link-edit map. For the IBM 3720, 3725, and 3745 Communication Controllers, the SVC trace table appears after the control blocks.

For more information on the SVC trace table, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

PERFORM Trace (IBM 3720 and 3745)

This section applies to NCP V5R3 (VSE), NCP V5R4 and later.

The PERFORM trace records the execution of the PERFORM macro (a subroutine linkage utility). This trace is activated under program control and is shown as part of the dispatcher trace table. The *P* character in the first byte distinguishes PERFORM trace entries in the dispatcher trace table.

Branch Trace

The branch trace lets you trace all branches that occur while NCP is active. The trace table shows the come-from level and address and the go-to level and address for each branch, including no-op instructions. Trace options enable you to:

- Trace by interrupt level and storage address range
- Stop the trace when the trace table is full
- Wrap the trace table
- Stop on an address compare interrupt (see the *Problem Determination and Extended Services* for your IBM communication controller for information on the address compare function).

Use the branch trace when you have an NCP abend, loop, or performance problem. Because of added cycles on each branch instruction, the branch trace may affect performance.

To trace the initialization sequence, start the branch trace before initializing NCP and specify the branch trace buffer from the MOSS keyboard. Refer to *Problem Determination and Extended Services* for your IBM communication controller for the branch trace buffer allocation procedure. Be sure the load module for the trace table is the same as the load module specified during NCP generation.

Starting the Branch Trace

To use the branch trace with NCP, specify BRANCH=*count* on the BUILD definition statement. The *count* parameter is entered as a number, 100 to 8000, that specifies the buffer size for the branch trace. Its default is 100.

Start the branch trace from the communication controller MOSS keyboard. To start and stop the branch trace, use the procedure found in *Problem Determination and Extended Services* or *Advanced Operations Guide* for your IBM communication controller.

Obtaining the Branch Trace

Display the branch trace by using the MOSS display long function or show it as part of the NCP dump. For information on the display long function, see "Dynamic Display of Registers and Storage" on page 169. For information on the how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

You can also use the SSP CLIST IFWITRAC to display the contents of the branch trace table online. See Chapter 11 for more information on SSP CLISTs.

- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

If you show the branch trace as part of the NCP dump, get a formatted printout of the branch trace table by specifying the formatted option on the DUMP control statement. To find the branch trace in a formatted NCP dump, see "Formatted Dump Contents" on page 195.

To find the branch trace table (BTT) in an unformatted NCP dump, look at location X'6E8' for the pointer to XDA.

NCP V6R1 and Later: To find BTT in an unformatted NCP dump, look at location X'38' for the pointer to XDA.

NCP V4R1 (VSE) and NCP V4R2: The control program information table (CPIT) is at offset X'3C' in XDA.

NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later: The CPIT pointer is at offset X'10' in FAX. Find the FAX pointer at offset X'78' of XDA. For more information on the CPIT pointer and BTT, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

BTT may contain extra entries that are difficult to interpret. Refer to *Problem Determination and Extended Services* for your IBM communication controller for a complete description of the extra entries in the trace table.

Conditional Branch Trace (IBM 3745-130, 3745-150, 3745-160, 3745-170 and 17A)

The conditional branch trace (CBT) aids in debugging. It lets you trace limited areas of code, including lower-priority level 5 code. For example, with CBT you can trace a single module rather than a complete level of NCP. CBT also lets you trace several parts of the code based on a condition. For example, you can trace a mailbox path by starting CBT on the IN mailbox and stopping it on the OUT mailbox for the specified modules. You cannot run conditional branch trace and branch trace simultaneously.

CBT is offered as an option on the IBM 3745-130, 3745-150, 3745-160, 3745-170, or 3745-17A Communication Controller MOSS keyboard to change only the default options of the conditional branch according to your specification (fewer interrupt levels, for example). The CBT default values are:

- All interrupt levels
- Branch trace buffer wrap
- Lower address = 0000000
- Upper address = maximum.

Use CBT when you have an NCP abend, loop, or performance problem.

Starting and Stopping CBT

To start CBT, turn on the CBT-is-active bit in XDB and issue the OUT X'76' with bit 0.2 on.

To stop CBT, turn off the CBT-is-active bit in XDB and issue the OUT X'76' with bit 0.2 off.

Obtaining CBT

Display CBT by using the MOSS display long function or show it as part of the NCP dump. For information on the display long function, see "Dynamic Display of Registers and Storage" on page 169. For information on the dump facilities, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

  You can also use the SSP CLIST IFWITRAC to display CBT online. See Chapter 11 for more information on SSP CLISTs.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

If you show CBT as part of the NCP dump, get a formatted printout of the CBT table by specifying the formatted option on the DUMP control statement. To find the CBT table in a formatted NCP dump, see "Formatted Dump Contents" on page 195.

To find the CBT table in an unformatted NCP dump, look at location X'6E8' for the pointer to XDA.

NCP V6R1 and Later: To find the CBT table in an unformatted NCP dump, look at location X'38' for the pointer to XDA.

NCP V5R3 (VSE), NCP V5R4 and later: The CPIT pointer is at offset X'10' in FAX. Find the FAX pointer at offset X'78' of XDA. For more information on the CPIT and the conditional BTT, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

The CBT table may contain extra entries that are difficult to interpret. Refer to *Problem Determination and Extended Services* for your IBM communication controller for a complete description of the extra entries in this trace table.

NTRI Snap Trace

The snap trace provides diagnostic information for NTRI, and frame- relay resources. It traces module flow during the execution of NTRI or NCP and captures certain information during the execution of each module.

Use the snap trace when you have an abend, an endless loop, or a performance problem related to NTRI or frame-relay resources. Running this trace may have an adverse effect on NCP performance.

Starting the 3745 NTRI Snap Trace

To start the snap trace from the MOSS console while NCP is running, use the MOSS display and alter (DAL) function and perform the following steps:

1. Display X'06E9'. This contains the 24-bit address of XDA.

   NCP V6R1 and Later: Display X'39' for the 24-bit address of XDA.
2. Display XDA+X'79'. This contains the 24-bit address of FAX.
3. Display FAX+X'25'. This contains the 24-bit address of AVB.
4. Display AVB+X'00'. This address should contain X'C1E5'.
5. Display AVB+X'08'. This contains an 8-bit field in which bit 0 is the snap-trace-active bit. To start the snap trace, alter the 8-bit field to change bit 0 from 0 to 1 (for example, change X'00' to X'80'). To stop the snap trace, change bit 0 from 1 to 0.

NCP V5R3 (VSE) and NCP V5R4: To start the snap trace when you load NCP, code the NTRISNAP keyword on the BUILD definition statement.

NCP V6R1 and Later: To start the snap trace when you load NCP, code the NCPTRACE keyword on the BUILD definition statement. For more information on the BUILD definition statement, see *NCP, SSP, and EP Resource Definition Reference.*

Obtaining the NTRI Snap Trace

The information collected by the snap trace is contained in the communication controller storage. Dump the controller storage and specify the formatted option on the dump control statement to format the output of the snap trace. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

  You can also use the SSP CLIST IFWISNAP to display the output of the trace online. See Chapter 11 for more information on SSP CLISTs.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

3746 Model 900 Connectivity Subsystem Snap Trace

This section applies to NCP V6R2 and later.

The 3746 Model 900 Connectivity Subsystem (CSS) Snap Trace provides diagnostic information for 3746 Model 900 resources. It traces the main 3746 Model 900 interface control blocks (NPSAs, LPSAs, NDPSAs, and LDPSAs), but does not trace any data associated with the NDPSAs or LDPSAs. You can trace four types of interfaces using the connectivity subsystem snap trace:

- Physical line
- Target processor (adapter)
- Controller bus processor
- Trace.

You can trace one or any combination of interface types. The traces are associated with the physical line you select by specifying a line address. If you select the physical line interface type, this address specifies the line to be traced. If you select the target processor or controller bus processor interface type, the processor associated with the line you specify is traced. If you select the trace interface type, the connectivity subsystem adapter trace and connectivity subsystem line trace interface for the line you specify is traced.

Starting the Connectivity Subsystem Snap Trace

Activate the Connectivity Subsystem Snap Trace from the MOSS console using the MOSS data exchange function. The data you send to the CCU control program has the following format:

```
DATA ==> aabbbb          FUNCTION ==> 04          CCU LVL3 ==>
```

where:

aa is a bit string interpreted as follows:

0001	Start the trace
0000	Stop the trace
000. ...1	Physical line interface
000. ..1.	Target processor interface
000. .1..	Controller bus processor interface
000. 1...	Trace interface

bbbb is the line address as coded on ADDRESS keyword on the LINE definition statement. For more information on the LINE definition statement, see *NCP, SSP, and EP Resource Definition Reference.*

If you want all 3746 Model 900 lines to be traced, enter the line address of FFFF.

For example, to start a connectivity subsystem snap trace for the physical line and target processor interfaces associated with line 2432, enter the 6 digits 132432. To start the snap trace for the same interfaces associated with all the 3746 Model 900 lines, enter the 6 digits 13FFFF.

Refer to the operations manual for your communication controller for more information on the MOSS data exchange function.

Obtaining the Connectivity Subsystem Snap Trace

The connectivity subsystem snap trace data is written to NCP storage and can be found in the formatted section of the NCP dump. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

The connectivity subsystem snap trace wraps when the trace table is full, which can cause trace data to be lost.

IP Snap Trace

This section applies to NCP V7R1 and later.

The IP Snap Trace is used only by IBM support personnel. Do not start this trace unless instructed to by IBM support personnel.

The IP Snap Trace is used when you have problems with:

- The IP routing tables
- Datagrams that are being discarded by NCP
- IP interfaces that are not coming active
- A loop in NCP caused by the IP component.

Running this trace may have an adverse effect on NCP performance.

Starting the IP Snap Trace

To start the IP snap trace when you load NCP, code the IPSNAP keyword on the BUILD definition statement. For more information on the BUILD definition statement, see *NCP, SSP, and EP Resource Definition Reference*.

To start the IP snap trace from the MOSS console while NCP is running, use the MOSS display and alter (DAL) function and perform the following steps:

1. Display X'39' for the 24-bit address of XDA.
2. Display XDA+X'79'. This contains the 24-bit address of FAX.
3. Display FAX+X'31'. This contains the 24-bit address of RDA.
4. Display AVB+X'00'. This contains an 8-bit field in which bit 0 is the snap-trace-active bit. To start the IP snap trace, alter the following:
   - For datagram, change bit 6 from 0 to 1
   - For routing, change bit 7 from 0 to 1

Obtaining the IP Snap Trace

The information collected by the IP snap trace is contained in the communication controller storage. Dump the controller storage and specify the formatted option on the dump control statement to format the output of the IP snap trace. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

Parameter Status Area Trace

The parameter status area (PSA) is a high-level interface between NCP and the communication controller scanners. Commands, command modifiers, and status information are passed back and forth through PSA.

The PSA trace records 4 bytes of data from the status area of PSA for a designated scanner line. This trace is always enabled; when an abnormal level 2 interrupt from the scanner occurs, the trace saves 4 bytes of data for up to four different interrupts on the scanner line before the data wraps. This trace data is stored at

the end of the adapter control block extension (AXB) and is up to 16 bytes in length.

Use the PSA trace when you suspect you have an NCP problem, a scanner problem, an NCP abend, or a loop problem.

NCP V6R2 and Later: NCP does not support the data link control (DLC) and parameter status area (PSA) traces for 3746 Model 900 lines. The function provided by the DLC trace is provided by the connectivity subsystem snap trace for 3746 Model 900 lines.

Starting the PSA Trace

The PSA trace automatically traces on interrupts when the PSA service request bit is off because of an abnormal level 2 interrupt. Enable the trace for all level 2 interrupts by no-oping the first IF test on the service bit in the level 2 router routine (CXDCG00). It will not be enabled if the service bit is on, which occurs if there is a normal level 2 interrupt.

Obtaining the PSA Trace

The NCP dump includes the PSA trace data. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

To locate the PSA trace data in an NCP dump, find AXB in a formatted dump. The last 18 bytes include 16 bytes of data and 2 bytes of control fields. Starting at offset X'2C' (NCP V4R1, VSE) or offset X'30' (NCP V4R2, NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4 and later), there are 16 bytes of data and a 1-byte control field.

Adapter Control Block Trace

The adapter control block (ACB) contains line control information and the status of I/O operations for links. The ACB trace records 4 bytes of data from select ACB fields, depending on the type of data link control (DLC) operation being traced. This trace is always enabled, and the eight trace entries of 4 bytes each are stored in the ACB trace table (ATT) control block. ATT contains a trace entry control field in the first byte. This trace entry control field contains a value that indicates in which entry the next trace data is to be stored.

Use the ACB trace when you want to examine the status of I/O operations on a line.

NCP V6R2 and Later: You can use the ACT trace to trace 3746 Model 900 lines. NCP traces identical fields for both 3746 Model 900 lines and non-3746 Model 900 lines at the same trace points.

You can use ATT to trace 3746 Model 900 lines. NCP records ATT trace records for 3746 Model 900 lines for the following situations:

- When the results of a line I/O command are passed to level 5

- When a reset command is issued to the I/O layer
- When a level-3 interrupt is processed.

NCP always records the CCBEND1 field. It may also record fields containing information about a diagnostic code, and a command or reason.

Starting the ACB Trace

The ACB trace is always enabled, and no operator action is required to start or stop the trace.

Obtaining the ACB Trace

The NCP dump includes ATT. For information on how to get an NCP dump, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."

  You can also use the SSP CLIST IFWINAU to display ATT online. See Chapter 11 for more information on SSP CLISTs.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

To locate ATT in an NCP dump, find AXB in a formatted dump. ATT immediately follows AXB, and the entry control field is labeled appropriately.

SDLC I/O Level 3 Trace

The Synchronous Data Link Control (SDLC) I/O level 3 trace is an optional diagnostic and debugging aid that stores certain fields from ACB and station control block (SCB) in a trace table. This can be done for all ACBs, a single ACB, or for a pair of ACBs in the case of a duplex line. You identify the ACBs to be traced by storing (or super-zapping) the ACB addresses into the two fullwords at label ACBPTRS in the CXECEND CSECT (module CXDCG0D). If only one ACB is to be traced, its address should be stored at the first fullword leaving the second unaltered. If all ACBs are to be traced, a fullword of 0's should be stored at the second fullword. The number of trace entries is 40 and cannot be specified by the user.

Each time a level 3 line I/O interrupt occurs for an SDLC line (CXECEND executes), an entry is placed in the trace table. Refer to *NCP and EP Reference Summary and Data Areas*, Volume 1, for a detailed description of the trace table controls and entry format.

Dynamic Panel Displays (IBM 3720)

The IBM 3720 Communication Controller allows you to dynamically display information on lines, registers, and storage. The MOSS functions allow you to display on the MOSS screen:

- A line test
- Contents of local storage registers (LSRs), work registers, or central control unit (CCU) input registers
- Controller storage

- Address or branch trace data.

Use dynamic panel displays to check information in the external registers or to change or check storage values at a specific time.

For further information on dynamic panel displays on the IBM 3720 Communication Controller, see *3720/3721 Communication Controller Extended Services Guide*.

Dynamic Panel Displays (IBM 3725)

The IBM 3725 Communication Controller allows you to dynamically display information on lines, registers, and storage. The MOSS functions allow you to display on the MOSS screen:

- A line interface block, with selectable information on serial data, secondary control, set mode, control, modem-in, modem-out, and hexadecimal mask
- Contents of LSRs, work registers, or CCU input registers
- 16 or 128 bytes of communication controller storage
- Address or branch trace data.

Use dynamic panel displays to check information in the external registers or to change or check storage values at a specific time.

Dynamic Panel Displays (IBM 3745)

The IBM 3745 Communication Controller allows you to dynamically display information on lines, registers, and storage. The MOSS functions allow you to display on the MOSS screen:

- A line test
- Contents of LSRs, work registers, or CCU input registers
- Communication controller storage
- Address or branch trace data.

Use dynamic panel displays when you want to check information in the external registers or when you want to change or check storage values at a specific time.

For further information on dynamic panel displays on the IBM 3745 Communication Controller, see *IBM 3745 Advanced Operations Guide*.

Starting Dynamic Panel Displays

The following sections describe how to start and stop the different types of dynamic displays.

Dynamic Display of the Line Interface Block

To display a line interface block for a specific line:

1. Press the SELN AREA key on the MOSS keyboard, enter an L, press the SEND key, enter a 2, and then press the SEND key again.
2. The screen displays a prompt for the line interface address. Enter either the decimal or hexadecimal line address; then press the SEND key. (To distin-

guish between a decimal and hexadecimal line interface address, enter an X as the first character of the hexadecimal address.)

For the correlation of the line address and the line interface address, see *3725 Problem Determination and Extended Services* or your communication controller's equivalent book.

3. The screen lists the fields that can be displayed. To suppress a field, enter an N before the field. When you have selected all fields or if you wish to display all fields without selecting specific ones, press the SEND key.
4. The screen displays the field options list again, but shows the position number of any bit turned on in a selected field. For bit meanings and additional information on running this function, see the *3725 Problem Determination and Extended Services* or your communication controller's equivalent book.

Dynamic Display of Registers and Storage

Two functions can display registers and storage: the display/alter function and the display long function.

The display/alter function allows you to display the following:

- 16 bytes of CCU storage
- 4 LSRs
- All work registers.

The display long function allows you to display the following:

- 128 bytes of CCU storage
- 16 LSRs
- All work registers
- CCU input registers from X'70' to X'7F'.

For information on the differences between the display/alter and display long functions, see the *3725 Communication Controller Problem Determination and Extended Services*.

Display/Alter Function for the IBM 3725 Communication Controller

To use the display/alter function to display registers or storage, use the following procedure:

1. Press the CCU FNCTN key on the MOSS keyboard. The screen displays the CCU options list. Enter 3 to specify the display alter function; then press the SEND key.
2. The screen now displays three options: S (storage address), L (LSRs), and W (work registers).
   - To display storage, enter Sxxxxxx, where S indicates storage and xxxxxx is the storage address. The screen displays 16 bytes of storage, beginning with the requested address.
   - To display LSRs, enter Lxx, where L indicates LSRs and xx is the first LSR to be displayed. The screen displays four local storage registers, beginning with the requested register.

- To display work registers 0–3, enter a W only. To display work registers 4–7, press the PF5 key.

After you select the option, press the SEND key.

Ten lines per screen are available to display storage and registers. This means that more than one option can be displayed on the same screen. For additional information on the display/alter function, see the *3725 Communication Controller Problem Determination and Extended Services*.

Display Long Function for the IBM 3725 Communication Controller

To use the display long function to display storage or registers, use the following procedure:

1. Press the CCU FNCTN key on the MOSS keyboard. The screen displays the CCU options list. Enter 4 to specify the display long function; then press the SEND key.
2. The screen now displays four options: S (storage), L (LSRs), W (work registers), and I (input registers).
   - To display 128 bytes of storage, enter Sxxxxxx, where S indicates storage and xxxxxx is the beginning storage address.
   - To display 16 LSRs, enter Lxx, where L indicates LSRs and xx is the first register to be displayed.
   - To display all work registers, enter a W only.
   - To display input registers X'71' to X'7F', enter an I only.

   After selecting an option, press the SEND key.

For additional information on the display long function, see the *3725 Communication Controller Problem Determination and Extended Services*.

Line Test

The line test allows you to address, poll, dial, and transmit to, or receive from a terminal. You can perform tests of lines, modems, and terminals without an active application program running in the host. Start a test by entering variables through the MOSS operator keyboard of the communication controller. The panel-initiated line tests can be run for EP only if the test function is included in EP by specifying TEST=YES on the BUILD definition statement. The line test is not supported for NTRI.

Use the line test when you want to check lines, modems, and terminals to verify proper operation in your network.

Online testing is a user-selected option that provides an IBM Support Center representative with an online test and the customer with a tool to aid in problem recovery. OLTT tests binary synchronous communication (BSC) and start-stop devices. OLTT is controlled by terminal online test executive program (TOLTEP), which resides in the access method. OLTT is included in the system by specifying OLT=YES on the BUILD definition statement.

The host initiates an online test by sending an Execute Test PIU to NCP. The request/response unit (RU) portion of the path information unit (PIU) contains the actual test and its parameters (see Figure 28 on page 172). If the test is an OLTT, the execute test processor (CXDKETP) converts the PIU to a test basic transmission unit (BTU) and passes it to the OLTT initiator (CXDHOLTI) to be decoded and executed.

The first PIU must be a Test with Contact or a Test with Contact and Disconnect. This establishes a session with the line or device to be tested. Once the session is established, the TEST NORMAL and TEST WITH DISCONNECT commands are valid. The last OLTT command must be either a TEST WITH DISCONNECT or TEST WITH CONTACT AND DISCONNECT command. If the device or line indicated in the first TEST command is already in session, the PIU is returned to the host with a syntax error indicated.

The actual test consists of interpretive commands contained in the text portion of the command PIU. These commands are so arranged by the executive program that they constitute a sort of subprogram, which is executed by NCP to perform the online test. The interpretive commands allow NCP to set and test counters and flags in the online test control block, to branch to another interpretive command in the series associated with this test, to start I/O operations for the device requesting the test, and so on.

Interpretive commands are executed sequentially beginning with the first command, which is assigned the relative address X'0000'. The TERMINATE command, always the last interpretive command in the test, stops execution of the command chain. When the interpretive TERMINATE command is reached, NCP returns a PIU to the host indicating normal completion of the TEST command.

The host executive program can request that data be returned before a test ends by including a RETURN DATA command among the interpretive commands. When NCP encounters this command, it builds a PIU with the appropriate system response. The PIU text is the last block of test data received (optional) and the OLTT control block.

The OLTT control block is the primary means of communication between the test and NCP. The control block is formatted in a buffer when a TEST WITH CONTACT or TEST WITH CONTACT AND DISCONNECT command is received. It is released from the buffer on completion of a TEST WITH DISCONNECT or TEST WITH CONTACT AND DISCONNECT command. The interpretive TERMINATE command also releases the control block from the buffer if the proper modifier is specified.

Prefix	Request Code	Element Address	BTU Command	BTU Modifier	BTU Response	Text

Request Code — X'01' (execute test)

Element Address — Element address of the resource to be tested.

BTU Command — X'03'

BTU Modifier

X'00'	Test device normal
X'01'	Test device with contact
X'02'	Test device with disconnect
X'03'	Test device with contact and disconnect

BTU Response — See *NCP and EP Reference Summary and Data Areas*, Volume 2.

Text — Interpretive commands.

Figure 28. Request/Response Unit of a Test PIU

OLTT Operating Procedure Summary

The following steps summarize the online terminal testing procedure for BSC and start-stop terminals.

1. Operator at control terminal enters a test request (indicated by 99999 for start-stop devices and by SOH %/ for BSC devices).
2. NCP recognizes the test request and indicates in the BTU that this is a TEST REQUEST message.
3. VTAM recognizes the test request and calls TOLTEP.
4. TOLTEP decodes the request and sends the control terminal the message `ENTER DEV/TEST/OPT`.
5. The control terminal operator enters the name of the desired test and device to be tested. It can be the control terminal.

Steps 4 and 5 go through NCP but are not apparent to it.

6. TOLTEP calls the appropriate online terminal test routine.
7. The OLTT routine constructs a FID1 PIU WITH A TEST WITH CONTACT command and generates a string of interpretive commands using macro expansions.
8. VTAM sends the PIU to NCP.
9. NCP recognizes the TEST WITH CONTACT command, establishes a session with the test terminal, and builds an OLTT control block.
10. NCP executes the interpretive commands and receives and stores the test data from the terminal.
11. NCP returns the test data and OLTT control block to VTAM for each interpretive RETURN DATA AND TERMINATE command.

12. The OLTT routine analyzes the test data and determines the next step to be taken.
13. The OLTT builds and sends the next TEST command PIU to NCP.
14. Steps 10 through 13 are repeated until the OLTT routine sends a TEST WITH DISCONNECT command. A TEST WITH DISCONNECT command can be the only TEST command sent.
15. NCP ends the session with the test device and returns the final test data to the host.
16. The host sends pertinent test results to the control terminal.

OLTT Interpretive Commands

The following interpretive commands are listed in descending order by operation code.

Branch If Flags Off

Branches to the specified interpretive command if the indicated flags are off.

Byte	Bit	Description
0	0–3	Operation code. X'E'
	4–7	Flag byte select. Specifies which of the 16 flag bytes in the OLTT control block to set.
1		Flag bit select. Specifies the bits in the selected fields to test.
2–3		Branch address. The displacement from the beginning of the interpretive command string to the command to be branched to.

Branch If Flags On

Branches to the specified interpretive command if the indicated flags are on.

Byte	Bit	Description
0	0–3	Operation code. X'D'
	4–7	Flag byte select. Specifies which of the 16 flag bytes in the OLTT control block to test.
1		Flag bit select. Specifies the bits in the selected fields to test.
2–3		Branch address. The displacement from the beginning of the interpretive command string to the command to be branched to.

Decrement Counter

Decrements the specified counter in the OLTT control block by one and tests for a 0 or negative value. The fifth byte of the 16 flag bytes is reserved for counter status.

Byte	Bit	Description
0	0–3	Operation code. X'C'
	4–7	Counter select. Specifies which of the 16 counters in the OLTT control block to decrement.
1		Flag bit select. Specifies the bits in flag byte 5 that are modified as a result of the counter changing state. The bits are set to 1 if the counter reaches 0 or goes negative. They are set to 0 is the counter goes positive.

Set Counter

Initializes the selected counter in the OLTT control block.

Byte	Bit	Description
0	0–3	Operation code. X'B'
	4–7	Counter select field. Specifies which of the 16 counters in the OLTT control block to initialize
1		Value. Specifies the value to which the counter is to be set.

Set Flags Off

Sets any combination of bits in the selected flag byte to 0's.

Byte	Bit	Description
0	0–3	Operation code. X'A'
	4–7	Flag byte select. Specifies which of the 16 flag bytes in the OLTT control block to modify.
1		Flag bit select. Specifies the bits in the selected fields that are set to 0.

Set Flags On

Sets any combination of bits in the selected flag byte to 1's.

Byte	Bit	Description
0	0–3	Operation code. X'9'
	4–7	Flag byte select. Specifies which of the 16 flag bytes in the OLTT control block to modify.
1		Flag bit select. Specifies the bits in the selected fields are set to 1.

Test under Mask

Tests one of six fields against the bit configuration specified by the mask.

Byte	Bit	Description
0	0–3	Operation code. X'8'
	4–7	Flag byte select. Specifies which of the 16 flag and control bytes in the OLTT control block the command modifies as a result of the test.
1	0–5	Index. Selects one of size 4-byte fields in the OLTT control block to test. `......` Counters 0 to 3 `.....1` Counters 4 to 7 `....1.` Flags 0 to 3 (counters 8 to 11) `....11` Flags 4 to 7 (counters 12 to 15) `...1..` IOB status and extended status `...1.1` Phase error, first status, and final status.
	6	
	7	Flag hex select. Indicates the hexadecimal digit within the selected flag byte that the command modifies as a result of the test. `0` High-order (left) digit `1` Low-order (right) digit The high-order 3 bits in the indicated hexadecimal digit are set to the following bit patterns as a result of the test: `100` All of the selected bits under the mask are 1's. `010` All of the selected bits under the mask are 0's. `001` Some of the selected bits under the mask are 1's.
2–5		Mask.

Compare

Compares the data received with the data in the data field.

Byte	Bit	Description
0		Operation code. X'5'
1		Compare data length. The length of the compare data field. The maximum length is 40 bytes.
Variable		Compare data.

Set Time Delay

Inserts time delays between the execution of the interpretive commands.

Byte	Bit	Description
0		Operation code. X'4'
1		Time delay. An unsigned 8-bit integer specifying the number of 1-second intervals of delay.

Terminate

Stops execution of the interpretive command chain and releases the associated buffers.

Byte	Bit	Description
0		Operation code. X'2'
1		Terminate modifier. Specifies which of the 16 flag bytes in the OLTT control block
		X'00' Release the OLTT control block and restore the line. X'01' Retain the OLTT control block. X'03' NO-OP.

Return Data

Transfers the entire OLTT control block and any received data to the OLTT module in the host for analysis.

Byte	Bit	Description
0		Operation code. X'1'
1		Return modifier.
		X'00' Transfer OLTT control block and received data. X'01' Transfer OLTT control block.

Diagnostic I/O (Dial)

Establishes a connection with a remote terminal.

Byte	Bit	Description
0		Operation code. X'0'
1		XIO flags. X'20'
2		I/O Command. One-byte IOB command.
3–4		Command modifiers. Two-byte IOB modifier.
5		Count of dial digits.
Variable		Dial digits.

Diagnostics I/O (Immediate)

Performs immediate I/O for the OLTT.

Byte	Bit	Description
0		Operation code. X'0'
1		SIO flags. X'40'
2		Command. Loaded into register 1 before the XIO is issued. It specifies the immediate command that is performed.
	0	Reset immediate.
	1	Conditional reset.
	2	Monitor mode.
	3	Send interrupt.
	4	Conditional send interrupt.
	5–7	Not used.
3		X'00'

Diagnostic I/O (Normal)

Performs all communication line I/O operations for the OLTT. The XIO flags, the I/O command, and command modifiers are stored in the IOB before the XIO command is issued.

Byte	Bit	Description
0		Operation code. X'0'
1		XIO flags. X'00'
2		I/O command. One-byte IOB command.
3–4		Command modifiers. Two-byte IOB command modifier.

Variable		Count field. Contains the number of bytes of data in the data field. The count field begins with the first byte following the command modifier field and ends with the first byte that is not X'FF'.
		Example:
		`Data Length  Count Field`
		
		`18 bytes  X'12'`
		`256 bytes  X'FF01'`
		`512 bytes  X'FFFF02'`

Variable		Data. Immediately follows the last byte of the count field. Received data is stored in buffers chained to the OLTT control block. If data is provided with this ENABLE command (byte 2), the first 2 data bytes are used to modify the set-mode SDF field by using the first byte as an AND mask and the second as an OR mask.

Requests for NCP Information

In addition to using traces and tests to gather diagnostic data about NCP, you can obtain NCP information using certain requests. This section describes these requests:

- Session information retrieval (SIR)
- Query product set ID
- Dynamic threshold alteration
- Dynamic LPDA.

Session Information Retrieval

Native-network system services control points (SSCPs) can obtain data from active gateway sessions by issuing the following subvector requests through the NMVT PIU:

- Modify-SIR-data for a particular gateway session. NCP enables or disables SIR for a specific resource and returns an NMVT PIU reply.
- Modify-SIR-data for all gateway sessions. NCP enables or disables SIR for all SNA network interconnection (SNI) resources and returns an NMVT PIU reply.
- Query-SIR-data. NCP replies to this solicited request for data from active gateway sessions by returning to the SSCP:
  - Last outgoing PIU sequence number
  - Next-to-last outgoing PIU sequence number
  - Last incoming PIU sequence number
  - Next-to-last incoming PIU sequence number
  - Data from network interconnection extension (NIX) control block, programmed resource logical unit block extension (NLX), and NIX control blocks for both the native and the outboard network addressable unit (NAU).

When a gateway session ends, NCP sends the same data (as described previously under the solicited query SIR data) in an unsolicited reply using the NMVT PIU. This unsolicited reply is sent to all SSCPs that have enabled SIR for that session or for all gateway sessions.

For detailed RU formats, see *NCP and EP Reference Summary and Data Areas*, Volume 2.

Query Product Set ID

NetView Performance Monitor (NPM) can obtain NCP software identification numbers by issuing a product set ID request using the NMVT PIU. NCP returns an NMVT PIU reply that includes the version and release numbers. NPM uses this information to assist the IBM Support Center representative in SIR data analysis. See information on the product set ID request in *NCP and EP Reference Summary and Data Areas*, Volume 2, or for information on the content and format of the software identification returned in the product set identifier (PSI) control block, see *NCP and EP Reference Summary and Data Areas*, Volume 1.

Dynamic Threshold Alteration

When you want to access or change the transmit and error thresholds of a binary synchronous communication (BSC) device or an SNA station, you use the dynamic threshold alteration (DTA) facility and issue the following subvector requests using the NMVT PIU:

- Query-link-station-attributes threshold values. If the query is for the total-data-transmitted thresholds, NCP returns (in the NMVT PIU reply) the following:
  - BSC device and the traffic count threshold from the DVBSRTT field
  - SDLC station and the total-transmission threshold value from the CUBSRTT or SCBSRTT field.

  If the query is for the total-errors-transmitted thresholds, NCP returns (in the NMVT PIU reply) the following:
  - BSC device and the error-count threshold from the DVBSRTR field
  - SDLC station and the total-retries threshold value from the CUBSRTR or SCBSRTR field.

  NCP also returns the following with the threshold values:
  - LPDA modems supported
  - Modem and line configuration
  - Link segment on which the station or terminal resides.
- Alter-link-station-attributes threshold values. If the alter is to set new data-transmitted threshold values, NCP stores 2 bytes (right-justified) from the data furnished in the request in the following fields:
  - For a BSC device, the DVBSRTT field
  - For an SDLC station, the CUBSRTT or SCBSRTT field.

  If the alter is to set new errors-transmitted threshold values, NCP stores 2 bytes (right justified) from the data furnished in the request in the following fields:
  - For a BSC device, the DVBSRTR field
  - For an SDLC station, the CUBSRTR or SCBSRTR field.

For detailed RU formats for all NMVT PIUs, *NCP and EP Reference Summary and Data Areas*, Volume 2.

Dynamic LPDA

The dynamic link problem determination aid (LPDA) function sets or queries the attributes of links. It also alters or queries the attributes of link stations. You issue the following subvector requests using the NMVT PIU:

- Query-link attributes. NCP returns (in the NMVT PIU reply):
  - LPDA modems supported
  - Modem and line configuration
  - Link segment on which the station or terminal resides.

- Set-link attributes. NCP sets the alter-LPDA data from the request in the following fields:
  - For BSC, the LCBSST field
  - For SDLC, the LKBSST field.

  NCP accepts and processes the set-link attribute request only if LPDA is not in progress for the link.
- Query-link-station attributes. NCP returns (in the NMVT PIU reply):
  - LPDA support
  - Modem and line configuration
  - Link segment on which the station or terminal resides.
- Alter-link-station attributes. Depending on the request, NCP either blocks or allows LPDA tests to this link station.

For detailed RU formats for all NMVT PIUs, see *NCP and EP Reference Summary and Data Areas*, Volume 2.

Error and Statistics Reporting

NCP and MOSS report errors occurring in the communication network. These errors include program checks, adapter checks, station errors, and line errors. NCP also reports statistics on lines and stations in the network. These statistics give you a day-to-day report on network performance.

Use error and statistics reporting capabilities when you suspect temporary line errors, hardware errors, or performance problems, or when you are attempting to resolve a permanent error.

NCP Error and Statistics Reporting

The error and statistics reporting ability of NCP enables it to create record maintenance statistics (RECMS) records for the host. These records are sent to a data set called LOGREC in the host and to a network problem determination application, if you have one installed. To get a printout of the records kept in LOGREC, use the Environmental Record Editing and Printing (EREP) program. For information on how to use EREP, see the EREP manual or the service aids manual for your operating system.

The records NCP builds are grouped into five types, according to the way they are created and prepared for transfer to the host. These five types are:

- BSC and start-stop station statistics and permanent BSC and start-stop line and station errors
- SNA statistics
- Permanent SNA link errors or permanent SNA station errors
- Intensive mode recording of temporary SDLC errors
- Channel link statistics for channel link errors.

VTAM Operation, Volume 2, shows the formats for all the RECMS records.

These records are transferred to the host when permanent errors occur or when temporary error or traffic counters overflow. Analyze these records for intermittent and permanent errors of communication controller hardware and for line errors. A permanent failure of NCP may not allow the RECMS records to be sent to the host. These records or record counters are then available in an NCP dump.

For more detail on error and statistics information, see the following chapters in the *NCP and EP Reference*:

- Chapter 4, Serviceability Aids
- Chapter 7, Support for the 3746 Model 900 Connectivity Subsystem
- Chapter 8, NCP Internet Protocol Support
- Chapter 9, Frame Relay

MOSS Error Recording

The IBM 3720, 3725, or 3745 maintenance and operator subsystem (MOSS) maintains an error log called the box event record (BER) file. If an error is detected in the communication controller or the program, a record is stored in the BER file. This file contains records of any errors in the channel adapters, the transmission subsystem, the control program, the central control unit (CCU), the I/O control, and the MOSS. This file also contains records of all alarms. The BER file is transferred to the host as part of a MOSS or CSP dump. Also, the BER file can be displayed at
the MOSS operator display using the error log function. For more information on BERS, see the following books (as applicable to your operating system):

- *IBM 3745 Maintenance Information Reference*
- *IBM 3720/3721 Communications Controllers Maintenance Information Reference*
- *IBM 3725/3726 Communications Controller Expansion VHSA Maintenance Information.*

Chapter 5. Emulation Program Diagnostic Aid

This chapter describes the diagnostic aids available for EP, including aids performed for EP by MOSS. These EP diagnostic aids are:

- EP serviceability aids
- Invalid host I/O channel commands
- Online terminal tests (OLTTs)
- EP storage dumps
- EP scanner interface trace (EP SIT)
- EP dynamic storage and trace dump
- MOSS diagnostic aids.

EP Serviceability Aids

EP provides status and sense responses to the host processor access method in a manner similar to that of the IBM 2701, 2702, and 2703 transmission control units. This ensures that host access method error recovery procedures and error recording facilities can operate without modification. Internal communication controller error conditions either are mapped to a corresponding IBM 2701, 2702, or 2703 recoverable error condition or result in a hard stop condition.

The communication controller in emulation mode does not retry unsuccessful transmissions. Rather, it responds to the host processor as the transmission control units being emulated would respond. This preserves the interface with the host routines that implement these functions.

Invalid Host I/O Channel Commands

All commands from the I/O channel are accepted initially by the channel adapter hardware. EP then validates the command codes. If EP discovers an invalid command, it returns a channel end (CE), device end (DE), and unit check (UC) status to the host with the COMMAND REJECT message indicated in the sense byte.

Online Terminal Tests

NCP has three types of online tests: online terminal test (OLTT); link test, level 2; and link problem determination aid (LPDA) modem tests. This section discusses OLTTs. For information on the other types of online tests, see *NCP and EP Reference*.

EP does not provide OLTT facilities within the communication controller. It depends on the host to verify proper operation of terminals and communication lines and to aid in diagnosing line or terminal trouble.

OLTT facilities provided by access methods (such as QTAM, BTAM, and TCAM) to initiate and control test procedures can be executed when the communication controller is in emulation mode. EP responds similarly to the IBM 2701, 2702, and 2703 units, requiring no modification of the host routines or terminal procedures, unless the host routines are dependent on control unit timing considerations.

EP Storage Dumps

EP includes a storage dump facility. The dump is a permanent record of the state of the communication controller and may be used to determine conditions in the communication controller. Storage contents are transferred to the host to be printed. To continue operation following a storage dump, the communication controller must be reloaded. The dump is available both formatted and unformatted.

You can also use the SSP CLIST IFWIEPCB to display the dump online.

The unformatted storage dump is printed in hexadecimal with EBCDIC equivalents on the right side of the page. For information on the SSP dump utilities, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

EP Scanner Interface Trace

In addition to the EP line trace facility, EP scanner interface trace (SIT) is provided to obtain a trace of activity between EP and the CSP and between the CSP and the front-end scanner. The first 8 bytes of each trace data buffer contain the buffer header. The identifier in the header indicates whether the data in the buffer is from EP SIT (X'000E') or line trace (X'0009').

Both line trace and EP SIT can be used to trace activity on an odd interface, as during wrap testing. They both can be started and stopped either from MOSS or from the host dynamic dump utility; however, an EP line trace to an odd interface can only be started from MOSS. Both traces have an option not to collect data that is transmitted or received over a communication line. This reduces the chance of trace-induced overrun as well as reduces output volume when only control information is needed.

EP can trace only level 2 and level 3 interrupts, with or without data. You can use the trace entries to find the cause of errors on an EP line. For information on trace record formats, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS."
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM."
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE."

EP Dynamic Storage and Trace Dump

If EP line trace support and dynamic subchannel support are specified during EP generation, this service aid provides the capability to dump communication controller storage or EP line trace output to a host data set without bringing the system down. This facility must be initiated from the host. Commands allow you to chose one of the following options:

- Dump communication controller storage in its entirety
- Display up to 144 bytes of communication controller storage beginning at a selected location
- Dump the EP line trace table or EP SIT buffers

- Trace level 2 or level 3 interrupts or both
- Dynamically dump entries to the EP line trace table
- Stop the dynamic subchannel support functions.

If EP line trace support or dynamic subchannel support is selected at EP generation and the EP line trace option is not selected, the communication controller dynamic storage dump facility is still available. The following sections explain how the dynamic dump utility operates.

EP Dump Storage and Display

The host issues a WRITE command to set the starting address of the dump. The host then issues a READ command to read in the contents of the communication controller storage. The READ command is terminated by the channel stop condition, which occurs when the channel control word (CCW) byte count goes to 0. When the next READ command is received by the communication controller, the data returned starts where the preceding READ command left off. The read operation is ended with the UNIT EXCEPTION command when the upper boundary of storage is reached.

EP Dump Trace Table

The host issues an INHIBIT command to read the contents of the communication controller starting at the trace table and ending when the upper boundary of the table is reached.

EP Dynamic Trace Dump

The host issues a READ CLEAR command to read the contents of the trace table as entries are built. The data starts with the current entry at the time of the READ CLEAR and continues until the command is ended by channel stop. When the next READ CLEAR command is received by the communication controller, the data returned starts where the preceding read operation left off. For each READ CLEAR command, the EP SIT buffers are checked before the line trace buffers. The operation is terminated either by the WRITE BREAK command or by stopping the trace from the MOSS console.

If the dump cannot keep up with trace activity (the trace table entries are overlaid by trace before dynamic dump has retrieved them), the first wrapped entry in the trace table will be flagged with X'FF' in the identifier field, and dynamic dump will restart at the current trace pointer to allow resynchronization of the dump and trace. This resynchronization occurs only if both the EP line trace and the dynamic subchannel support options were selected at EP generation.

The three preceding functions use the dynadump cycle-steal queue (CDDOQ) for data transfer.

Diagnostic Commands Not Supported by EP

EP does not provide functional support for the DIAGNOSTIC WRITE or DIAGNOSTIC READ command. If these commands are issued, EP does not request data to be transferred from the host processor and it does not transfer data to the host processor. The commands are ended in a normal manner (that is, with CE,DE status) to ensure compatibility with the IBM 2701 online diagnostics.

The implementation restrictions of DIAGNOSTIC WRITE and DIAGNOSTIC READ commands do not impair operation of the IBM Type 1 (BTAM/QTAM) error and recovery procedures (ERPs); however, indications of successful or unsuccessful execution of these commands may be misleading. It is recommended that diagnostic routines employing the wrap facility be used for error isolation of suspected system faults.

Maintenance and Operator Subsystem

The following functions for EP are performed by the maintenance and operator subsystem (MOSS):

- Wrap tests
- Storage displays
- Branch trace
- Error recording and notification.

Wrap Tests

Two types of wrap tests are available:

- line interface coupler (LIC) wrap tests
- two external cable and modem wrap tests.

The LIC-level wrap tests the LIC internally; the LIC tailgate wrap tests the complete LIC path without including the modem. The NTT cable-level wrap tests the link out to the modem; the modem-level wrap tests the path up to and including the internal local modem.

Wrap tests verify that a transmission path is clear when the same pattern is transmitted and received. Operator intervention may be required, depending on the specific wrap test, to set a test switch on the modem or attach a wrap plug that connects the transmit leg back to the receive leg.

You can use wrap tests on SDLC lines, X.21 leased lines, and CSS-attached lines. Both types of wrap tests are invoked by the MOSS operator after the host operator disables the line to be tested. While in wrap mode, the line functions as a duplex line.

Storage Displays

MOSS allows the communication controller operator to display and make changes to registers and main storage without intervention or support from EP. The character control block (CCB) display is supported by EP as panel function 6. The CCB display allows the communication controller operator to specify the actual hexadecimal displacement of the halfword of CCB data to be displayed.

Branch Trace

This function is invoked by the MOSS operator. The hardware stores the come-from address, the go-to address, and the associated program levels in the branch trace table (BTT) created by NCP generation.

Error Recording and Notification

A check record pool is built and initialized as part of the shared code processing for each of the levels 1, 2, 3, and 4. EP error processing generates a box event record (BER) and stores it as an entry in the check record pool for hardware checks of the program levels.

The BERs are sent to MOSS, which maintains the most recent BERs in the event log (ELD) on the MOSS disk.

The MOSS operator can display the following:

- Error summaries by type
- A list of the most recent BERs
- Full information on a selected BER.

The following information is common to all BER formats and should be useful during problem analysis. In the event that the BERs are not available, the same information should be in the level 1 block (CXTL1B) in a dump of EP:

- The level 1 request register X'7E' (what caused the interrupt)
- The lagging address register (LAR) X'74' (the instruction preceding the one in error)
- The interrupted level (X'79') and the number of level 1 interrupts taken.

For a detailed description of the BER formats and their contents, see the *NCP and EP Reference Summary and Data Areas*, Volume 1.

MOSS Panel Functions for EP

Elementary data exchange and CCU control program procedures are two MOSS microcode functions that provide the interface to the EP panel functions. The panel functions supported by EP are the following:

Function 1 — Storage display. Displays 4 bytes of central processing unit (CPU) storage.

Function 2 — MSLA switching, channel adapter selection, channel adapter reset, and subchannel status presentation.

Function 3 — Not used.

Function 4 — Activate or deactivate EP line trace or EP SIT with or without data on a normal line or an autocall interface. The traces can be used on the even, odd, or both interfaces during wrap test processing.

Function 5 — Panel line test.

Function 6 — CCB display. The operator can specify the actual displacement of the halfword of CCB data to be displayed. The display is static rather than dynamic unless the MOSS CCU storage display is in refresh mode.

Function 7 — Panel switch. In a PEP environment this switch is used to switch the panel function between NCP and EP mode. A specific mode, NCP or EP, must be selected.

Functions 8–E — Not used.

Chapter 6. SSP Dump Utilities

Besides the diagnostic aids described in *NCP, SSP, and EP Trace Analysis Handbook*, and Chapter 4 and Chapter 5 of this book, three types of dumps are also available to help you diagnose a problem:

- NCP dump
- Maintenance and operator subsystem (MOSS) dump
- Communication scanner processor (CSP) dump.

An NCP dump contains the contents of the communication controller storage and registers. You can dump NCP and transfer it to the host by using the SSP dumper utility or by entering access method commands.

A MOSS dump contains the information that MOSS collects as it continually monitors the operation of the communication controller. MOSS compiles and stores all error data, executes recovery routines, and issues alarm messages. When it detects an error, MOSS automatically dumps its contents and stores the dump data on the MOSS diskette. NCP sends an alert message to the host to notify it of the error. If you want to manually dump MOSS, you can do so from the control panel. See the operating guide for your communication controller for information on how to dump MOSS manually from the control panel. To transfer the MOSS dump to the host, you can enter access method commands.

A CSP dump contains information on the scanners and associated line-coupling hardware that are controlled and monitored by CSP. When CSP detects an error, it automatically dumps its contents and stores the CSP dump on the MOSS disk. NCP sends an alert message to the host to notify it of the error. To transfer the CSP dump to the host, you can enter access method commands.

Both the MOSS and the CSP dump contain several files and tables:

- Graphic configuration file
- Configuration data file
- Machine-level table
- Box event record (BER) file
- Program code fix file (ZAP for IBM 3725 and MCF for IBM 3720 and 3745)
- Token-ring interface coupler (TIC) file
- Line description file.

See the operating guide for your communication controller for additional information on these files.

NCP Dump Transfer Using MOSS-E

This section applies to NCP V6R2 and Later.

You can also use a maintenance and operator subsystem extended (MOSS-E) function to transfer NCP dumps to the host. To transfer the NCP dump via the SNA backbone, you need to access the Service Processor (directly or through DCAF). You can use the Service Processor console to logon to a session with the host and then use the MOSS-E menu to select *Transfer NCP Dump* with the *Host* option.

You must have 3270 emulation in the service processor before you can transfer files to the host using the MOSS-E application. See the *Service Processor Installation and Maintenance* book for more information on setting up the 3270 emulation.

Follow these steps to transfer the NCP DUMP from the service processor to the host.

- Logon to a host ID on the service processor using the 3270 emulation and then click to the MOSS-E application.
- Select the Service Processor icon and the Service Processor Menu displays.
- Select NCP Dump Transfer and the NCP Dump Transfer panel displays.
- On the NCP Dump Transfer panel, make the appropriate selections and then select the Upload button.

  The transfer may take a few minutes.

Once the dump is on your host system you can use your normal formatting and printing procedures.

The rest of this chapter contains general information related to dumping, formatting, and printing NCP, MOSS, and CSP dumps and transferring them to the host using the SSP dumper utility and the dump formatter utility.

The SSP Dumper Utility

To dump NCP in a channel-attached communication controller, invoke either an access method dump facility or a stand-alone job using the SSP dumper utility. To dump a link-attached communication controller, use the access method facility.

The SSP dumper utility consists of two separately called programs:

- The *SSP dumper utility* dumps the storage contents of the communication controller and copies them to a direct-access file or data set.
- The *SSP dump formatter utility* produces a formatted copy of the communication controller's storage contents and places it on a sequential output file or data set.

For information on using the SSP dumper utility with your operating system, see the following:

- For MVS, see Chapter 7, "Using the SSP Dump Utilities in MVS" on page 201.
- For VM, see Chapter 8, "Using the SSP Dump Utilities in VM" on page 219.
- For VSE, see Chapter 9, "Using the SSP Dump Utilities in VSE" on page 227.

Initial Program Load Contention Sense and Status

When a communication controller has multiple channel adapters, each attached to a different host, initial program load (IPL) contention occurs when one host attempts to dump the communication controller (or perform an IPL for the communication controller) while it is being loaded or dumped by another host over another channel. To resolve this contention, whenever a host issues a WRITEIPL command to dump a communication controller, a SENSE command is chained to the WRITEIPL command. The WRITEIPL command will execute only if the communication controller is in an abended state. If the communication controller is in

an online state, the host issues a stand-alone WRITEIPL command. If the communication controller is busy, the SSP dumper utility terminates.

Internal I/O Trace for the SSP Dumper Utility

If a communication controller channel error occurs while dumping NCP, the SSP dumper utility produces a trace table containing information on the channel programs executed by the utility. The trace table is written to the end of the dump data set and is formatted by the SSP dump formatter utility.

The trace table for a dump describes the last 15 channel programs executed; each channel program is represented by one entry in the table. Each table entry contains the following information:

- The channel command words (CCWs) that compose the channel program (there may be up to three CCWs)
- The channel status word (CSW) for the channel program
- The first 20 bytes of the channel data transfer buffer immediately after execution of the channel program (READ, WRITE, WRITEIPL, or WRITEBRK CCWs only).

The CCWs, CSW, and channel data are formatted in separate columns in the formatted dump.

Access Method Dump Commands

Use the access method (VTAM or TCAM) dump commands to:

- Transfer the NCP, MOSS, or CSP dump from the communication controller to the host
- Dump a link-attached communication controller
- Obtain a static or dynamic dump of NCP.

For information on using access method dump commands with your operating system, see the following:

- For MVS, see "Using Access Method Dump Commands" on page 213.
- For VM, see "Using Access Method Dump Commands" on page 224.
- For VSE, see "Using Access Method Dump Commands" on page 234.

Printing Dumps Transferred by Access Method Dump Commands

Print statements of the independent SSP dump formatter utility produce NCP, MOSS, and CSP dumps, which are transferred by the VTAM or TCAM dump commands. If you use the access method facility to dump the contents of communication controller storage to a direct-access file or data set, you must run an independent job to produce a readable dump listing.

For information on JCL statements needed for your operating system, see the following:

- For MVS, see "Printing Dumps Transferred By Access Method Dump Commands" on page 215.

- For VM, see "Printing Dumps Transferred by Access Method Dump Commands" on page 225.
- For VSE, see "Printing Dumps Transferred by Access Method Dump Commands" on page 236.

SSP Dump Utility Features

The following section describes some of the features of the SSP dump formatter utility. See "Formatted Dump Contents" on page 195 for a complete description of the contents and the order of the formatted dump.

- The first page of formatted output contains the system status (normal, slowdown, CWALL, or pseudo slowdown) and the module and offset of the lagging address register (LAR) if it is nonzero.
- You can print the complete buffer prefix and print the free-buffer chain pointers with the total number of buffers in the chain.
- The module name and offset for all negative responses are in the negative response buffer. To get this information, you can take an NCP dump of the buffer pool. The name is located at decimal 62–69 in the buffer, and the offset is 70 and 71.

  NCP has an internal trace that captures the address of the code currently releasing a buffer. Find this address at the fullword starting at byte 64 (X'40') in the buffer. This address overlays part of the module name. The generalized PIU trace (GPT) can still use the module name and offset because the buffer is not released while GPT is running. However, a dump of the buffer pool has the name overlaid for a released buffer. This can be avoided if the buffer is large enough. If the buffer size is greater than 81 bytes, the module name and displacement are copied into bytes 72–81. If the NCP generation definition specifies a smaller buffer size, the RELEASE trace overlays the module name in negative responses. The minimum buffer length and default buffer length remain the same. The minimum length is 72 bytes, and the default length is 88 bytes.
- The formatted dump contains the RETAIN search argument, which includes:

  The name of the RIDS/module where the abend occurred
  The PIDS/Component ID (9-byte field from the PSI control block)
  The AB/abend code, preceded by the letter *S*
  The ADRS/offset into the module where the abend occurred.
- The SSP dump formatter utility has the ability to format dump data sets with record lengths of either 512 bytes or 2KB.
- The SSP dump formatter utility recognizes when the count of NVT entries is one less than the actual number (LNID X'FF'). The formatter prints 256 entries, the Reference Network entry, and a note.
- The following control blocks and tables appear in a dump from a communication controller that has the 370 I/O channel attachment function included in its generation definition:

  Channel-link LKB headers are identified as such.

  CAB headers are identified as peripheral node or subarea node CABs.

If the 370 I/O channel attachment has been generated in an NCP, each CAB appears beneath its owning LKB.

The channel-link group control block (GCBB) appears beneath each channel-link LKB.

If the channel adapter parameter table (CAP) was created during the generation definition, it appears in the dump beneath each CAB.

- For MVS, the PARM option enables you to specify if you want the SSP dump formatter utility automatically executed.
- If you have an IBM 3745, the dump formatter utility provides the following features:
  - The CDS appears beneath the Adapter Interface table (AIT).
  - The storage protect key section of the dump reflects the 4KB (KB equals 1024 bytes) granularity of IBM 3745 storage-protect keys.
  - If the LKB AIT index is valid, the LKB line adapter/channel adapter number and bus number are obtained from the AIT and printed in the LKB header.

Using the DUMP Control Statement

The DUMP control statement lets you select options that affect the output of the dump formatter utility. The following list briefly describes the DUMP control statement options that are available. Before you create the job stream to produce the formatted dump, see page 203, page 220, and page 228 for information about using the DUMP control statement in the MVS, VM, and VSE environments.

- You can use FROMADDR and TOADDR to specify the range of controller storage addresses that are dumped.
- BUF enables you to specify whether the formatted NCP buffer pool, the unformatted buffer pool, or both appear in the dump.
- The FORMAT option specifies whether the dump formatter utility prints NCP control blocks and the branch trace table.
- PRINT lets you select as many as nine different reports that can appear in the dump.
- INDEX=Y specifies that an index is printed at the end of the dump. The index is a guide to the location of the major control blocks by page number. It also indicates the other key sections of the dump such as registers, buffer pool, and save areas. Each control block entry includes the storage address and, if present, the element address. The index dump control statement parameter controls the printing of the index.
- MAP=Y specifies that a copy of the load map, sorted alphabetically by module name, is printed after the normal load map.
- The MOD option can inhibit the printing of the load module (the hexadecimal dump up to the beginning of the buffer pool).
- By coding the TREE keyword on the DUMP control statement you can format the inbound and outbound session routing binary search trees.
- The TYPE option lets you select how control blocks will be formatted by data link control:

TYPE=S inhibits the formatting of the non-Systems Network Architecture (SNA) device control blocks and formats only the SNA device control blocks.

TYPE=N inhibits the formatting of the SNA control blocks; only the non-SNA control blocks will be formatted.

TYPE=B causes both SNA and SNA control blocks to be formatted.

The IBM Sort/Merge Program

The IBM Sort/Merge program or its equivalent is required to run the SSP dump formatter utility program. The interface to the sort/merge program is as follows:

For MVS:

```
SORT FIELDS=(4,8,CH,A,14,6,CH,A)
RECORD TYPE=F,LENGTH=(50)                    (load map)

SORT FIELDS=(1,25,CH,A,28,6,CH,A)
RECORD TYPE=F,LENGTH=(24)                    (index)
```

For VSE:

```
SORT FIELDS=(4,8,CH,A,14,6,CH,A),WORK=0      (load map)
SORT FIELDS=(1,25,CH,A,28,6,CH,A),WORK=0     (index)
```

Formatted Dump Contents

The following list shows the contents of an NCP V7R2 dump formatted by the SSP V4R2 dump formatter utility and shows the order of the actual NCP V7R2 dump. Information for other releases is also shown, but the output generated by these other releases appears in the NCP V7R2 order. Any items not included in your generation definition are omitted. See page 199 for a list of notes referenced by the superscripts in the list.

- RETAIN search argument, containing the four RETAIN parameters
- Date and time of generation (DTG)[1]
- Direct addressable control blocks (XDB, XDH, NTI, NTT, NTW, XDA, FAX, FX2, HWE, HWX)[1]
- ERP control blocks (L1B, L1X)[1]
- Get error status table (GES)
- Adapter information table (AIT)
- Abend control block (ABN)
- Save areas for each level[1]
- Box-unique control blocks (CST, PSB, PSI, CBQ, CPIT, QCB, CRP, MBX, PSTT, PSTA, GPT, NQB, NSA, NSC, NGA, NTN, NDR)[1]
- Vector table of SNPs (VTS) and SSCP-NCP session control block (SNPs)[1]
- SMMF control blocks (SMM, MLT, and SWT)
- Subarea vector table (SVT) and transmission control blocks (TGBs)[1]
- Multilink transmission group control block free address chain
- Network vector table (NVT) entry (one for each network)[1]
- Queue anchor block for a native network (QAN)
- Network interconnect control block (NIB) pool anchor block for the native network
- Free native NIB address chains
- Programmed resource logical unit control block (NLB) pool anchor block for the native network
- Free NLB address chains for the native network
- TGB pool anchor block for the native network
- Transit routing table (TRT) pool anchor block for the native network
- Network vector table extension (NVX)
- Network-unique control blocks in a native network (RMB, TRT, SIT, VIT)[1]
- Internet Protocol congestion control block (IPC, IPS, IPX)
- Routing data area control block (RDA, RDF, RDM, RDO, NRP)
- Local address table control block (LAT)
- Route interface control block (RIB)
- HRT and address of the associated RIB chain
- SRT and address of the associated RIB chain
- NRT and address of the associated RIB chain
- Resource vector table (RVT) in a native network[1]
- Resource vector control block (RVB) in a native network[1]
- Dynamic RVT entries
- BSC-SS resources[1,2]
  - Line control blocks (LCB, ACB, AXB, PSA, LGT, CBB)
  - Cluster/terminal control blocks (DVB, RCB)
- SNA programmed resources[1,2]
  - Line control blocks (VLB, PUV)
  - Physical unit control blocks (NPB, RCB, LUV)
  - Logical unit control blocks (NLB, RCB, NLX, RCB, NSP)
  - SNA-IP session interface control block (SSI)
- SNA resources[1,3]
  - Channel adapter vector table (CAVT)[5]
  - Peripheral node: (For NCP V6R2 and later or NCP V7R1 and later frame relay–physical units)
    - Line control blocks (LKB, ACB-R, AXB, ATT, PSA, LGT, ACB-X, AXB,

ATT, PSA, GCB, PUA-R, PUA-X, XUA, DTL, XMTLS, PLB, PLX, PNDB)
- Physical unit control blocks (CUB, CXI, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
- Pre-pending active BSB chain
- Logical unit control blocks (LUB, LNB, LRB, BSB (SSCP-LU), SPC/SEB, BSB (LU-LU), SPC/SEB, RCB, BXI, LDA, LTX, NSC)
- Inbound tree (SHB, SEBs)[4]
- Outbound trees (SHB with corresponding LNB address)

– Peripheral node: (For NCP V6R2 and later or NCP V7R1 and later NTRI or 3745 frame relay–logical units)
- Line control blocks (LKB, GCB, LLUA, LAXB, LLB, LLBTE, LXC, LNDB, PUV)
- Physical unit control blocks (CUB, CXI, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
- Pre-pending active BSB chain
- Logical unit control blocks (LUB, LNB, LRB, BSB (SSCP-LU), SPC/SEB, BSB (LU-LU), SPC/SEB, RCB, BXI, LDA, LTX, NSC)
- Inbound tree (SHB, SEBs)[4]
- Outbound trees (SHB with corresponding LNB address)

– Peripheral node: (For NCP V6R2 and later or NCP V7R1 and later non-NTRI–physical units)
- Line control blocks (LKB, LKE, TLB, HSH, AVA, ATTL, AVPOOL, TRPL, CBB, ACB-R, LACB, AXB, ATT, LPSA, LDPs, LGT, ACB-X, NACB, AXB, ATT, NPSA, NDPs)
- Physical unit control blocks (CUB, CXI, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
- Pre-pending active BSB chain
- Ethernet interface control block (ENI)

– Peripheral node: (For NCP V6R2 and later or NCP V7R1 and later 3746 Model 900–logical units)
- Line control blocks (LKB, LKE, SLB, CBB, LACB, ACB, AXB, ATT,
- Physical unit control blocks (CUB, CXI, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
- Pre-pending active BSB chain
- Logical unit control blocks (SCB, SXB, SCE, SX2, CBB, SSB, TSB)

– Peripheral node: (For NCP V5R4 NTRI–physical units)
- Line control blocks (LKB, GCB, PUA-R, AXB-R, PUA-X, AXB-X, XUA, LIT, AVB, PLBAT, LLBAT, SNAP, PLHT, RCVLS, XMTLS, DLLB, PLB, PLX, PNDB)
- Physical unit control blocks (CUB, CXI, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
- Pre-pending active BSB chain
- Logical unit control blocks (LUB, LNB, LRB, BSB (SSCP-LU), SPC/SEB, BSB (LU-LU), SPC/SEB, RCB, BXI, LDA, LTX, NSC)
- Inbound tree (SHB, SEBs)[4]
- Outbound trees (SHB with corresponding LNB address)

– Peripheral node: (For NCP V5R4 NTRI–logical units)
- Line control blocks (LKB, GCB, LLUA, LAXB, LLB, LLBTE, LLX, LXC, LNDB, PUV)
- Physical unit control blocks (CUB, CXI, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
- Pre-pending active BSB chain
- Logical unit control blocks (LUB, LNB, LRB, BSB (SSCP-LU), SPC/SEB, BSB (LU-LU), SPC/SEB, RCB, BXI, LDA, LTX, NSC)
- Inbound tree (SHB, SEBs)[4]
- Outbound trees (SHB with corresponding LNB address)

– Subarea node: (For NCP V4R1 (VSE) and NCP V4R2)
- Line control blocks (LKB, ACB, AXB, PSA, LGT, PUV)
- Physical unit control blocks (SCB, SXB, CBB, SX2)

– Peripheral node: (For NCP V4R1 (VSE) and NCP V4R2 non-NTRI)

- Line control blocks (LKB, ACB, AXB, PSA, LGT, PUV)
- Physical unit control blocks (CUB, RCB, CXB, CBB, LUV)
- Logical unit control blocks (LUB, RCB)

– Peripheral node: (For NCP V4R1 (VSE) and NCP V4R2 NTRI–physical units)

- Line control blocks (LKB, GCB, PUA-R, AXB-R, PUA-X, AXB-X, XUA, LIT, AVB, PLBAT, LLBAT, SNAP, PLHT, RCVLS, XMTLS, DLLB, PLB, PUV)
- Physical unit control blocks (CUB, RCB, CXB, CBB, LUV)
- Logical unit control blocks (LUB, RCB)

– Peripheral node: (For NCP V4R1 (VSE) and NCP V4R2 NTRI–logical units)

- Line control blocks (LKB, GCB, LLUA, LAXB, LLB, LLBTE, PUV)
- Physical unit control blocks (CUB, RCB, CXB, CBB, LUV)
- Logical unit control blocks (LUB, RCB)
- Inactive CABs
- Undefined CABs

- 3746 Model 900-attached Enterprise Systems Connection (ESCON) resources (LMB, LME, CBB, ACB-R, LACB, AXB, ATT, LPSA, LDP, AXB-X, NACB, AXB, ATT, NPSA, NDP, LGT)
- 3746 Model 900-attached token-ring resources (TRB, TRE, CBB, TRA-R, LACB, TRX, ATT, LPSA, LDP, TRA-X, NACB, TRX, ATT, NPSA, NDP, LGT)
- 3746 Model 900-attached frame-relay resources
  – Line control blocks (LKB, LKE, FPB, FPB attached list, DTS, CBB, ACB-R, LACB, LPSA, LDPS, LGT, ACB-X, NACB, NPSA, NDPS)
  – Physical unit control blocks (CUB, PRB/SHB, SPC/SEB, RCB, CX2, CXB, CBB)
  – Pre-pending active BSB chain
  – Inbound tree (SHB, SEG)
  – Outbound tree (SAB with corresponding LNB address)
  – Logical unit line control blocks (LKE, CBB, LACB, ACE-X, AXB, AT, NACB)
  – Physical unit control blocks (SQB, SXB, SX2, SCF, CBB, FSB)
- BFSESSINFO control table (BCT)[1]
- Network names table (NNT)[1]
- Dynamic NNT entries
- Queue anchor block (QAB)[1]
- CUB pool anchor block[1]
- Free CUB address chains[1]
- LUB pool anchor block[1]
- Free LUB address chains[1]
- LNB pool anchor block[1]
- Free LNB address chains[1]
- LND pool anchor block[1]
- Free LND address chains[1]
- Independent BSB pool anchor block[1]
- Free BSB address chains[1]
- NSC pool anchor block[1]
- Free NSC address chains[1]
- NSX pool anchor block
- Free NSX address chains
- LTX pool anchor block[1]
- Free LTX address chains[1]
- LUX pool anchor block
- Free LUX address chains[1]
- VAT pool anchor block
- VVT pool anchor block
- NSB pool anchor block
- Free NSB address chains
- SCE pool anchor block
- Free SCE address chains
- LKE pool anchor block
- Free LKE address chains
- SSB pool anchor block
- Free SSB address chains
- ODLC LAN logical pool anchor block

- NQX pool anchor block
- Free NQX address chains
- NIX pool anchor block
- Free NIX address chains
- NNT pool anchor block
- Free NNT address chains
- CBB pool anchor block
- Free CBB address chains
- BSB (SSCP-LU) pool anchor block
- Free BSB address chains
- BSB (LU-LU) pool anchor block for depenednt LUs
- Free BSB address chains
- BXI pool anchor block for dependent LUs
- Free BXI address chains
- BXI pool anchor block for independent LUs
- Free BXI address chains
- CXB pool anchor block
- Free CXB address chains
- CXI pool anchor block
- Free CXI address chains
- LDA pool anchor block
- Free LDA address chains
- NLX pool anchor block
- Free NLX address chains
- RVT pool anchor block
- Free RVT address chains
- LLB pool anchor block for token-ring logical lines
- LLB pool anchor block for frame-relay logical lines
- Queue anchor block extension (QAX)[1]
- FCT pool anchor block
- NVT pool anchor block
- NQE pool anchor block
- Free NQE address chain
- VTS pool anchor block
- HRE pool anchor block
- Free HRE address chains
- SRE pool anchor block
- Free SRE address chains
- NRE pool anchor block
- Free NRE address chains
- CX2 pool anchor block
- Free CX2 address chains
- SNI resources for a native network (NLB, RCB, NIB, NLX, NSP, RCB, NIX)[1]
- NVT in a non-native network
- Queue anchor block for a network (QAN)
- NIB pool anchor block
- Free NIB address chains
- NLB pool anchor block
- Free NLB address chains
- TGB pool anchor block
- TRT pool anchor block
- Network-unique control blocks in a non-native network (RMB, TRT, SIT, VIT)[1]
- RVT in a non-native network[1]
- RVB in a non-native network[1]
- Dynamic RVT entries
- SNI resources for a non-native network (NLB, RCB, NIB, NLX, RCB, NIX)[1]
- Virtual routing control blocks (VST, VVT, VRBs, FLB)[1]
- SNAP trace table (NCP)
- Trace tables (dispatcher, channel adapter, channel adapter IOH trace, address trace)[1]
- Dispatcher queues[1]
- MOSS control blocks (MIF, MTF)[1]
- Channel adapter vector table (CAVT) (EP, PEP)
  - Channel adapter ERP control blocks (CERs) (EP, PEP)
- Channel control block (CHCB) (EP, PEP)
- Channel vector table (CHVT) (EP, PEP)
  - CCBs (EP, PEP)

- Registers
- Storage protect keys
- Raw dump of the NCP load module[6]
- Buffer pool[7]
- Free buffers chain[7]
- Branch trace table[1]
- Address vector table block (AVB)
- Physical link block address table (PLBAT)
- Logical link block address table (LLBAT)
- SNAP trace table (NCP V6R1 and later, NTRI only)
- Load map[8]
- Index to dump contents.

Notes for Formatted Dump:

1. If FORMAT=Y on the DUMP control statement.
2. In element address order.
3. In element address order according to the line (all resources associated with a line—physical units or logical units—appear under the line).
4. If TREE=Y on the DUMP control statement.
5. Always printed before the first channel-attached LKB.
6. Amount printed determined by MOD, BUF, FROMADDR, and TOADDR parameters on the DUMP control statement.
7. If BUF=B or F on the DUMP control statement.
8. If MAP=Y on the DUMP control statement.

Chapter 7. Using the SSP Dump Utilities in MVS

To dump NCP in a channel-attached communication controller, invoke either an access method dump facility or a stand-alone job using the SSP dumper utility. To dump a link-attached communication controller, use the access method facility. For information on the access method facility, see "Using Access Method Dump Commands" on page 213.

Use the SSP dumper utility to dump the storage contents of all communication controllers in MVS. The utility includes two separately called programs that apply in two steps:

Step 1. IFLREAD dumps the storage contents of the communication controller and copies them to a direct-access data set (SYSUT2). (This program is called the *SSP dumper utility*.)

Step 2. IFLDUMP produces a formatted copy of the communication controller's storage contents and places it on a sequential output data set (SYSPRINT). The SYSUT2 data set from IFLREAD (Step 1) is input to this program. (This program is called the *SSP dump formatter utility*.)

The SSP dumper utility has a PARM field option that enables you to specify whether you want the IFLDUMP program to be executed automatically following the execution of the IFLREAD program. In the job control language (JCL), you can execute both of these programs in just one job step, but by specifying PARM=NOFORMAT when executing the IFLREAD program, you can dump the storage without formatting it. The IFLREAD output data set (SYSUT2) can then be used either as input to the next job step in the JCL (the IFLDUMP program execution) or as input to the SSP CLISTs.

If you use the access method facility to dump communication controller storage, the dump process stops after the storage contents of the communication controller are dumped and copied to a direct-access data set. To produce a formatted dump listing, you must then run a stand-alone job to execute IFLDUMP (Step 2).

Host Processor and Communication Controller Requirements

The SSP dumper utility consists of eight load modules. Seven of these run in the host processor. The other module is transferred to the communication controller but runs only in IBM 3705 Communications Controllers.

The SSP dumper utility modules can run in any host processor that accommodates OS/VS2 (MVS), where it operates in a minimum virtual region. You can calculate the amount of work data set space required as equal to the size of the communication controller storage, in KB, plus 6KB.

For information on dumping communication controller storage using the VTAM dump facility, see *VTAM Operation*.

Dumping Communication Controller Storage

Dumping from the communication controller to the direct-access data set is the first step of the SSP dumper utility. Step 1 (IFLREAD) in the dumping process always transfers the contents of communication controller storage and local storage registers to the host processor, which places them on a direct-access data set. When Step 1 is complete, the SSP dumper utility informs the host processor operator. At this point, the communication controller is unusable and must be reloaded with an NCP using the SSP loader utility (or the access method loader facility).

For the JCL needed to both dump and print the contents of communication controller storage, see "Job Control to Activate and Print an NCP Dump" on page 204.

Using the SSP Dump Formatter Utility

The formatting step, Step 2 (IFLDUMP), of the SSP dumper utility is the SSP dump formatter utility. It formats all or a selected part of the dumped data and then places the data on a sequential output data set. The output listing shows the hexadecimal representation of communication controller storage and register contents and gives the character equivalents of all EBCDIC bit patterns that represent characters. Several additional options can be specified by a DUMP control statement to:

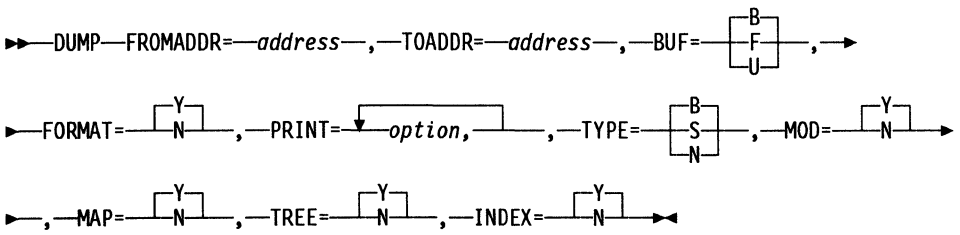
- List the complete contents, or any specified section, of storage.
- Format or unformat the buffer pool. The FORMAT option displays the buffer pool area of communication controller storage as individual buffers. The UNFORMAT option does not individually format the buffers.
- Format or unformat NCP control blocks. The FORMAT option labels and prints network node control blocks at the beginning of the dump listing for convenient reference. It also formats and shows the branch trace table at the end of the dump. The UNFORMAT option does not format the control blocks or branch trace table.
- Print the MOSS or CSP dump with any of the nine files that are contained within these dumps.

  For information on how to obtain MOSS and CSP dump data, see "Using Access Method Dump Commands" on page 213.

The SSP dumper utility has a PARM field to specify whether the IFLDUMP program is to be executed automatically following the execution of the IFLREAD program. For more information, see page 201.

The DUMP Control Statement

The SSP dump formatter utility requires one control statement, DUMP, in the input job stream (SYSIN). This statement specifies your choice of the options. The control statement format is as follows:



FROMADDR=*address*

Specifies the lower limit of the communication controller storage to appear on the listing. If you omit FROMADDR, the listing starts at address X'000'.

TOADDR=*address*

Specifies the upper limit of the communication controller storage to appear on the listing. If you omit TOADDR, the listing ends at the upper limit of storage. If you specify a value higher than the upper limit of storage, the SSP dump formatter utility issues message IFW201I and dumps the storage contents.

BUF=B|F|U

Specifies whether the SSP dump formatter utility is to print the formatted (F) NCP buffer pool, the unformatted buffers (U), or both (B).

FORMAT=Y|N

Specifies whether the SSP dump formatter utility is to format NCP control blocks and the branch trace table.

PRINT

Specifies whether the SSP dump formatter utility is to print any or all of nine available reports. These reports are:

- Configuration data file (CDF)
- MOSS or CSP dump (DMP)
- Microcode fixes (ZAP or MCF)
- Error log (BER)
- Port swap file (PSW)
- "Canned" testing procedures (PRO)
- Graphic machine configuration file (GCF)
- Line description file (LDF)
- Token-ring interface coupler (TIC) file.

Depending on your model of communication controller, some of these files may be unavailable. If you request a report that is not available for a particular model, an informational message is produced. Use commas between report names. The reports are printed in the order that you specify. If you omit the PRINT keyword, all the files are printed in the following order as they apply to your communication controller: GCF, CDF, ZAP or MCF, BER, PRO, LDF, TIC, PSW, and DMP.

TYPE=B|S|N

Specifies whether the SNA device control blocks (S), the non-SNA device control blocks (N), or both (B) are to be formatted.

MOD=Y|N
Specifies whether the hexadecimal dump of the load module is to be printed.

MAP=Y|N
Specifies whether the load map of the load module is to be printed.[3]

TREE=Y|N
Specifies whether the inbound and outbound session routing binary search trees are to be formatted.

INDEX=Y|N
Specifies whether an index is to be printed at the end of the dump.[3]

Some of the parameters for the DUMP control statement are not mutually exclusive; for example, you can code the MOD or BUF parameter with the TOADDR and FROMADDR parameters, and all will affect the dump output.

Job Control to Activate and Print an NCP Dump

Activating and printing the NCP dump is a two-step process. Step 1 (IFLREAD) dumps the NCP storage and Step 2 (IFLDUMP) formats the dump. Step 1 automatically executes Step 2.

To use the SSP dumper utility to dump and the SSP dump formatter utility to print the communication controller storage contents, provide job control statements only for Step 1 in the dumping process and one or more DUMP control statements for Step 2. Step 1 generates the required control statements for Step 2.

If you want to use the SSP dumper utility to dump the communication controller storage but you want to use the SSP CLISTs to view it, specify PARM=NOFORMAT on the EXEC statement. Specifying these parameters prevents Step 2 from being executed. The data set specified for SYSUT2 is used as input to the SSP CLISTs.

If you have used the access method to dump NCP and you wish to use the dump formatter utility to print the data, perform only Step 2 of the dump process. To perform Step 2, substitute the name IFLDUMP for the name IFLREAD in the EXEC statement. Specify the name of the data set containing the dump data to be formatted in the SYSUT2 DD statement and remove the SYSUT1 DD statement. For an example of this coding, see page 216. The statements needed to perform Steps 1 and 2 are as follows:

[3] An IBM-compatible sort program must be available before you can use these parameters.

//jobname	JOB	Initiates the job.
//stepname	EXEC	Specifies the programs IFLREAD or IFLDUMP or the name of a procedure containing the job control statements.
//STEPLIB	DD	Specifies the library that contains the dump program or IFLREAD.
//SYSUT1	DD	Specifies which communication controller's contents will be dumped.
//SYSUT2	DD	Specifies the DASD work data set onto which the communication controller's contents will be dumped. This must be allocated as DSORG=DA. To calculate the space needed for SYSUT2, add 6KB to the size of the communication controller storage in kilobytes. For example, to determine the space in a communication controller with 4MB (MB equals 1 048 576 bytes) of storage, convert the 4MB to kilobytes and add 6KB: ((4 x 1024 x 1024) + 6196) bytes. SYSUT2 is written at 512 byte records for a 3720 and 3725. **IBM 3745 at EC Level A47014 or IBM 3745-130, -150, or -170 EC Level A73290**: SYSUT2 is written at 2048 byte records. If you do not know the EC level of your communication controller, you should use a block size of 512 in your calculation. This block size ensures enough space is allocated for SYSUT2. However, do not specify the BLKSIZE option on this DD statement. Use these block sizes only to calculate storage space. The SSP dumper utility provides the BLKSIZE and LRECL specifications.

```
//SYSPRINT     DD     Specifies a sequential data set–that is,
                     the system output device, magnetic tape, or DASD
                     volume–onto which the dump program is to place
                     the dump listing.

                     If you specify DCB on the SYSPRINT DD, you must code
                     DCB=(LRECL=121, BLKSIZE=(n x 121), RECFM=FBA)
                     where BLKSIZE is a multiple of 121.

//SYSIN        DD     Specifies the data set, or input
                     stream, containing the utility
                     control statement, DUMP.

//SYSOUT       DD     Specifies the SORT/MERGE message
                     data set.  This is required by the SORT/MERGE
                     program.

//SORTLIB      DD     Specifies the data set that contains the
                     SSP dump formatter utility sort routine.

/*
```

Add the following DD statements to the JCL that invokes the SSP dump formatter utility if you request the load map (MAP=Y):

```
//SORTIN       DD     Defines the DASD data set used as
                     input to the MVS sort routine.

//SORTOUT      DD     Defines the DASD data set used as
                     output to the MVS sort routine.

//SORTWK01     DD     Defines an intermediate storage data set.
```

Add the following DD statements to the JCL if you request the index to control blocks (INDEX=Y):

```
//INDXIN       DD     Defines the input data set.

//INDXOUT      DD     Defines the output data set.

//INDXWK01     DD     Defines the intermediate storage data set.
```

Example: Assume that (1) a communication controller whose unit address is 030 is to be dumped, (2) the dump listing is to show the contents of communication controller storage from address X'000' to the end, and (3) the NCP control blocks and buffer pool are to be formatted. An example of the JCL used to get the dump listing is as follows:

```
//CCDUMP      JOB    123456,SMITH,MSGLEVEL=1
//JOBLIB      DD     DSN=SYS1.DUMPCC,DISP=SHR,UNIT=3380,
//                   VOL=SER=333333
//EXEC        EXEC   PGM=IFLREAD
//STEPLIB     DD
//SYSUT1      DD     UNIT=030
//SYSUT2      DD     UNIT=3380,DISP=NEW,
//                   SPACE=(TRK,(100),,CONTIG),
//                   DCB=(DSORG=DA)
//SYSPRINT    DD     SYSOUT=A
//SYSOUT      DD     SYSOUT=A
//SORTLIB     DD     DSN=SYS1.SORTLIB,DISP=SHR
//SORTIN      DD     DSN=&&SPOOL1,UNIT=SYSDA,SPACE=(CYL,(10,5)),
//                   DISP=(NEW,DELETE)
//SORTOUT     DD     DSN=&&SPOOL2,UNIT=SYSDA,SPACE=(CYL,(10,5)),
//                   DISP=(NEW,DELETE)
//SORTWK01    DD     DSN=TEMP1,DISP=(NEW,DELETE),UNIT=(SORTWK),
//                   SPACE=(CYL,(5,2),,CONTIG)
//INDXIN      DD     DSN=&&SPOOL3,UNIT=SYSDA,SPACE=(CYL,(10,5)),
//                   DISP=(NEW,DELETE)
//INDXOUT     DD     DSN=&&SPOOL4,UNIT=SYSDA,SPACE=(CYL,(10,5)),
//                   DISP=(NEW,DELETE)
//INDXWK01    DD     DSN=TEMP2,DISP=(NEW,DELETE),UNIT=(SORTWK),
//                   SPACE=(CYL,(5,2),,CONTIG)
//SYSIN       DD     *
      DUMP            FROMADDR=000,FORMAT=Y,BUF=F
/*
```

Note: The dump data set must be DSORG=DA for all types of dumps.

If your communication controller has 4MB of storage and you are using a block size of 512, replace the SYSUT2 DD statement with the following:

```
//SYSUT2      DD     UNIT=SYSDA,DISP=NEW,
//                   SPACE=(512,(8205),,CONTIG),
//                   DCB=(DSORG=DA)
```

If your communication controller has 4MB of storage and you are using a block size of 2048, replace the SYSUT2 DD statement with the following:

```
//SYSUT2      DD     UNIT=SYSDA,DISP=NEW,
//                   SPACE=(2048,(2052),,CONTIG),
//                   DCB=(DSORG=DA)
```

The PARM Field Options in the EXEC Control Statement

You can specify the number of lines to be contained on each page of the SSP dump formatter utility output by coding one of the following parameters on the EXEC control statement:

```
PARM='LINECOUNT=nn'
PARM='LC=nn'
```

nn specifies a decimal number from 10 to 99, which represents the number of lines on each page printed by the SSP dump formatter utility.

If the LINECOUNT parameter is omitted, or is syntactically incorrect, the default is 55.

Example: To specify that the SSP dump formatter utility print 40 lines on each page of printed output, code the PARM field option as follows:

```
//STEP1 EXEC PGM=IFLREAD,PARM='LINECOUNT=40'
//STEP1 EXEC PGM=IFLDUMP,PARM='LINECOUNT=40'
```

LINECOUNT=nn is the only PARM field option recognized by the independent SSP dump formatter utilities.

By coding the NOFORMAT parameter on the EXEC control statement, you can bypass the automatic invocation of the SSP dump formatter utility and view the dump data using SSP CLISTs. For more information on SSP CLISTs, see Chapter 11, "Using SSP CLISTs in MVS" on page 275.

Example: To bypass the SSP dump formatter step, code the PARM field option as follows:

```
//STEP1 EXEC PGM=IFLREAD,PARM=NOFORMAT
```

Note: The LINECOUNT and NOFORMAT parameters cannot be coded together as PARM field options on the EXEC control statement.

Sample MVS Procedures for Activating and Printing the NCP Dump

Sample procedures for activating and printing the NCP dump under MVS are included on your licensed program tape. The data set name of the sample for the SSP dumper utility is DUMPJCL; the data set name of the sample for the SSP dump formatter utility is DMFTJCL. These data sets are found in the ASSPSAMP library on the tape. These procedures are provided to help you create and tailor the JCL in your MVS environment.

Sample JCL Used in DUMPJCL:

An example of the JCL used in the DUMPJCL sample (for the SSP dumper utility) is as follows:

```
//DUMP   JOB (account info),'name'
//DUMP   PROC OUT='*',UNITNME=sysda,CCADDR=xxx,SSPLIB='sys1.ssplib',
//            SORTLIB='sys1.sort.sortlib',SORTWK='sortwk'
//*********************************************************************
//**                                                                 **
//**     PROCEDURE:  DUMP                                            **
//**                                                                 **
//**     FUNCTION:   DUMP AND FORMAT CONTROLLER                      **
//**                                                                 **
//**     NOTE:                                                       **
//**        CHANGE ALL LOWER CASE CHARACTERS TO VALUES               **
//**        SUITABLE FOR YOUR INSTALLATION.                          **
//**                                                                 **
//**     SYMBOLIC PARMS:                                             **
//**     OUT      :  SYSOUT CLASS                                    **
//**     UNITNME  :  UNITNAME FOR TEMPORARY DATA SETS                **
//**     CCADDR   :  COMMUNICATION CONTROLLER ADDRESS                **
//**     SSPLIB   :  LIBRARY CONTAINING IFLREAD ROUTINE              **
//**     SORTLIB  :  LIBRARY CONTAINING MVS SORT ROUTINE             **
//**     SORTWK   :  UNIT NAME FOR SORT ROUTINE                      **
//**                                                                 **
//**     FOR MORE INFORMATION ABOUT THIS JCL SEE NCP/SSP/EP          **
//**     DIAGNOSIS GUIDE, FORM NUMBER LY43-0033                      **
//**                                                                 **
//**    ACTIVITY:                                                    **
//**    ---------------------------------------------------------    **
//**                                                                 **
//**    NONE                                                         **
//**                                                                 **
//*********************************************************************
//**  ADD ",PARM=NOFORMAT" TO BELOW STATEMENT TO SUPPRESS THE        **
//**  FORMATTING OF THE DUMP                                         **
//*********************************************************************
//EXEC     EXEC  PGM=IFLREAD
//*********************************************************************
//**  LIBRARY CONTAINING IFLREAD                                     **
//*********************************************************************
//STEPLIB  DD  DSN=&SSPLIB,DISP=SHR
//*********************************************************************
//**  DIAGNOSTIC OUTPUT                                              **
//*********************************************************************
//*SYSUDUMP DD  SYSOUT=&OUT
//*SYSABEND DD  SYSOUT=&OUT
//*********************************************************************
//**  COMMUNICATION CONTROLLER ADDRESS                               **
//*********************************************************************
//SYSUT1   DD UNIT=&CCADDR
//*********************************************************************
//**  WORK DATASET ONTO WHICH COMMUNICATION CONTROLLER CONTENTS      **
//**  WILL BE DUMPED --- DSORG=DA IS REQUIRED                        **
//*********************************************************************
```

```
//*********************************************************************
//SYSUT2   DD DISP=NEW,SPACE=(2048,(8204),,CONTIG),DCB=(DSORG=DA),
//            UNIT=&UNITNME
//*********************************************************************
//**  FORMATTED DUMP DATASET                                         **
//*********************************************************************
//SYSPRINT DD SYSOUT=&OUT
//*********************************************************************
//**  SORT/MERGE MESSAGE DATASET                                     **
//*********************************************************************
//SYSOUT   DD SYSOUT=&OUT
//*********************************************************************
//**  LIBRARY CONTAINING MVS SORT ROUTINE                            **
//*********************************************************************
//SORTLIB  DD DSN=&SORTLIB,DISP=SHR
//*********************************************************************
//**  SORT DATASETS REQUIRED IF LOAD MAP IS REQUESTED (MAP=Y)        **
//*********************************************************************
//SORTIN   DD DSN=&&SPOOL1,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//SORTOUT  DD DSN=&&SPOOL2,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//SORTWK01 DD DSN=&&TEMP1,DISP=(NEW,DELETE),UNIT=&SORTWK,
//            SPACE=(CYL,(5,2),,CONTIG)
//*********************************************************************
//**  SORT DATASETS REQUIRED IF INDEX IS REQUESTED (INDEX=Y)         **
//*********************************************************************
//INDXIN   DD DSN=&&SPOOL3,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//INDXOUT  DD DSN=&&SPOOL4,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//INDXWK01 DD DSN=&&TEMP2,UNIT=&SORTWK,
//            SPACE=(CYL,(5,2),,CONTIG),DISP=(NEW,DELETE)
//*********************************************************************
//PROCEND  PEND
//STEP1    EXEC DUMP
//*********************************************************************
//**  DATASET CONTAINING DUMP CONTROL STATEMENTS                     **
//**  (SEE NCP/SSP/EP DIAGNOSIS GUIDE, PUBLICATION # LY43-0033,      **
//**   FOR MORE DETAILS)                                             **
//*********************************************************************
//SYSIN    DD  *
           DUMP
/*
```

Sample JCL Used in DMFTJCL:

An example of the JCL used in the DMFTJCL sample (for the SSP dump formatter utility) is as follows:

```
//DMPFMT   JOB (account info),'name  '
//DMPFMT   PROC OUT='*',UNITNME=sysda,SSPLIB='sys1.ssplib',
//            SORTLIB='sys1.sort.sortlib',DUMPNME='dump.dataset',
//            SORTWK='sortwk'
//*********************************************************************
//*   PROCEDURE : IFLDUMP                                             *
//*                                                                   *
//*    FUNCTION : FORMAT CONTENTS OF COMMUNICATION CONTROLLER         *
//*                                                                   *
//*        NOTE :                                                     *
//*               CHANGE ALL LOWER CASE CHARACTERS TO VALUES          *
//*               SUITABLE FOR YOUR INSTALLATION.                     *
//*                                                                   *
//*   SYMBOLIC PARMS :                                                *
//*     OUT      : SYSOUT CLASS                                       *
//*     UNITNME  : UNITNAME FOR TEMPORARY DATA SETS                   *
//*     SSPLIB   : LIBRARY CONTAINING IFLDUMP ROUTINE                 *
//*     SORTLIB  : LIBRARY CONTAINING MVS SORT ROUTINE                *
//*     DUMPNME  : DATA SET NAME OF UNFORMATTED DUMP                  *
//*     SORTWK   : UNIT NAME FOR SORT ROUTINE                         *
//*                                                                   *
//*   FOR MORE INFORMATION ABOUT THIS JCL SEE NCP/SSP/EP              *
//*   DIAGNOSIS GUIDE, FORM NUMBER LY43-0033                          *
//*                                                                   *
//*   ACTIVITY :                                                      *
//*   ------------------------------------------------------------ *
//*   NONE                                                            *
//*********************************************************************
//EXEC     EXEC  PGM=IFLDUMP
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE LIBRARY CONTAINING IFLDUMP
//*
//STEPLIB  DD DSN=&SSPLIB,DISP=SHR
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE DASD WORK DATA SET ONTO WHICH
//*       THE STORAGE CONTENTS, MOSS DUMP, OR CSP DUMP WERE WRITTEN
//*
//SYSUT2   DD DSN=&DUMPNME,DISP=OLD
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE SEQUENTIAL DATA SET ONTO
//*       WHICH IFLDUMP IS TO PLACE THE DUMP LISTING
//*
//SYSPRINT DD SYSOUT=&OUT
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE DATA SET WHICH CONTAINS THE
//*       SORT ROUTINE
//SORTLIB  DD DSN=&SORTLIB,DISP=SHR
```

```
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       INPUT TO THE MVS SORT ROUTINE
//*
//SORTIN   DD DSN=&&SPOOL1,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       OUTPUT FROM THE MVS SORT ROUTINE
//*
//SORTOUT  DD DSN=&&SPOOL2,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES AN IMMEDIATE STORAGE DATA SET
//*
//SORTWK01 DD DSN=&&TEMP1,UNIT=&SORTWK,
//            SPACE=(CYL,(5,2),,CONTIG),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       INPUT TO THE MVS SORT ROUTINE
//*
//INDXIN   DD DSN=&&SPOOL3,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       OUTPUT FROM THE MVS SORT ROUTINE
//*
//INDXOUT  DD DSN=&&SPOOL4,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES AN IMMEDIATE STORAGE DATA SET
//*
//INDXWK01 DD DSN=&&TEMP2,UNIT=&SORTWK,
//            SPACE=(CYL,(5,2),,CONTIG),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH IS THE MESSAGE DATA SET
//*
//SYSOUT   DD SYSOUT=&OUT
//*********************************************************************
//*    DD STATEMENTS WHICH CONTAIN DIAGNOSTIC OUTPUT
//*
//*SYSUDUMP DD SYSOUT=&OUT
//*SYSABEND DD SYSOUT=&OUT
//*********************************************************************
//PROCEND  PEND
//STEP1    EXEC DMPFMT
//*********************************************************************
//*    DD STATEMENT WHICH CONTAINS THE DUMP CONTROL STATEMENTS
//SYSIN    DD  *
           DUMP
//*********************************************************************
//*  FOR MORE INFORMATION AND EXAMPLES
//*  SEE NCP SSP EP DIAGNOSIS GUIDE  (LY43-0033)
//*********************************************************************
```

Using Access Method Dump Commands

Use the procedures described in this section to dump NCP or transfer the MOSS or CSP dump.

Notes:

1. For the IBM 3725: If you want a MOSS, CSP, or TRSS dump, dump to diskette before invoking the access method. The MOSS or CSP dump may contain TRSS dump files. These files are transferred to the host when either MOSS or CSP is specified to the access method.
2. For the IBM 3720 and 3745: If you want a MOSS or CSP dump, dump to either diskette or disk, depending on the configuration of your communication controller and its operating mode. If you want a TRSS dump, however, you can dump only to diskette. Invoke the access method to transfer the dump to the host. The MOSS or CSP dump may contain the TRSS dump files. These files are transferred to the host when either MOSS or CSP is specified to the access method.

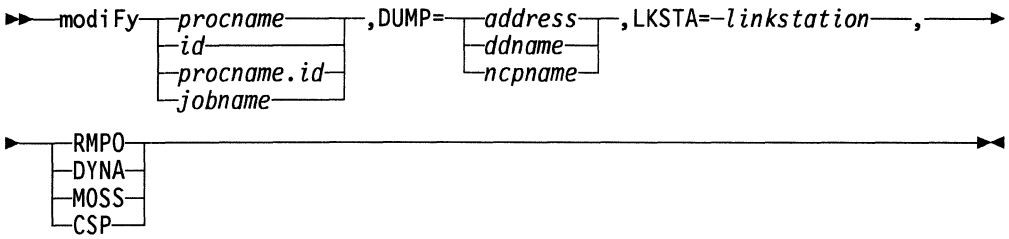
VTAM Operation

To dump NCP or transfer the contents of an NCP, CSP, or MOSS dump using VTAM, use the MODIFY DUMP command. For more information about this command, see *VTAM Operation*.

Note: You must have VTAM V3R2 to use this command for an IBM 3720 Communication Controller's disk.

TCAM Operation

To transfer the contents of an NCP, CSP, or MOSS dump using TCAM, use the following command:



procname
The name of a cataloged procedure in SYS1.PROCLIB that starts the TCAM message control program to which you are issuing this command.

id
An alternate name that can be specified for *procname.*

procname.id
The name used in the START TCAM command when TCAM was started. The same *id* variable must be specified when used in any succeeding TCAM command.

jobname
A name used only when TCAM is loaded and executed from the input stream.

address
The address of NCP. This keyword is valid only for channel-attached communication controllers.

ddname
The ddname of NCP. This keyword is valid only for channel-attached communication controllers.

ncpname
The name of NCP.

linkstation
The name of a link station for dumping over a link.

RMPO
Causes the link-attached communication controller to be dumped and then powered off. This keyword cannot be specified if DYNA, MOSS, or CSP is used.

DYNA
Specifies transfer of the communication controller storage dynamically.

MOSS
Specifies transfer of the MOSS dump.

CSP
Specifies transfer of the CSP dump.

Printing Dumps Transferred By Access Method Dump Commands

If you used the access method facility to dump the contents of communication controller storage to a direct-access data set, run an independent job to produce a readable dump listing. The JCL statements needed are as follows:

```
//jobname       JOB         Initiates the job.

//stepname      EXEC        Specifies the program IFLDUMP or
                            the name of a procedure containing
                            the job control statements.

//SYSUT2        DD          Specifies the DASD work data set
                            onto which the storage contents,
                            MOSS dump, or CSP dump were written.

//SYSPRINT      DD          Specifies a sequential data set–
                            the system output device, magnetic tape,
                            or DASD volume–onto which IFLDUMP
                            is to place the dump listing.

//SYSIN         DD          Specifies the data set, or input
                            stream, containing the
                            DUMP control statement.

//SORTLIB       DD          Specifies the data set which
                            contains the sort routine.

/*
```

The following two groups of DD statements are not required to print either the MOSS or CSP dump.

Add the following DD statements to the JCL that invokes the SSP dump formatter utility if you request the load map (MAP=Y):

```
//SORTIN        DD          Specifies the DASD data set to be
                            used as input to the MVS sort routine.

//SORTOUT       DD          Specifies the DASD data set to be
                            used as output from the MVS sort routine.

//SORTWK01      DD          Specifies an intermediate storage
                            data set.
```

Add the following DD statements to the JCL if you request the index to control blocks (INDEX=Y):

```
//INDXIN        DD          Specifies the input data set.

//INDXOUT       DD          Specifies the output data set.

//INDXWK01      DD          Specifies the intermediate storage data set.
```

Example: Assume that a communication controller was dumped by VTAM onto a data set called VTAM.DUMPNME. The following sample shows the JCL used to get the dump listing.

```
//DMPFMT   JOB (account info),'name  '
//DMPFMT   PROC OUT='*',UNITNME=sysda,SSPLIB='sys1.ssplib',
//            SORTLIB='sys1.sort.sortlib',DUMPNME='dump.dataset'
//*********************************************************************
//*   COPYRIGHT = NONE                                                *
//*                                                                   *
//*   PROCEDURE : IFLDUMP                                             *
//*                                                                   *
//*    FUNCTION : FORMAT CONTENTS OF COMMUNICATION CONTROLLER         *
//*                                                                   *
//*        NOTE :                                                     *
//*               CHANGE ALL LOWER CASE CHARACTERS TO VALUES          *
//*               SUITABLE FOR YOUR INSTALLATION.                     *
//*                                                                   *
//*   SYMBOLIC PARMS :                                                *
//*     OUT      : SYSOUT CLASS                                       *
//*     UNITNME  : UNITNAME FOR TEMPORARY DATA SETS                   *
//*     SSPLIB   : LIBRARY CONTAINING IFLDUMP ROUTINE                 *
//*     SORTLIB  : LIBRARY CONTAINING MVS SORT ROUTINE                *
//*     DUMPNME  : DATA SET NAME OF UNFORMATTED DUMP                  *
//*                                                                   *
//*   FOR MORE INFORMATION ABOUT THIS JCL SEE NCP/SSP/EP              *
//*   DIAGNOSIS GUIDE, FORM NUMBER LY43-0033                          *
//*                                                                   *
//*   ACTIVITY :                                                      *
//*   ------------------------------------------------------------    *
//*   NONE                                                            *
//*********************************************************************
//EXEC     EXEC  PGM=IFLDUMP
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE LIBRARY CONTAINING IFLDUMP
//*
//STEPLIB  DD DSN=&SSPLIB,DISP=SHR
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE DASD WORK DATA SET ONTO WHICH
//*       THE STORAGE CONTENTS, MOSS DUMP, OR CSP DUMP WERE WRITTEN
//*
//SYSUT2   DD DSN=&DUMPNME,DISP=OLD
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE SEQUENTIAL DATA SET ONTO
//*       WHICH IFLDUMP IS TO PLACE THE DUMP LISTING
//*
//SYSPRINT DD SYSOUT=&OUT
//*********************************************************************
//*    DD STATEMENT WHICH SPECIFIES THE DATA SET WHICH CONTAINS THE
//*       SORT ROUTINE
//*
//SORTLIB  DD DSN=&SORTLIB,DISP=SHR
```

```
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       INPUT TO THE MVS SORT ROUTINE
//*
//SORTIN   DD DSN=&&SPOOL1,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       OUTPUT FROM THE MVS SORT ROUTINE
//*
//SORTOUT  DD DSN=&&SPOOL2,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES AN IMMEDIATE STORAGE DATA SET
//*
//SORTWK01 DD DSN=&&TEMP1,UNIT=(SORTWK),
//            SPACE=(CYL,(5,2),,CONTIG),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       INPUT TO THE MVS SORT ROUTINE
//*
//INDXIN   DD DSN=&&SPOOL3,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES THE DASD DATA SET TO BE USED AS
//*       OUTPUT FROM THE MVS SORT ROUTINE
//*
//INDXOUT  DD DSN=&&SPOOL4,UNIT=&UNITNME,
//            SPACE=(CYL,(10,5)),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH DEFINES AN IMMEDIATE STORAGE DATA SET
//*
//INDXWK01 DD DSN=&&TEMP2,UNIT=(SORTWK),
//            SPACE=(CYL,(5,2),,CONTIG),DISP=(NEW,DELETE)
//*********************************************************************
//*    DD STATEMENT WHICH IS THE MESSAGE DATA SET
//*
//SYSOUT   DD SYSOUT=&OUT
//*********************************************************************
//*    DD STATEMENTS WHICH CONTAIN DIAGNOSTIC OUTPUT
//*
//*SYSUDUMP DD SYSOUT=&OUT
//*SYSABEND DD SYSOUT=&OUT
//*********************************************************************
//PROCEND  PEND
//STEP1    EXEC DMPFMT
//*********************************************************************
//*    DD STATEMENT WHICH CONTAINS THE DUMP CONTROL STATEMENTS
//SYSIN    DD  *
           DUMP
/*
```

Note: SORT DD statements are not necessary for printing the MOSS or CSP dump.

Example: Assume that a MOSS dump was transferred by VTAM onto a data set called VTAM.DUMPDSET. The following sample shows the JCL used to get the dump listing and the IBM 3725 error log:

```
//CCDUMP        JOB    123456,SMITH,MSGLEVEL=1
//EXEC          EXEC   PGM=IFLDUMP
//SYSUT2        DD     DSN=VTAM.DUMPDSET,DISP=OLD
//SYSPRINT      DD     SYSOUT=A
//SYSOUT        DD     SYSOUT=A
//SYSIN         DD     *
                DUMP   PRINT=(DMP,BER)
/*
//
```

Note: SORT DD statements are not necessary for printing the MOSS or CSP dump.

Chapter 8. Using the SSP Dump Utilities in VM

To dump NCP in a channel-attached communication controller, invoke either an access method dump facility or a stand-alone job using the SSP dumper utility. To dump a link-attached communication controller, use the access method facility. For information on the access method facility, see "Using Access Method Dump Commands" on page 224.

Use the SSP dumper utility to dump the storage contents of an IBM 3720, 3725, or 3745 Communication Controller in VM. The utility includes two separately called programs that occur in two steps:

Step 1. IFLREAD dumps the storage contents of the communication controller and copies them to a direct-access file (SYSUT2). This program is called the *SSP dumper utility.*

Step 2. IFLDUMP creates a printable copy of the communication controller's storage contents and places it on a sequential output file (SYSPRINT). The SYSUT2 file from IFLREAD (Step 1) is input to this program. (This program is called the *SSP dump formatter utility.*)

Host Processor and Communication Controller Requirements

The SSP dumper utility contains two load modules and seven text files. The SSP dumper utility modules can run in any host processor that runs under VM.

To calculate the amount of space needed for the dump data file (SYSUT2), add 6KB to the size of the communication controller storage in kilobytes. For example, to determine the space in a communication controller with 4MB of storage, convert the 4MB to kilobytes, and add 6KB: ((4 x 1024) + 6)KB.

IBM 3745 at EC Level A47014 or IBM 3745-130, -150, or -170 EC Level A73290: SYSUT2 is written at 2048 byte records.

If you do not know the EC level of your communication controller, you should use a block size of 512 in your calculation. This block size ensures enough space is allocated for the dump file. However, do not specify the BLKSIZE option on this FILEDEF. Use these block sizes only to calculate storage space. The SSP dumper utility provides the BLKSIZE and LRECL specifications.

For information on dumping communication controller storage using the VTAM dump facility, see *VTAM Operation.*

Dumping Communication Controller Storage

Dumping from the communication controller to the direct-access file is the first step of the SSP dumper utility. Step 1 (IFLREAD) in the dumping process always transfers the contents of the communication controller storage and local storage registers to the host processor, which places them on a direct-access file. When Step 1 is complete, the SSP dumper utility informs the host processor operator. At this point, the communication controller is unusable and NCP must be reloaded into it (or the access method loader utility).

For the FILEDEFs needed to both dump and print the contents of communication controller storage, see "Job Control to Activate and Print an NCP Dump" on page 222.

Using the SSP Dump Formatter Utility

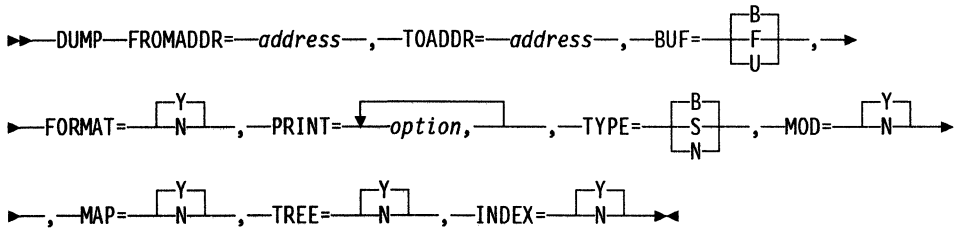
The formatting step, Step 2 (IFLDUMP), of the SSP dumper utility is the SSP dump formatter utility. It formats all or a selected part of the dumped data and then places the data on a sequential output file. The output listing shows the hexadecimal representation of communication controller storage and register contents and gives the character equivalents of all EBCDIC bit patterns that represent characters. Several additional options can be specified by the DUMP control statement:

- List the complete contents, or any specified section, of storage.
- Format or unformat the buffer pool. The FORMAT option displays the buffer pool area of communication controller storage as individual buffers. The UNFORMAT option does not individually format the buffers.
- Format or unformat NCP control blocks. Format labels and prints network node control blocks at the beginning of the dump listing for convenient reference. It also formats and shows the branch trace table at the end of the dump. UNFORMAT does not format the control blocks or branch trace table.
- Print the MOSS or CSP dump with any of the nine files that are contained within these dumps.

  For information on how to obtain MOSS and CSP dump data, see "Using Access Method Dump Commands" on page 224.

The DUMP Control Statement

The SSP dump formatter utility requires one control statement, DUMP, in the input job stream. This statement specifies your choice of the options. The control statement format is as follows:



FROMADDR=*address*
Specifies the lower limit of the communication controller storage to appear on the listing. If you omit FROMADDR, the listing starts at address X'000'.

TOADDR=*address*
Specifies the upper limit of the communication controller storage to appear on the listing. If you omit TOADDR, the listing ends at the upper limit of storage. If you specify a value higher than the upper limit of storage, the SSP dump formatter utility issues message IFW201I and dumps the storage contents.

BUF=B|F|U
Specifies whether the SSP dump formatter utility is to print the formatted (F) NCP buffer pool, the unformatted buffers (U), or both (B).

FORMAT=Y|N
Specifies whether the SSP dump formatter utility is to format NCP control blocks and the branch trace table.

PRINT
Specifies whether the SSP dump formatter utility is to print any or all of nine available reports. These reports are:

- Configuration data file (CDF)
- MOSS or CSP dump (DMP)
- Microcode fixes (ZAP or MCF)
- Error log (BER)
- Port swap file (PSW)
- "Canned" testing procedures (PRO)
- Graphic machine configuration file (GCF)
- Line description file (LDF)
- Token-ring interface coupler (TIC) file.

Depending on your model of communication controller, some of these files may be unavailable. If you request a report that is not available for a particular model, an informational message is produced. Use commas between report names. The reports are printed in the order that you specify. If you omit the PRINT keyword, all the files are printed in the following order as they apply to your communication controller: GCF, CDF, ZAP or MCF, BER, PRO, LDF, TIC, PSW, and DMP.

TYPE=B|S|N
Specifies whether the SNA device control blocks (S), the non-SNA device control blocks (N), or both (B) are to be formatted.

MOD=Y|N
Specifies whether the hexadecimal dump of the load module is to be printed.

MAP=Y|N
Specifies whether the load map of the load module is to be printed.[4]

TREE=Y|N
Specifies whether the inbound and outbound session routing binary search trees are to be formatted.

INDEX=Y|N
Specifies whether an index is to be printed at the end of the dump.[4]

Some of the parameters for the DUMP control statement are not mutually exclusive; for example, you can code the MOD and BUF parameters with the TOADDR and FROMADDR parameters, and all will affect the dump output.

[4] An IBM-compatible sort program must be available before you can use these parameters.

Job Control to Activate and Print an NCP Dump

You must establish several FILEDEFs before using the SSP dumper utility to dump and the SSP dump formatter utility to print the communication controller storage contents. To execute both Step 1 (IFLREAD) and Step 2 (IFLDUMP), issue the FILEDEFs before the first step. If the second step is carried out by itself, the same FILEDEFs are used.

To ensure that previously defined FILEDEFs are not in effect, clear all FILEDEFs by issuing the command FILEDEF * CLEAR *before* issuing the FILEDEFs for IFLREAD. When using IFLDUMP to format the MOSS or CSP dump, clear the FILEDEFs before issuing FILEDEFs for IFLDUMP.

The virtual channel and subchannel address where the communication controller is attached must be specified as a parameter when Step 1 (IFLREAD) is started. A DUMP control statement is required for Step 2 (IFLDUMP). The FILEDEFs needed to perform Steps 1 and 2 are as follows:

FILEDEF SYSUT2	Specifies the DASD work file onto which the contents of the communication controller are to be dumped, or the file on which the MOSS or CSP dump resides.
FILEDEF SYSPRINT	Specifies a sequential file-system output device, magnetic tape, or DASD volume onto which the dump program is to place the dump listing.
FILEDEF SYSIN	Specifies the file, or input stream, containing the utility control statement, DUMP. This file must have an LRECL of 80 and a RECFM of F.
FILEDEF SORTIN	Specifies a sequential file onto which the SSP dump formatter utility program is to place the dump listing.
FILEDEF SORTOUT	Specifies a sequential file to get the dump listing from.
FILEDEF INDXIN	Specifies a sequential file onto which the SSP dump formatter utility program is to place the dump index file.
FILEDEF INDXOUT	Specifies a sequential file to get the dump index from.
IFLREAD cuu	Specifies the name of the module used to dump communication controller storage and a parameter which is the communication controller address.

IFLDUMP	Specifies the name of the module used for the second step of the dump.

Example: Assume that (1) you want to dump an IBM 3725 Communication Controller attached as virtual address 104, (2) the dump listing will show the contents of communication controller storage from address X'000' to the end, and (3) NCP control blocks and buffer pool will be formatted. The following sample shows the FILEDEFs used to get the dump listing:

```
FILEDEF SYSUT2 DISK TEST DUMP A (RECFM F XTENT 62500)
FILEDEF SYSPRINT DISK PRINT LIST A
FILEDEF SYSIN DISK DUMP CARD A
FILEDEF SORTIN   DISK SORTIN FILE T (RECFM FBA)
FILEDEF SORTOUT  DISK SORTOUT FILE T (RECFM FBA)
FILEDEF INDXIN   DISK INDXIN FILE T (RECFM FBA)
FILEDEF INDXOUT  DISK INDXOUT FILE T (RECFM FBA)
```

After running these FILEDEFs, run the following statements to get the dump listing:

```
IFLREAD 104
IFLDUMP
```

where disk file DUMP CARD A contains:

```
DUMP FROMADDR=000,FORMAT=Y,BUF=F
```

This DUMP command must be preceded by two blank spaces.

Do not specify the BLKSIZE option.

LINECOUNT Parameter on the IFLDUMP Command

LINECOUNT is the only parameter recognized by the SSP dump formatter utility. This parameter specifies a decimal number from 10 to 99. It represents the number of lines for each page to be printed by the SSP dump formatter utility on the output that is produced. If the LINECOUNT parameter is omitted, or is given incorrectly, a default of 55 lines for each page is assumed.

Include the LINECOUNT parameter on the IFLDUMP command in one of two formats.

```
IFLDUMP  linecount nn
IFLDUMP  lc nn
```

Example: To specify that the SSP dump formatter utility print 40 lines on each page, call Step 2 (IFLDUMP) of the SSP dump formatter utility as follows:

```
IFLDUMP lc 40
```

Sample VM Procedures for Activating and Printing the Dump

Sample procedures for activating and printing the dump under VM are included on your licensed program tape. The file name of the sample for the SSP dumper utility is DUMPVM SMPLEXEC; the file name of the sample for the SSP dump formatter utility is DMFTVM SMPLEXEC. These procedures are provided to help you create and tailor the FILEDEFs in your VM environment.

Using Access Method Dump Commands

Use the procedures described in this section to dump NCP or transfer the MOSS or CSP dump.

Notes:

1. For the IBM 3725: If you want a MOSS, CSP, or TRSS dump, dump to diskette before invoking the access method. The MOSS or CSP dump may contain TRSS dump files. These files are transferred to the host when either MOSS or CSP is specified to the access method.
2. For the IBM 3720 and 3745: If you want a MOSS or CSP dump, dump to either diskette or disk, depending on the configuration of your communication controller and its operating mode. If you want a TRSS dump, however, you can dump only to diskette. Invoke the access method to transfer the dump to the host. The MOSS or CSP dump may contain the TRSS dump files. These files are transferred to the host when either MOSS or CSP is specified to the access method.

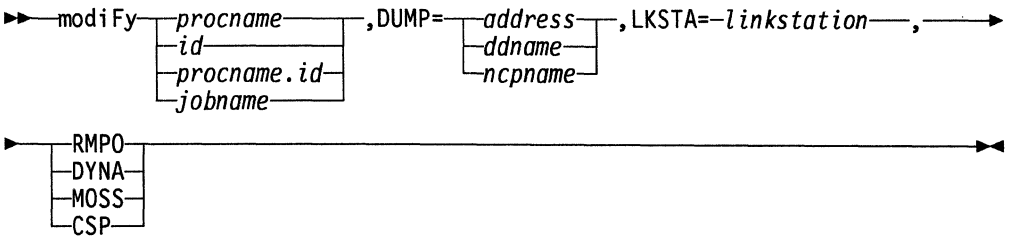
VTAM Operation

To dump NCP or transfer the contents of an NCP, CSP, or MOSS dump using VTAM, use the MODIFY DUMP command. For more information about this command, see *VTAM Operation.*

Note: You must have VTAM V3R2 to use this command for an IBM 3720 Communication Controller's disk.

TCAM Operation

To transfer the contents of an NCP, CSP, or MOSS dump using TCAM, use the following command:



procname
The name of a cataloged procedure in SYS1.PROCLIB that starts the TCAM message control program to which you are issuing this command.

id
An alternate name that can be specified for *procname.*

procname.id
The name used in the START TCAM command when TCAM was started. The same *id* variable must be specified when used in any succeeding TCAM command.

jobname
A name used only when TCAM is loaded and executed from the input stream.

address
The address of NCP. This keyword is valid only for channel-attached communication controllers.

ddname
The ddname of NCP. This keyword is valid only for channel-attached communication controllers.

ncpname
The name of NCP.

linkstation
The name of a link station for dumping over a link.

RMPO
Causes the link-attached communication controller to be dumped and then powered off. This keyword cannot be specified if DYNA, MOSS, or CSP is used.

DYNA
Specifies transfer of the communication controller storage dynamically.

MOSS
Specifies transfer of the MOSS dump.

CSP
Specifies transfer of the CSP dump.

Printing Dumps Transferred by Access Method Dump Commands

If you used the VTAM facility to dump the contents of communication controller storage to a direct-access file (Step 1, IFLREAD), run an independent job on CMS to produce a readable dump listing (Step 2, IFLDUMP). These steps cannot be executed under GCS. The following statements are needed to execute Step 2 (IFLDUMP):

```
FILEDEF SYSUT2      Specifies the DASD work file
                    containing the storage contents,
                    MOSS dump, or CSP dump.

FILEDEF SYSPRINT    Specifies a sequential file
                    where the SSP dump formatter utility
                    program will place the dump listing.

FILEDEF SORTIN      Specifies a sequential file
                    where the SSP dump formatter utility
                    will place the dump listing.

FILEDEF SORTOUT     Specifies a sequential file
```

	containing the dump listing.
FILEDEF INDXIN	Specifies a sequential file where the SSP dump formatter utility will place the dump index file.
FILEDEF INDXOUT	Specifies a sequential file containing the dump index file.
FILEDEF SYSIN	Specifies the file (input stream) containing the dump control statement.
IFLDUMP	Specifies the name of the module generated for the second step of the dump.

Example: Assume that VTAM dumped a communication controller onto a disk file called VTAM DUMP. The following sample shows the FILEDEFs used to get the dump listing:

```
FILEDEF SYSUT2 DISK VTAM DUMP A (RECFM F BLKSIZE 2048 XTENT 62500)
FILEDEF SYSPRINT DISK PRINT LIST A
FILEDEF SYSIN DISK DUMP CARD A
```

where disk file DUMP CARD A contains:

```
DUMP FROMADDR=000,FORMAT=Y,BUF=F
```

After running the FILEDEFs given in the example, issue:

```
IFLDUMP
```

Example: Assume that VTAM transferred a MOSS dump onto a disk file called VTAM DUMP. The following sample shows the FILEDEFs used to get the dump listing and the IBM 3725 error log:

```
FILEDEF SYSUT2 DISK VTAM DUMP A
FILEDEF SYSPRINT DISK PRINT LIST A
FILEDEF SYSIN DISK DUMP CARD A
```

where disk file DUMP CARD A contains:

```
DUMP PRINT=(DMP,BER)
```

After running the FILEDEFs given in the example, issue:

```
IFLDUMP
```

Chapter 9. Using the SSP Dump Utilities in VSE

To dump NCP in a channel-attached communication controller, invoke either the VTAM dumper utility or a stand-alone job using the SSP dumper utility. To dump a link-attached communication controller, use the VTAM dumper utility. For information on the VTAM dumper utility, see "Using Access Method Dump Commands" on page 234.

Use the SSP dumper utility to dump the storage contents of the IBM 3720, 3725, or 3745 Communication Controller in VSE. This utility includes two separately called programs:

Step 1. IFUREAD dumps the storage contents of the communication controller and copies them to a direct-access file (SYS008).

Step 2. IFUDUMP produces a formatted copy of the communication controller's storage contents and places that copy on a sequential output file (SYSLST). The SYS008 file from Step 1 serves as input to this step.

If you use the VTAM dumper utility to dump the communication controller storage, the dump process stops after the storage contents of the communication controller are dumped and copied to a direct-access file. To produce a formatted dump listing, run a stand-alone job to execute Step 2 (IFUDUMP). If, on the other hand, you invoke the SSP dumper utility, Step 2 executes immediately after Step 1 (IFUREAD). In the JCL, these two steps appear to be one job step.

Host Processor and Communication Controller Requirements

You can run the host processor module of the SSP dumper utility in any host processor that accommodates VSE. The SSP dumper utility operates in a minimum virtual partition. You can calculate the amount of work file space required as equal to the size of the communication controller storage, in KB, plus 6KB.

For information on dumping communication controller storage using the VTAM dump facility, see *VTAM Operation*.

Dumping Communication Controller Storage

Dumping from the communication controller to the direct access work file is the first step of the SSP dumper utility. Step 1 (IFUREAD) of the SSP dumper utility transfers the contents of the communication controller's storage and local storage registers to the host processor, which places them on a direct access file. When the dumping process is complete, the SSP dumper utility informs the host processor operator. At this point, the communication controller is unusable and must be reloaded with an NCP using the SSP loader utility (or the VTAM loader facility).

For the JCL needed to both dump and print the contents of communication controller storage, see "Job Control to Activate and Print an NCP Dump" on page 229.

Using the SSP Dump Formatter Utility

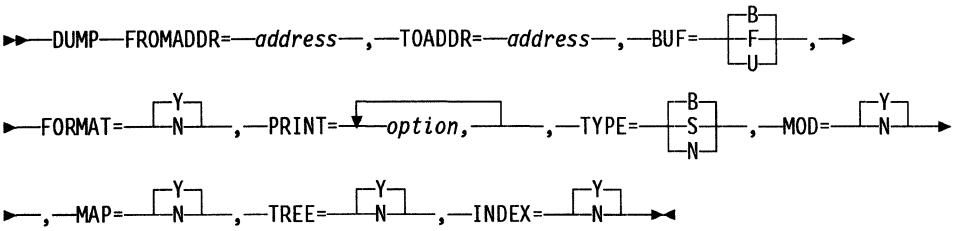
The formatting step, Step 2 (IFUDUMP), of the SSP dumper utility is the SSP dump formatter utility. It formats all or a selected part of the dumped data and then places the data on a sequential output file. The output listing shows the hexadecimal representation of communication controller storage and register contents and gives the character equivalents of all EBCDIC bit patterns that represent characters. Several additional options can be specified by the DUMP control statement:

- List the complete contents, or any specified section, of storage.
- Format or unformat the buffer pool. The FORMAT option displays the buffer pool area of communication controller storage as individual buffers. The UNFORMAT option does not individually format the buffers.
- Format or unformat NCP control blocks. The FORMAT option labels and prints network node control blocks at the beginning of the dump listing for convenient reference. It also formats and shows the branch trace table at the end of the dump. UNFORMAT does not format the control blocks or branch trace table.
- Print the MOSS or CSP dump with any of the nine files that are contained within these dumps.

  For information on how to obtain MOSS and CSP dump data, see "Using Access Method Dump Commands" on page 234.

The DUMP Control Statement

The SSP dump formatter utility requires one control statement, DUMP, in the input job stream. This statement specifies your choice of the options. The control statement format is as follows.



FROMADDR=*address*
Specifies the lower limit of the communication controller storage to appear on the listing. If you omit FROMADDR, the listing starts at address X'000'.

TOADDR=*address*
Specifies the upper limit of the communication controller storage to appear on the listing. If you omit TOADDR, the listing ends at the upper limit of storage. If you specify a value higher than the upper limit of storage, the SSP dump formatter utility issues message IFW201I and dumps the storage contents.

BUF=B|F|U
Specifies whether the SSP dump formatter utility is to print the formatted (F) NCP buffer pool, the unformatted buffers (U), or both (B).

FORMAT=Y|N
Specifies whether the SSP dump formatter utility is to format NCP control blocks and the branch trace table.

PRINT
Specifies whether the SSP dump formatter utility is to print any or all of nine available reports. These reports are:

- Configuration data file (CDF)
- MOSS or CSP dump (DMP)
- Microcode fixes (ZAP or MCF)
- Error log (BER)
- Port swap file (PSW)
- "Canned" testing procedures (PRO)
- Graphic machine configuration file (GCF)
- Line description file (LDF)
- Token-ring interface coupler (TIC) file.

Depending on your model of communication controller, some of these files may be unavailable. If you request a report that is not available for a particular model, an informational message is produced. Use commas between report names. The reports are printed in the order that you specify. If you omit the PRINT keyword, all the files are printed in the following order as they apply to your communication controller: GCF, CDF, ZAP or MCF, BER, PRO, LDF, TIC, PSW, and DMP.

TYPE=B|S|N
Specifies whether the SNA device control blocks (S), the non-SNA device control blocks (N), or both (B) are to be formatted.

MOD=Y|N
Specifies whether the hexadecimal dump of the load module is to be printed.

MAP=Y|N
Specifies whether the load map of the load module is to be printed.[5]

TREE=Y|N
Specifies whether the inbound and outbound session routing binary search trees are to be formatted.

INDEX=Y|N
Specifies whether an index is to be printed at the end of the dump.[5]

Some of the parameters for the DUMP control statement are not mutually exclusive; for example, you can code the MOD or BUF parameter with the TOADDR and FROMADDR parameters, and all will affect the dump output.

Job Control to Activate and Print an NCP Dump

To use the SSP dumper utility to dump and the SSP dump formatter utility to print the communication controller's storage contents, you provide JCL only for Step 1 (IFUREAD) in the dumping process and one or more DUMP statements for Step 2 (IFUDUMP). Step 1 generates the required control statements for Step 2. If you have used the access method to dump NCP, you must now perform Step 2 of the dump process. To perform Step 2, substitute the name IFUDUMP for the name IFUREAD in the EXEC statement.

[5] An IBM-compatible sort program must be available before you can use these parameters.

The statements needed to perform Steps 1 and 2 are as follows:

// JOB		Initiates the job.
// ASSGN	SYS007	Specifies the unit address of the communication controller to be dumped. You may omit this statement if a permanent assignment was made for the controller during the NCP generation process.
// ASSGN	SYS008,X'nnn'	Specifies the unit address of the direct-access device that contains the dump file. You must define the file with DLBL and EXTENT statements if the file was not permanently assigned. The DLBL statement must have a file ID of NCPDUMP. To calculate the amount of space needed for SYS008, add 6KB to the size of the communication controller storage in kilobytes. For example, to determine the space in a communication controller with 4MB of storage, convert the 4MB to kilobytes and add 6KB: ((4 x 1024 x 1024) + 6196) bytes. **IBM 3745 at EC Level A47014 or IBM 3745-130, -150, or -170 EC Level A73290)**: SYS008 is written at 2048 byte records. If you do not know the EC level of your communication controller, you should use a block size of 512 in your calculation. This block size ensures enough space is allocated for the dump file.
// ASSGN	SYS001,X'nnn'	Specifies the unit address of the direct-access device that contains the sort routine output file. You must define the file with DLBL and EXTENT statements if the file was not permanently assigned. The DLBL statement must have a file ID of SORTOUT.

// ASSGN	SYS002,X'nnn'	Specifies the unit address of the direct-access device that contains the sort routine input file. You must define the file with DLBL and EXTENT statements if the file was not permanently assigned. The DLBL statement must have a file ID of SORTIN1.
// ASSGN	SYS003,X'nnn'	Specifies the unit address of the direct-access device that contains the sort routine input file. You must define the file with DLBL and EXTENT statements if the file was not permanently assigned. The DLBL statement must have a file ID of SORTIN2.
// ASSGN	SYS004,X'nnn'	Specifies the unit address of the direct-access device that contains the sort routine work area. You must define the file with DLBL and EXTENT statements if the file was not permanently assigned. The DLBL statement must have a file-ID of SORTWK1.
// LIBDEF		Specifies the location of the SSP dump formatter utility program.
// EXEC		Specifies the programs IFUREAD or IFUDUMP.

Note: The symbolic unit address of the communication controller and the dump file must be SYS007 and SYS008, respectively, as shown in the example of the JCL used to get a dump listing.

Example: Assume that (1) you want to dump a communication controller with a unit address of 019, (2) the dump listing will show the contents of communication controller storage from address X'000' to the end, and (3) NCP control blocks and buffer pool will be formatted.

The following sample shows the JCL to get the dump listing:

```
//       JOB       DUMP
//       LIBDEF    PHASE,SEARCH=(SSPLIB.DUMPFORM),TEMP
//       ASSGN     SYS007,X'019'
//       DLBL      NCPDUMP,'NCP3DUMP',,DA
//       EXTENT    SYS008,111111,,,2000,80
//       ASSGN     SYS008,X'131'
//       DLBL      SORTOUT,'SORTOUT',,SD
//       EXTENT    SYS001,111111,,,3000,90
//       ASSGN     SYS001,X'131'
//       DLBL      SORTIN1,'SORTIN1',,SD
//       EXTENT    SYS002,111111,,,3090,90
//       ASSGN     SYS002,X'131'
//       DLBL      SORTIN2,'SORTIN2',,SD
//       EXTENT    SYS003,111111,,,3180,90
//       ASSGN     SYS003,X'131'
//       DLBL      SORTWK1,'SORTWK1',,SD
//       EXTENT    SYS004,111111,,,3270,90
//       ASSGN     SYS004,X'131'
//       EXEC      IFUREAD
         DUMP      FROMADDR=000,FORMAT=Y,BUF=F
/*
/&
```

Link-Editing Modules from the Relocatable Library

If the host processor modules of the independent SSP dumper utility are cataloged in the relocatable library, use the following JCL to link-edit them into the core image library:

```
//       JOB       LINKDUMP
//       LIBDEF    OBJ,SEARCH=(SSPLIB.DUMPFORM)
//       LIBDEF    PHASE,CATALOG=(SSPLIB.DUMPFORM),PERM
//       OPTION    CATAL
         INCLUDE   IFUWLINK
//       EXEC      LNKEDT
/*
/&
```

The use of fixed block architecture devices, such as the IBM 3310 or 3370, is implemented in the dump routines using VSAM as an access method. VSAM data space must be allocated to receive the dump data. The following example shows how to allocate the data space for a 1MB communication controller and the JCL needed to run the SSP dumper utility. When using this example, apply the characteristics of your particular installation.

```
// JOB                    VSAMFILE (Define a relative record file)
// DLBL                   IJSYSCT,'VSAM.MASTER.CATALOG',,VSAM
// EXTENT                 SYSCAT,DT1301
// DLBL                   NCPDUMP,'NCPDUMP',,VSAM
// EXTENT                 SYSCAT,DT1301,,,2900,500
// EXEC                   IDCAMS,SIZE=AUTO
   DEFINE CLUSTER                                -
            NAME(NCPDUMP)                        -
            FILE(NCPDUMP)                        -
            NONINDEXED                           -
            RECORDSIZE(2048 2048)                -
            TRACKS(500 1)                        -
            REUSE                                -
            VOL(DT1301)                          -
            CATALOG(VSAM.MASTER.CATALOG)
/*
/&
// JOB DUMPIT    (Dump a 3720, 3725, or 3745 to disk using VSAM)
// OPTION        DUMP
// LIBDEF        PHASE,SEARCH=(SSPLIB.DUMPFORM)
// DLBL          NCPDUMP,'NCPDUMP',,SD
// ASSGN         SYS008,X'120'
// DLBL          SORTOUT,'SORTOUT',,SD
// EXTENT        SYS001,DT1301,,,3000,90
// ASSGN         SYS001,X'120'
// DLBL          SORTIN1,'SORTIN1',,SD
// EXTENT        SYS002,DT1301,,,3090,90
// ASSGN         SYS002,X'120'
// DLBL          SORTIN2,'SORTIN2',,SD
// EXTENT        SYS003,DT1301,,,3180,90
// ASSGN         SYS003,X'120'
// DLBL          SORTWK1,'SORTWK1',,SD
// EXTENT        SYS004,DT1301,,,3270,90
// ASSGN         SYS004,X'120'
// ASSGN         SYS007,X'041'
// EXEC          IFUREAD
   DUMP          FORMAT=Y
/*
/&
```

Using Access Method Dump Commands

Use the procedures described in this section to dump NCP or transfer the MOSS or CSP dump.

Notes:

1. **IBM 3725:** If you want a MOSS, CSP, or TRSS dump, dump to diskette before invoking the access method. The MOSS or CSP dump may contain TRSS dump files. These files are transferred to the host when either MOSS or CSP is specified to the access method.
2. **IBM 3720 and 3745:** If you want a MOSS or CSP dump, dump to either diskette or disk, depending on the configuration of your communication controller and its operating mode. If you want a TRSS dump, however, you can dump only to diskette. Invoke the access method to transfer the dump to the host. The MOSS or CSP dump may contain the TRSS dump files. These files are transferred to the host when either MOSS or CSP is specified to the access method.

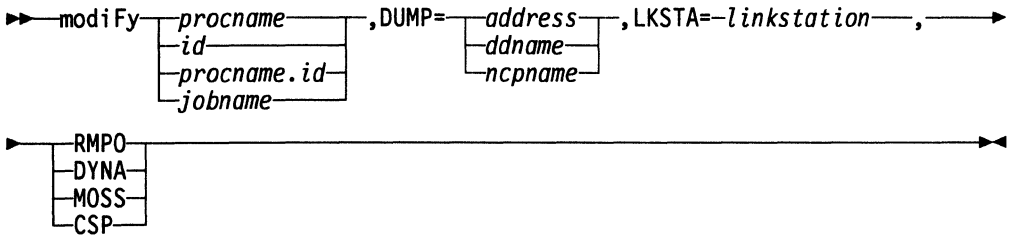
VTAM Operation

To dump NCP or transfer the contents of an NCP, CSP, or MOSS dump using VTAM, use the MODIFY DUMP command. For more information about this command, see *VTAM Operation*.

Note: You must have VTAM V3R2 to use this command for an IBM 3720 Communication Controller's disk.

TCAM Operation

To transfer the contents of an NCP, CSP, or MOSS dump using TCAM, use the following command:



procname
The name of a cataloged procedure in SYS1.PROCLIB that starts the TCAM message control program to which you are issuing this command.

id
An alternate name that can be specified for *procname.*

procname.id
The name used in the START TCAM command when TCAM was started. The same *id* variable must be specified when used in any succeeding TCAM command.

jobname
A name used only when TCAM is loaded and executed from the input stream.

address
The address of NCP. This keyword is valid only for channel-attached communication controllers.

ddname
The ddname of NCP. This keyword is valid only for channel-attached communication controllers.

ncpname
The name of NCP.

linkstation
The name of a link station for dumping over a link.

RMPO
Causes the link-attached communication controller to be dumped and then powered off. This keyword cannot be specified if DYNA, MOSS, or CSP is used.

DYNA
Specifies transfer of the communication controller storage dynamically.

MOSS
Specifies transfer of the MOSS dump.

CSP
Specifies transfer of the CSP dump.

Printing Dumps Transferred by Access Method Dump Commands

If you used the VTAM facility to dump the contents of communication controller storage to a direct-access file, run an independent job to produce a readable dump listing. The JCL statements needed are as follows.

```
// JOB                          Initiates the job.

// ASSGN      SYS008,X'nnn'     Specifies the unit address
                                of the direct-access device
                                that contains the dump file.
                                Unless it is permanently assigned,
                                define the file
                                with DLBL and EXTENT statements.
                                Note that VTAM applies a
                                file ID of NCPDUMP to
                                the dump file it creates.

// ASSGN      SYS001,X'nnn'     Specifies the unit
                                address of the direct-access device that
                                contains the sort routine output file.
                                Unless it is permanently assigned,
                                define the file
                                with DLBL and EXTENT statements.
                                The DLBL statement must have a
                                file ID of SORTOUT.

// ASSGN      SYS002,X'nnn'     Specifies the unit
                                address of the direct-access device that
                                contains the sort routine input file.
                                Unless it is permanently assigned,
                                define the file
                                with DLBL and EXTENT statements.
                                The DLBL statement must have a
                                file ID of SORTIN1.

// ASSGN      SYS003,X'nnn'     Specifies the unit
                                address of the direct-access device that
                                contains the sort routine input file.
                                Unless it is permanently assigned,
                                define the file
                                with DLBL and EXTENT statements.
                                The DLBL statement must have a
                                file ID of SORTIN2.

// ASSGN      SYS004,X'nnn'     Specifies the unit
                                address of the direct-access device that
                                contains the sort routine work area.
                                Unless it is permanently assigned,
                                define the file
                                with DLBL and EXTENT statements.
                                The DLBL statement must have a
                                file ID of SORTWK1.

// EXEC       IFUDUMP           Specifies the program IFUDUMP.
```

Example: Assume that VTAM dumped the storage contents of a communication controller onto a file whose unit address is 131. The following sample shows the JCL required to get the dump listing:

```
//      JOB      DUMPRT
//      LIBDEF   PHASE,SEARCH=(SSPLIB.DUMPFORM),TEMP
//      ASSGN    SYS008,X'131'
//      DLBL     NCPDUMP,'NCP3DUMP',,DA
//      EXTENT   SYS008,111111
//      DLBL     SORTOUT,'SORTOUT',,SD
//      EXTENT   SYS001,111111,,,3000,90
//      ASSGN    SYS001,X'131'
//      DLBL     SORTIN1,'SORTIN1',,SD
//      EXTENT   SYS002,111111,,,3090,90
//      ASSGN    SYS002,X'131'
//      DLBL     SORTIN2,'SORTIN2',,SD
//      EXTENT   SYS003,111111,,,3180,90
//      ASSGN    SYS003,X'131'
//      DLBL     SORTWK1,'SORTWK1',,SD
//      EXTENT   SYS004,111111,,,3270,90
//      ASSGN    SYS004,X'131'
//      EXEC     IFUDUMP
         DUMP     FROMADDR=000,FORMAT=Y,BUF=F
/*
//
```

Note: SORT dtfnames are not necessary for printing the MOSS or CSP dump.

Example: Assume that VTAM transferred the contents of a MOSS dump onto a file whose unit address is 131. The following sample shows the JCL required to obtain the dump listing and the IBM 3725 error log:

```
//      JOB      DUMPRT
//      LIBDEF   PHASE,SEARCH=(SSPLIB.DUMPFORM),TEMP
//      ASSGN    SYS008,X'131'
//      DLBL     NCPDUMP,'NCP3DUMP',,DA
//      EXEC     IFUDUMP
         DUMP     PRINT=(DMP,BER)
/*
//
```

Note: SORT dtfnames are not necessary for printing the MOSS or CSP dump.

Chapter 10. Using the Dynamic Dump Utility in EP

The dynamic dump utility is available to NCP users who are also running EP in a PEP environment. Use this utility when trouble or error conditions indicate that a dynamic dump of communication controller storage can help to isolate a problem. This chapter explains how to use the dynamic dump utility to send communication controller storage to the host without interfering with NCP or EP execution.

The dynamic dump utility uses an EP subchannel to send communication controller storage to the host without interfering with NCP or EP execution. To use the dynamic dump utility for NCP or EP running in PEP, code the DYNADMP keyword on the BUILD definition statement. For more information on the BUILD definition statement, see *NCP, SSP, and EP Resource Definition Reference*.

For operating systems that need a device type defined during system generation, specify the dynamic dump subchannel address as an IBM 3720, 3725, or 3745.

NCP V5R4 and NCP V6R1 and Later: During dynamic dump processing the dispatcher trace is disabled. It returns to its previous status when the dynamic dump is complete.

The dynamic dump utility is an optional SSP utility that can:

- Obtain the following without terminating the program:
  - A storage dump from location 0 through the end of storage of the communication controller
  - A printout of the entire storage dump
  - A display on the operator's console at the host processor of sections of communication controller storage (up to 144 bytes) starting at any location
  - A dump of only the emulation mode trace table.
- Activate or deactivate the EP line trace or scanner interface trace (SIT) functions.
- Get a dynamic dump of EP trace table entries as they are entered into the trace table, and SIT entries as they are produced.

The dynamic dump utility physically consists of two modules. One module resides in the host processor (as load module IFLSVEP), and the other resides in the communication controller as part of EP. (The module for the communication controller is included in the program only if DYNADMP=YES is specified on the BUILD definition statement during program generation). The two dynamic dump modules communicate to transfer specified communication controller storage to the host module. If the DISPLAY command is used to enter a request, the transferred storage data is displayed at the operator's console. Otherwise, the host module writes the received data to the work data set in 516-byte blocks. You can then invoke the print function of the dynamic dump utility to print the contents of this work data set.

When a particular user request is satisfied, the host module of the dynamic dump utility issues message IFL503I to inform the operator that the transfer of data to the work data set is complete.

Use control statements to request the various functions of the dynamic dump utility. Include these control statements in the SYSIN data set (input stream), or enter them by way of the operator's console.

Initially, the dynamic dump utility reads control statements from the SYSIN data set until it reads either an END statement or a PAUSE statement. The PAUSE statement instructs the dynamic dump utility to read control statements from the operator's console until either an END statement or a SYSIN statement is entered at the operator's console. The SYSIN statement instructs the dynamic dump utility to return to the SYSIN data set for control statements beginning with the next statement after the last PAUSE statement. An END statement either in the SYSIN data set or from the operator's console causes the dynamic dump utility to terminate.

The dynamic dump utility provides the following types of output:

- *Work Data Set or File*: This is a temporary data set or file where the storage contents are written. This data set or file usually resides on a tape unit.
- *Work Data Set or File*: This is a temporary data set or file where the SIT contents are written. This data set or file usually resides on a tape unit.
- *Output Data Set or File*: This is the data set or file on which the trace or the storage dump is printed from the work data set or file. It also contains the dynamic dump control statements and applicable error messages.
- *Operator's Console*: The operator's console at the host processor can receive output because of a DISPLAY statement, control statement responses, or error conditions.

Coding DYNADMP for Channels

DYNADMP may be active on only one channel at a time. Use the following coding to define DYNADMP for channels:

- If you transfer dynamic dump data over the emulation subchannel of the first channel adapter, code DYNADMP=(YES,*adr0*).
- If the communication controller has two channel adapters, code DYNADMP=(YES,*adr0,adr1*) to permit dump data transfer over a specified emulation subchannel of each of the channel adapters. Code DYNADMP=(YES,NONE,*adr1*) to permit transfer over only the specified subchannel of the second channel adapter.

Table 10 on page 241 shows how DYNADMP represents subchannels used to transfer dynamic dump data to the host processor.

Table 10. Subchannel Address Specification for Dynamic Dump Data Transfer

If CA=	To Allow Dynamic Dump Data Transfer over These Emulation Sub-channels	Code DYNADMP=
TYPE5	ESC[1]	(YES,*adr1*)
(TYPE,TYPE5)	ESC[1]	(YES,*adr0*)
	ESC[2]	(YES,NONE,*adr1*)
	ESC[1] and ESC[2]	(YES,*adr0,adr1*)

Superscripts indicate channel adapter position:

[1] Adapter address 0, position 1
[2] Adapter address 1, position 2

Coding DYNADMP for Channel Links

For channel links, you transfer dynamic dump data over an emulation subchannel associated with the channel adapter you defined using ADDRESS. Code DYNADMP=*adr*.

NCP Dynamic Storage Display

Use the NCP dynamic storage display to examine NCP storage contents and the contents of a dump on the communication controller's disk, without stopping the execution of NCP. The actual contents of NCP storage may change by the time your request executes and displays the results, unless you are displaying a dump on the communication controller disk.

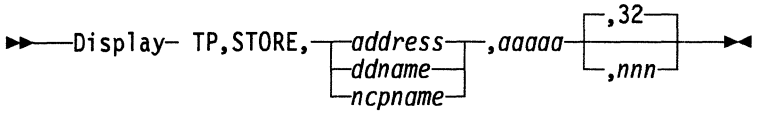
To get a dynamic display of NCP storage, use the DISPLAY NCP STORAGE command. This command lets you display up to 256 bytes of NCP storage data on the operator's console of the host processor while NCP remains active. Using VTAM, you can also display up to 256 bytes of an NCP dump or state vector stored on the disk. To use this command, include STORDSP in the options field of the SYSCNTRL definition statement. For more information on the SYSCNTRL definition statement, see *NCP, SSP, and EP Resource Definition Reference*.

VTAM Operation

To dynamically display NCP storage using VTAM, use the DISPLAY NCPSTOR command. For more information about the DISPLAY NCPSTOR command, see *VTAM Operation*.

TCAM Operation

To dynamically display NCP storage using TCAM, use the following command:



address
Specifies the subchannel address of the communication controller you want to dump.

ddname
Specifies the symbolic label of the DD statement that defines the DCB for the communication controller you want to dump.

ncpname
Specifies the symbolic name of the communication controller you wish to dump as specified on the TERMINAL definition statement defining NCP. For more information on the TERMINAL definition statement, see *NCP, SSP, and EP Resource Definition Reference*.

aaaaa
Specifies the address of the first byte of storage to be displayed.

nnn
Specifies the number of bytes of storage to be displayed. The maximum value is 256; the default is 32.

You can also include a short user-written routine that increments the address of the first byte of storage to be displayed each time. This allows you to display the NCP storage contents. The storage contents may change while your request is being formatted for transmission.

Dynamic Dump Utility in MVS

The following section discusses how to use the dynamic dump utility in MVS.

Host Processor and Communication Controller Requirements

The host processor module of the dynamic dump utility can run in any host processor that accommodates OS/VS2 (MVS). The OS/VS2 (MVS) dynamic dump utility operates in a minimum virtual region. Calculate the number of 516-byte blocks required for work data set space for SYSUT2 as equal to twice the size of the communication controller storage, in KB, plus 1.

If you request a dynamic dump of trace table entries, you must ensure that the work data set is large enough to hold all the trace data being dumped. It is preferable to use a tape unit for this activity.

NCP, SSP, and EP Resource Definition Reference shows the valid ways the DYNADMP keyword on the BUILD definition statement is used to specify subchannels for the transfer of dynamic dump data to the host processor.

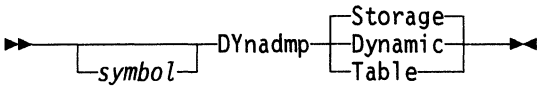
Utility Control Statements

With the dynamic dump utility control statements, you can:

- Get a full or partial storage dump
- Display a section of storage
- Print the work data set to be sent to the output data set
- Request a line trace or SIT
- Allow the selection of available channel adapters
- Allow control statements to be entered after the PAUSE control statement
- End a job and stop the program after the trace output is printed
- Cause control statements to be read from the input stream.

DYNADMP Control Statement

The DYNADMP control statement requests a dump of the entire communication controller storage or a specified section. The communication controller does not become idle and does not require reloading.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

Dynamic specifies that the line or SIT tables are to be dumped dynamically as entries are made. This type of dump requires operator intervention to stop the trace. Before starting a dynamic trace dump, start a trace on a communication line using the control panel of the communication controller or using the dynamic dump utility (the OPTION control statement).

Storage specifies that the entire contents of communication controller storage are to be dumped. NCP execution continues both during the operation and after the storage contents have been dumped. Storage is the default keyword if no keyword is specified.

Table specifies that only the trace table section of communication controller storage is to be dumped.

DISPLAY Control Statement

The DISPLAY control statement displays a section of the communication controller storage on the operator's console at the host processor.

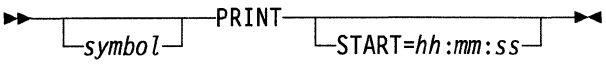
symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Omit a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

hhhhhh specifies the beginning address, in hexadecimal, of the storage to be displayed.

n specifies the number of lines (16 bytes of storage for each line) to be displayed. The maximum number of lines you may specify is 9. If *n* is omitted, 1 is the default.

PRINT Control Statement

The PRINT control statement requests that a printout (32 bytes of storage for each line) of the complete work data set (SYSUT2) be sent to the SYSPRINT device (the output data set).



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

START=hh:mm:ss (hours:minutes:seconds) specifies that only those trace blocks that were written to the work data set after time hh:mm:ss are to be printed.

hh:mm:ss specifies a time that is both later than (or equal to) the time stamp associated with the first trace block and earlier than (or equal to) the time stamp associated with the last trace block on the work data set. Otherwise, message IFL5101 is issued to show that no trace blocks that satisfied the PRINT command were found.

Example 1: Assume that the first trace block is recorded at 09:05:00 (9:05 a.m.) and the last is recorded at 09:20:00 a.m. The statement PRINT START=09:17:30 prints trace blocks recorded between 9:17:30 a.m. and 9:20 a.m.

The print function correctly interprets a postmidnight time stamp (for a last-written trace block) as later than a premidnight time stamp (for a first-written trace block), even though the numeric value of hh:mm:ss is lower for the postmidnight time (for example, the values 23:55:00 and 00:02:00 could represent the 7-minute interval from 11:55 p.m. to 12:02 a.m.).

Example 2: Assume that a trace is started just before midnight. If the first trace block was written to the work data set at 23:25:23 (11:25 p.m.) and the last was written at 00:40:57 (12:40 a.m. the following day), then either of the following PRINT statements produces the intended results:

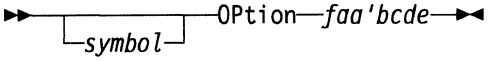
```
PRINT     START=23:40:00   (Trace entries written to the work data
                           set between 11:40 p.m. and 12:40 a.m. are
                           printed.)

PRINT     START=00:20:00   (Trace entries written to the work data
                           set between 12:20 a.m. and 12:40 a.m. are
                           printed.)
```

If you omit the START keyword, the complete work data set is printed.

If you specify the START keyword and there are storage dumps in the work data set with the trace blocks, these storage dumps are also printed regardless of whether they satisfy the START constraint. Storage dumps are not time stamped.

OPTION Control Statement

The OPTION control statement requests a line trace or SIT and allows the selection of any of the available channel adapters. Also, the OPTION statement starts, stops, or alters the program interrupt levels being traced. OPTION traces level 2 interrupts (line data), level 3 interrupts (time-out complete or channel data such as initial selection, data, and status), or both. OPTION continuously traces level 1 error log entries after a level 3 trace is started.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

faa'bcde specifies the trace functions desired: the start trace or stop trace, the channel adapter to trace, the SIT options and the line trace data options, the program level to trace, and the subchannels to trace. The values for *f, a, a', bc,* and *de* and their meanings are as follows.

f	a	a'	bc	de	Meaning (L=level)
4	*n*[1]	4	00	xx	Start SIT without line data on subchannel xx.
4	*n*[1]	6	00	xx	Start SIT with line data on subchannel xx.
4	*n*[1]	4	01	xx	Stop SIT on subchannel xx.
4	*n*[1]	0	10	xx	Start L2 trace without line data on subchannel xx.
4	*n*[1]	1	10	xx	Start L2 trace with data on subchannel xx.
4	*n*[1]	4	10	xx	Start SIT without line data on subchannel xx. Start L2 trace without line data on subchannel xx.
4	*n*[1]	5	10	xx	Start SIT without line data on subchannel xx. Start L2 trace with data on subchannel xx.

[1] Channel adapter:

Number 1–2 for the IBM 3720
Number 1–6 for the IBM 3725
Logical address 0–F for the IBM 3745.

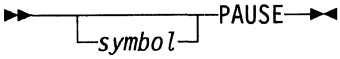
f	a	a'	bc	de	Meaning (L=level)
4	*n*[1]	6	10	xx	Start SIT with line data on subchannel xx. Start L2 trace without line data on subchannel xx.
4	*n*[1]	7	10	xx	Start SIT with line data on subchannel xx. Start L2 trace with data on subchannel xx.
4	*n*[1]	0	11	xx	Stop L2 trace on subchannel xx.
4	*n*[1]	4	11	xx	Stop SIT on subchannel xx. Stop L2 trace on subchannel xx.
4	*n*[1]	0	20	xx	Start L3 trace on subchannel xx.
4	*n*[1]	4	20	xx	Start SIT without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	6	20	xx	Start SIT with line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	0	21	xx	Stop L3 trace on subchannel xx.
4	*n*[1]	4	21	xx	Stop SIT on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	0	30	xx	Start L2 trace without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	1	30	xx	Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	4	30	xx	Start SIT without line data on subchannel xx. Start L2 trace without data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	5	30	xx	Start SIT without line data on subchannel xx. Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	6	30	xx	Start SIT with line data on subchannel xx. Start L2 trace without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	7	30	xx	Start SIT with line data on subchannel xx. Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	0	31	xx	Stop L2 trace on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	4	31	xx	Stop SIT on subchannel xx. Stop L2 trace on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	0	70	00	Start L3 trace on defined subchannel.
4	*n*[1]	0	71	00	Stop L3 trace on defined subchannel.
4	*n*[1]	0	70	FF	Start L3 trace on all subchannels.
4	*n*[1]	0	71	FF	Stop L3 trace on all subchannels.

[1] Channel adapter:

Number 1–2 for the IBM 3720
Number 1–6 for the IBM 3725
Logical address 0–F for the IBM 3745.

PAUSE Control Statement

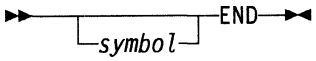
The PAUSE control statement allows control statements to be entered at the console of the host processor after the PAUSE statement is read from the input job stream or entered from the console.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Omit a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

END Control Statement

The END control statement specifies the end of job and stops the program after the trace output has been printed.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

This control statement does not end the trace. You must stop the trace from the console. Press the console Interrupt key to establish operator communication with the host processor for a background partition. Reply 'MSG Fx' to the attention routine for foreground partition Fx.

SYSIN Control Statement

The SYSIN control statement causes control statements to be read from the input stream.

Obtaining a Dynamic Dump of Trace Entries

To dynamically dump the EP line trace table entries or SIT records, first start the traces on the desired range of EP subchannels using the OPTION control statement. Then, to begin the transfer of trace entries (trace blocks) to the dynamic dump utility host module, enter the DYNADMP DYNAMIC control statement. The operator's console receives message IFL505E, which requires a response. Reply *S* to this message to stop the transfer of trace blocks to the host module.

The trace blocks can be written to two different work data sets, depending on which traces are active. If only the line trace is active, the trace blocks are written to SYSUT2. If only SIT is active, the trace blocks are written to SYSUT3. If both the line trace and SIT are active, both line and SIT records are written to SYSUT3, but only line trace records are written to SYSUT2.

Each trace block received by the host module is time-stamped before being written to the work data set. The time stamp, in the format hh:mm:ss (hours:minutes:seconds), shows the time when the host module received the trace block. Periodically, IFL508I messages appear at the operator console. Typical IFL508I messages are:

```
IFL508I SIT BLOCK        200 WRITTEN AT 13:28:20
IFL508I TRACE BLOCK      200 WRITTEN AT 13:28:37
```

Stopping Trace Activity

To stop the trace activity, the operator must first respond with *S* to the message (IFL505E) issued when the trace is started. The *S* response stops the transfer of trace blocks to the host module when the next trace block is received.

If you are dynamically dumping the SIT, or communication controller line trace entries, and the controller's DYNADMP module has stopped sending trace blocks to the host module, start a line trace on an active line from the MOSS console. This allows you to get a last trace block and allows the host module to end the DYNADMP DYNAMIC session.

To stop trace activity, which was started by the OPTION control statement, enter a second OPTION statement with the appropriate parameters specified. You can also start and stop the trace at the MOSS keyboard. Do not stop the trace at the MOSS keyboard until the *S* response to message IFV505D is given and accepted.

See the operating guide for your communication controller for information on the EP or PEP line and SIT.

Printing the Trace

When the trace activity is completed, you can get a readable output listing of the trace blocks. Use the PRINT command to print the EP line trace blocks in SYSUT2. Use ACF/TAP to format SIT.

If both SIT and line trace blocks are in SYSUT3, ACF/TAP formats the SIT records. The line trace blocks appear as unformatted hexadecimal records. (See the *NCP, SSP, and EP Trace Analysis Handbook* for information on using ACF/TAP.)

The PRINT command formats and prints the complete SYSUT2 work data set. Suppose, however, that you want to print only the last section of the trace blocks to trap a sporadic line error. Stop the trace when the line error occurs, and get a printout of the last section of the trace blocks. To get this printout, enter a PRINT command such as the following:

```
PRINT START=13:40:00
```

This command prints only those trace blocks written to the work data set after 1:40 p.m. You may also refer to the IFL508I time-stamp message when you print the work data set.

Note: Two hundred trace blocks are equivalent to about 72 pages of printed output (assuming 55 lines for each page).

JCL Statements

The MVS JCL statements:

- Execute or invoke the dynamic dump utility
- Define the output data set, the control statement data set, the work data set, and the communication controller.

If you request a trace entry dump, the work data set must be large enough to hold all the trace data being dumped. If the work data set is exhausted, the job will end abnormally. It is preferable to use a tape unit for this activity.

The following are JCL statements that invoke the dynamic dump utility:

```
//jobname     JOB    Initiates the job.

//name        EXEC   Specifies PGM=IFLSVEP
                     or the procedure name if
                     the job control statements
                     reside in a procedure library.

//STEPLIB     DD     Specifies the library that contains the
                     dump program or IFLREAD.

//SYSPRINT    DD     Defines a sequential output data set.
                     This data set can be written onto a
                     system output device, a magnetic tape
                     volume, or a direct-access volume.
                     The data control block's (DCB's)
                     block size can be specified.

//SYSUT1      DD     Defines the communication controller
                     subchannel over which the emulation
                     mode dynamic dump utility communicates
                     with the host processor.  See the
                     note following this example.

//SYSUT2      DD     Defines an optional temporary work
                     data set to receive dumps.  The contents
                     of the communication controller are written
                     to this data set (optional).
                     DISP=OLD must be specified.

//SYSUT3      DD     Defines the required work data set for
                     the SIT data.  This can be either a
                     tape or a disk.

//SYSIN       DD     Defines the input data set.

(Control statements)

/*

//
```

See the description of the DYNADMP keyword on the BUILD or LINE definition statement in *NCP, SSP, and EP Resource Definition Reference* for requirements for selecting a subchannel for the dynamic dump function.

Dynamic Dump Examples

This section contains examples of JCL and dynamic dump utility statements as well as examples of the statements required to dynamically dump trace entries.

Example of JCL and Dynamic Dump Utility Statements: The following example shows the statements required to dynamically dump, to the work data set, the entire contents of the communication controller, with a subchannel address of 007, to the work data set. After the dump is completed, the work data set contents are transferred to the output data set and printed. The job ends without operator intervention.

```
//DYNADMP     JOB     MSGLEVEL=(1,1),other parameters
//STEP1       EXEC    PGM=IFLSVEP
//STEPLIB     DD
//SYSPRINT    DD      SYSOUT=A
//SYSUT1      DD      UNIT=007
//SYSUT2      DD      UNIT=3400,VOL=SER=SVTAPE,LABEL=(,NL),
                      DISP=OLD,DSN=WORK
//SYSUT3      DD      UNIT=3400,VOL=SER=SITAPE,LABEL=(,NL),
                      DISP=OLD,DSN=SIT
//SYSIN       DD      *
            PAUSE   (Returns control to console)
/*
//
```

Example of Statements to Dynamically Dump Trace Entries: The following example shows the statements required to dynamically dump the SIT and EP line trace entries as they are created:

```
//DYNADMP     JOB     MSGLEVEL=(1,1),other parameters
//STEP1       EXEC    PGM=IFLSVEP
//STEPLIB     DD
//SYSPRINT    DD      SYSOUT=A
//SYSUT1      DD      UNIT=007
//SYSUT2      DD      UNIT=3400,VOL=SER=SVTAPE,LABEL=(,NL),
                      DISP=OLD,DSN=WORK
//SYSUT3      DD      UNIT=3400,VOL=SER=SITAPE,LABEL=(,NL),
                      DISP=OLD,DSN=SIT
//SYSIN       DD      *
            PAUSE   (Returns control to console)
/*
//
```

The following appears at the operator's console:

```
@08 IFI501A - REPLY WITH DESIRED FUNCTION OR 'END'
```

The operator then enters the following commands (indicated in bold type) and receives the following responses; the information in parentheses defines the purpose of each command:

```
r 08, option 4373023          (Activates SIT, line data,
                              level 2, and level 3
                              trace activity for channel
                              adapter 3 on subchannel 23.)

IFI503I  FUNCTION COMPLETED - 00
@09 IFL501A - REPLY WITH DESIRED FUNCTION OR 'END'

r 09, dy dynamic              (Starts the transmission of
                              trace entries to the host module,
                              and places the line trace entries
                              in the SYSUT2 work data set and
                              both line and SIT entries in the
                              SYSUT3 work data set.)

@10 IFL505E - REPLY S to STOP TRACE

IFI508I SIT   BLOCK      1 WRITTEN AT 13:27:54
IFL508I TRACE BLOCK      1 WRITTEN AT 13:27:56
IFL508I SIT   BLOCK    200 WRITTEN AT 13:28:20
IFI508I TRACE BLOCK    200 WRITTEN AT 13:28:37

r 10,s                        (Stops the transfer of trace
                              blocks to the host module.)

IFI506I  STOP COMMAND ACKNOWLEDGED
IFI508I  TRACE BLOCK   219 WRITTEN AT 03:83:0
IFL508I  SIT   BLOCK   382 WRITTEN AT 03:83:00
IFI503I  FUNCTION COMPLETED - 00
@11  IFL501A - REPLY WITH DESIRED FUNCTION OR 'END'

r 11,print start=13:25:00     (Causes a printout of only
                              those trace blocks written to the
                              SYSUT2 work data set after 13:25.)

IFI503I FUNCTION COMPLETED - 00
@12 IFL501A - REPLY WITH DESIRED FUNCTION OR 'END'

r 12,option 4343123           (Halts trace activity on
                              channel adapter 3, subchannel 23.)

IFI503I FUNCTION COMPLETED - 00
@13 IFL501A - REPLY WITH DESIRED FUNCTION OR 'END'

r 13,end                      (Terminates the DYNADMP job.)

IEF404I DYNADMP ENDED  TIME=13:30:15
//
```

Sample MVS Procedure for Running Dynamic Dump Utility

A sample procedure for running the dynamic dump utility under MVS is included on your licensed program tape. The data set name of this sample, found in the ASSPSAMP library on your tape, is DYNJCL. This procedure is provided to help you create and tailor the JCL in your MVS environment. An example of the JCL used in the DYNJCL sample is as follows:

```
//DYNADMP  JOB   (account info),'name'
//DYNADMP  PROC SSPLIB='sys1.ssplib',UNITNME=sysda,OUT='*',
//            CCADDR=xxx,WORKDMP='user.dump',VOLSER1='work',
//            SITDATA='user.trace',VOLSER2='sit',
//            MOSSCSP='user.mosscsp'
//*********************************************************************
//*********************************************************************
//**
//**     PROCEDURE:  IFLSVEP
//**
//**     FUNCTION:   SAMPLE JCL TO EXECUTE DYNADMP
//**
//**     NOTES:
//**          1. CHANGE ALL LOWER CASE CHARACTERS TO VALUES
//**             SUITABLE FOR YOUR INSTALLATION.
//**
//**          2. ENTER DESIRED DYNADMP CONTROL STATEMENTS IN SYSIN DATA
//**             STREAM BELOW.
//**
//**     SYMBOLIC PARMS:
//**
//**           SSPLIB   :  NAME OF DATA SET CONTAINING IFLSVEP
//**           UNITNME  :  UNIT NAME FOR TEMPORARY DATA SETS
//**           OUT      :  SYSOUT CLASS
//**           CCADDR   :  COMMUNICATION CONTROLLER ADDRESS
//**           WORKDMP  :  WORK DATA SET TO RECEIVE DUMPS
//**           VOLSER1  :  VOLUME SN OF TEMPORARY DUMP / LT DATA SET
//**           SITDATA  :  WORK DATA SET FOR SIT DATA
//**           VOLSER2  :  VOLUME SN OF TEMPORARY SIT TRACE DATA SET
//**           MOSSCSP  :  WORK DATA SET FOR MOSS AND CSP DUMPS
//**
//**     FOR MORE INFORMATION ABOUT THIS JCL SEE NCP/SSP/EP
//**     DIAGNOSIS GUIDE, FORM NUMBER LY43-0033
//**
//**     ACTIVITY:
//**     ____________________________________________________________
//**     NONE
//*********************************************************************
//         EXEC  PGM=IFLSVEP
//*********************************************************************
//*   DD CARD FOR DATA SET CONTAINING IFLSVEP
//*********************************************************************
//*
//STEPLIB  DD    DSN=&SSPLIB,DISP=SHR
//*
```

```
//*********************************************************************
//*   DD CARD FOR USER TERMINATION DUMP (COMMENTED OUT INITIALLY)
//*********************************************************************
//*
//*SYSUDUMP DD    SYSOUT=&OUT
//*
//*********************************************************************
//*   DD CARD FOR ABNORMAL TERMINATION DUMP (COMMENTED OUT INITIALLY)
//*********************************************************************
//*
//*SYSABEND DD    SYSOUT=&OUT
//*
//*********************************************************************
//*   DD CARD FOR SEQUENTIAL DATA SET FOR DYNADMP OUTPUT
//*********************************************************************
//SYSPRINT DD    SYSOUT=&OUT
//*
//*********************************************************************
//*   DD CARD WHICH DEFINES THE COMMUNICATION CONTROLLER SUBCHANNEL
//*      OVER WHICH DYNADMP COMMUNICATES WITH THE HOST PROCESSOR
//*********************************************************************
//*
//SYSUT1   DD    UNIT=&CCADDR
//*
//*********************************************************************
//*   DD CARD FOR WORK DATA SET TO RECEIVE DUMPS AND LINE TRACE DATA
//*********************************************************************
//*
//SYSUT2   DD    UNIT=&UNITNME,VOL=SER=&VOLSER1,DISP=OLD,DSN=&WORKDMP
//*
//*********************************************************************
//*   DD CARD FOR WORK DATA SET FOR SIT DATA
//*********************************************************************
//*
//SYSUT3   DD    UNIT=&UNITNME,VOL=SER=&VOLSER2,DISP=OLD,DSN=&SITDATA
//*
//*********************************************************************
//*   DD CARD FOR WORK DATA SET FOR MOSS AND CSP DUMPS
//*      (NOT APPLICABLE WITH PEP)
//*********************************************************************
//SYSUT4   DD    DSN=&MOSSCSP,DISP=OLD
//*********************************************************************
//PROCEND  PEND
//STEP1    EXEC DYNADMP
//*********************************************************************
//*   DD CARD FOR INPUT STREAM CONTAINING DYNADMP CONTROL STATEMENTS
//*********************************************************************
//*
//SYSIN    DD    *
           DYNADMP control statements go here.
/*
```

PARM Field Option in the EXEC Control Statement

The only PARM field option that the dynamic dump utility recognizes is LINECOUNT=nn:

```
PARM='LINECOUNT=nn'
PARM='LC=nn'.
```

nn specifies a decimal number from 10 to 99, which represents the number of lines on each page the dynamic dump utility prints.

If the LINECOUNT parameter is omitted or is syntactically incorrect, the default of 55 lines on each page is assumed.

Example: To specify that the dynamic dump utility print 40 lines on each page, code the PARM field option as follows:

```
//STEP1 EXEC  PGM=IFLSVEP,PARM='LINECOUNT=40'
```

Dynamic Dump Utility in VM

The following section discusses how to use the dynamic dump utility in VM.

Host Processor and Communication Controller Requirements

Any host processor that runs under VM can run the dynamic dump utility. The dynamic dump utility requires a 16KB section of user virtual storage. Calculate the number of 516-byte blocks required for work file space for SYSUT2 as equal to twice the size of the communication controller storage, in KB, plus 1.

If you request a dynamic dump of trace table entries, the work file must be large enough to hold all the dumped trace data. A tape unit is preferable for this activity.

NCP, SSP, and EP Resource Definition Reference shows the valid ways the DYNADMP keyword on the BUILD definition statement is used to specify subchannels for the transfer of dynamic dump data to the host processor.

To run the dynamic dump utility in VM, you must use the ATTACH command. When you finish using the dynamic dump utility, use the DETACH command. These two commands enable and disable the emulator subchannel.

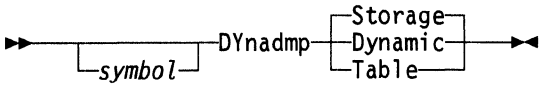
Utility Control Statements

With the dynamic dump utility control statements, you can:

- Get a full or partial storage dump
- Display a section of storage
- Print the work file to be sent to the output file
- Request a line trace or SIT
- Allow the selection of available channel adapters
- Allow control statements to be entered after the PAUSE control statement
- End a job and stop the program after the trace output is printed
- Cause control statements to be read from the input stream.

DYNADMP Control Statement

The DYNADMP control statement requests a dump of the entire communication controller storage or a specified section. The communication controller does not become idle and does not require reloading.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

Dynamic specifies that the line or SIT tables are to be dumped dynamically as entries are made. This type of dump requires operator intervention to stop the trace. Before starting a dynamic trace dump, start a trace on a communication line using the control panel of the communication controller or using the dynamic dump utility (the OPTION control statement).

Storage specifies that the entire contents of communication controller storage are to be dumped. NCP operation continues both during and after the storage contents have been dumped. Storage is the default.

Table specifies that only the trace table section of communication controller storage is to be dumped.

DISPLAY Control Statement

The DISPLAY control statement displays a section of the communication controller storage on the operator's console at the host processor.

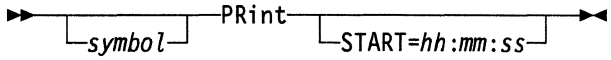
symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

hhhhhh specifies the beginning address, in hexadecimal, of the storage to be displayed.

n specifies the number of lines (16 bytes of storage on each line) to be displayed. The maximum number of lines you can specify is 9. If *n* is omitted, 1 is the default.

PRINT Control Statement

The PRINT control statement requests that a printout (32 bytes of storage for each line) of the entire SYSUT2 work file be sent to the SYSPRINT device (the output file).



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

START=hh:mm:ss (hours:minutes:seconds) specifies that only those trace blocks written to the SYSUT2 work file after time *hh:mm:ss* are to be printed.

hh:mm:ss specifies a time that is both later than (or equal to) the time stamp associated with the first trace block and earlier than (or equal to) the time stamp associated with the last trace block that was written to the work file. Otherwise, message IFV510I is issued to specify that no trace blocks that satisfied the PRINT command were found.

Example 1: Assume that the first trace block is recorded at 09:05:00 (9:05 a.m.) and the last is recorded at 09:20:00 a.m. The statement PRINT START=09:17:30 prints trace blocks recorded between 9:17:30 a.m. and 9:20 a.m.

The print function correctly interprets a postmidnight time stamp (for a last-written trace block) as later than a premidnight time stamp (for a first-written trace block), even though the numeric value of hh:mm:ss is lower for the postmidnight time (for example, the values 23:55:00 and 00:02:00 could represent the 7-minute interval from 11:55 p.m. to 12:02 a.m.).

Example 2: Assume that a trace is started just before midnight. If the first trace block was written to the work file at 23:25:23 (11:25 p.m.) and the last was written at 00:40:57 (12:40 a.m. the following day), then either of the following PRINT statements produces the intended results:

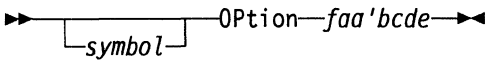
```
PRINT       START=23:40:00      (Trace entries written to the work file
                                between 11:40 p.m. and 12:40 a.m. are
                                printed.)

PRINT       START=00:20:00      (Trace entries written to the work file
                                between 12:20 a.m. and 12:40 a.m. are
                                printed.)
```

If you omit the START keyword, the entire SYSUT2 work file is printed.

If you specify the START keyword and there are storage dumps in the work file with the trace blocks, these storage dumps are also printed regardless of whether they satisfy the START constraint. Storage dumps are not time stamped.

OPTION Control Statement

The OPTION control statement requests a line trace or SIT and allows the selection of any of the six available channel adapters for the IBM 3725 Communication Controller or the four available channel adapters for the locally attached IBM 3720 Communication Controller. Also, the OPTION control statement starts, stops, or alters the program interrupt levels being traced. OPTION traces level 2 interrupts (line data), level 3 interrupts (time-out complete or channel data such as initial selection, data, and status), or both. OPTION continuously traces level 1 error log entries after a level 3 trace is started.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

faa'bcde specifies the trace functions desired: the start trace or stop trace, the channel adapter to trace, the SIT and line trace data options, the program level to trace, and the subchannels to trace. The values for *f, a, a', bc,* and *de* and their meanings follow:

f	a	a'	bc	de	Meaning (L=level)
4	*n*[1]	4	00	xx	Start SIT without line data on subchannel xx.
4	*n*[1]	6	00	xx	Start SIT with line data on subchannel xx.
4	*n*[1]	4	01	xx	Stop SIT on subchannel xx.
4	*n*[1]	0	10	xx	Start L2 trace without line data on subchannel xx.
4	*n*[1]	1	10	xx	Start L2 trace with data on subchannel xx.
4	*n*[1]	4	10	xx	Start SIT without line data on subchannel xx. Start L2 trace without line data on subchannel xx.
4	*n*[1]	5	10	xx	Start SIT without line data on subchannel xx. Start L2 trace with data on subchannel xx.
4	*n*[1]	6	10	xx	Start SIT with line data on subchannel xx. Start L2 trace without line data on subchannel xx.
4	*n*[1]	7	10	xx	Start SIT with line data on subchannel xx. Start L2 trace with data on subchannel xx. subchannel xx.
4	*n*[1]	0	11	xx	Stop L2 trace on subchannel xx.
4	*n*[1]	4	11	xx	Stop SIT on subchannel xx. Stop L2 trace on subchannel xx.
4	*n*[1]	0	20	xx	Start L3 trace on subchannel xx.

[1] Channel adapter:

Number 1–2 for the IBM 3720
Number 1–6 for the IBM 3725
Logical address 0–F for the IBM 3745.

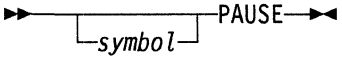
f	a	a'	bc	de	Meaning (L=level)
4	*n*[1]	4	20	xx	Start SIT without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	6	20	xx	Start SIT with line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	0	21	xx	Stop L3 trace on subchannel xx.
4	*n*[1]	4	21	xx	Stop SIT on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	0	30	xx	Start L2 trace without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	1	30	xx	Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	4	30	xx	Start SIT without line data on subchannel xx. Start L2 trace without data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	5	30	xx	Start SIT without line data on subchannel xx. Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	6	30	xx	Start SIT with line data on subchannel xx. Start L2 trace without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	7	30	xx	Start SIT with line data on subchannel xx. Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	0	31	xx	Stop L2 trace on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	4	31	xx	Stop SIT on subchannel xx. Stop L2 trace on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	0	70	00	Start L3 trace on defined subchannel.
4	*n*[1]	0	71	00	Stop L3 trace on defined subchannel.
4	*n*[1]	0	70	FF	Start L3 trace on all subchannels.
4	*n*[1]	0	71	FF	Stop L3 trace on all subchannels.

[1] Channel adapter:

Number 1–2 for the IBM 3720
Number 1–6 for the IBM 3725
Logical address 0–F for the IBM 3745.

PAUSE Control Statement

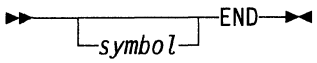
The PAUSE control statement allows control statements to be entered at the console of the host processor after the PAUSE statement is read from the input job stream or entered from the console.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

END Control Statement

The END control statement specifies the end of job and stops the program after the trace output has been printed.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

This control statement does not end the trace. You must stop the trace from the console. Press the console Interrupt key to establish operator communication with the host processor.

SYSIN Control Statement

The SYSIN control statement reads control statements from the input stream.

Obtaining a Dynamic Dump of Trace Entries

To dynamically dump the EP line trace table entries or SIT records, first start the traces on the desired range of EP subchannels using the OPTION control statement. Then, to begin the transfer of trace entries (trace blocks) to the dynamic dump utility host module, enter the DYNADMP DYNAMIC control statement. Message IFV521I will be issued. When enough data has been transferred, press Enter. The operator's console receives message IFV505D, which requires a response. Reply *S* to this message to stop the transfer of trace blocks to the host module.

The trace blocks can be written to two different work files, depending on which traces are active. If only the line trace is active, the trace blocks are written to SYSUT2. If only SIT is active, the trace blocks are written to SYSUT3. If both the line trace and SIT are active, both line and SIT records are written to SYSUT3, but only line trace records are written to SYSUT2.

Each trace block received by the host module is time stamped before being written to the work file. The time stamp, in the format hh:mm:ss (hours:minutes:seconds), shows the time when the host module received the trace block. Periodically, the operator receives message IFV508I, which shows these time stamps. Typical IFV508I messages are:

```
IFV508I SIT BLOCK       200 WRITTEN AT 13:28:20
IFV508I TRACE BLOCK     200 WRITTEN AT 13:28:37
```

Stopping Trace Activity

To stop the trace activity, the operator must first respond with *S* to the message (IFV505D) issued when the trace is started. The *S* response stops the transfer of trace blocks to the host module when the next trace block is received.

If you are dynamically dumping the SIT or communication controller line trace entries, and the controller's DYNADUMP module has stopped sending trace blocks to the host module, start a line trace on an active line from the MOSS console. This allows you to get a last trace block and allows the host module to end the DYNADMP DYNAMIC session.

To stop the trace activity in the communication controller, which was started by the OPTION control statement, enter a second OPTION statement with the appropriate parameters specified. You can also start or stop the trace at the MOSS keyboard. Do not stop the trace at the MOSS keyboard until the *S* response to message IFV505D has been given and accepted.

See the operating guide for your communication controller for information on the EP or PEP line and SIT.

Printing the Trace

When the trace activity is completed, you can get a readable output listing of the trace blocks. Use the PRINT command to print the EP line trace blocks in SYSUT2. Use ACF/TAP to format SIT blocks in SYSUT3. (See the *NCP, SSP, and EP Trace Analysis Handbook* for information on using ACF/TAP.)

If both SIT and line trace blocks are in SYSUT3, ACF/TAP formats the SIT records. The line trace blocks appear as unformatted hexadecimal records.

The PRINT command formats and prints the entire SYSUT2 work file. Suppose, however, that you want to print only the last section of the trace blocks to trap a sporadic line error. The trace is stopped when the line error occurs, and a printout of the last section of the trace blocks is required. To get this printout, enter a PRINT command such as the following:

```
PRINT START=13:40:00
```

This command prints only those trace blocks written to the work file after 1:40 p.m. You can also use the IFV508I time stamp message when you print the work file.

Note: Two hundred trace blocks are equivalent to about 72 pages of printed output (assuming 55 lines on each page).

FILEDEFs

To run the dynamic dump program, establish FILEDEFs for the output file, the control statement file, and the necessary work files. Then issue the command IFLSVEP to call the nonrelocatable module generated for the dynamic dump program. Specify the value for the virtual channel and emulation subchannel address over which dynamic dump data can be transferred to the host processor as a parameter with this command.

If you request a trace entry dump, the work file must be large enough to hold all the trace data being dumped. If, however, the work file is exhausted, the job will abend. It is preferable to use a tape unit for this activity.

The FILEDEF statements needed to call the dynamic dump utility are as follows:

FILEDEF SYSPRINT	Defines a sequential output file. This file can be written onto a system output device, a magnetic tape volume, or a direct-access volume. The data control block's (DCB's) block size can be specified.
FILEDEF SYSUT2	Defines an optional temporary work file to receive dumps. The contents of the communication controller are written to this file (optional).
FILEDEF SYSUT3	Defines the required work file for the SIT data. This can be either a tape or disk.
FILEDEF SYSIN	Defines the input file.
Control statements	Issued from the console or SYSIN file.
IFLSVEP	Defines the nonrelocatable module generated for the dynamic dump and defines the required parameters.

Notes:

1. To ensure that previously defined FILEDEFs are not in effect, clear all FILEDEFs with the command FILEDEF * CLEAR *before* issuing the FILEDEFs for IFLSVEP.
2. See the description of the DYNADMP keyword on the BUILD or LINE definition statement in *NCP, SSP, and EP Resource Definition Reference* for requirements on selecting a subchannel for the dynamic dump function.

Dynamic Dump Examples

This section contains examples of FILEDEFs and dynamic dump utility statements as well as examples of the statements required to dynamically dump trace entries.

Example of FILEDEFs and Dynamic Dump Utility Statements: The following example shows the statements required to dynamically dump, to the SYSUT2 work file, the entire contents of the IBM 3725 Communication Controller with a subchannel address of 0B8. After the dump is completed, the contents of the work file are transferred to the output file and printed. The job ends without operator intervention.

```
FILEDEF SYSUT2 DISK TEST DUMP A (RECFM F BLOCK 516 LRECL 516 XTENT 62500
FILEDEF SYSPRINT PRINTER
FILEDEF SYSIN DISK CONTROL CARD A
```

Disk file CONTROL CARD A contains the following statements. When using the statement from a file, insert a blank character before each statement to accommodate the *symbol*.

```
DY STORAGE
PRINT
END
```

Issue these FILEDEF statements given in the example; then run the following:

```
IFLSVEP 0B8
```

Example of Statements to Dynamically Dump Trace Entries: The following statements dynamically dump the SIT and EP line trace entries as they are created:

```
FILEDEF SYSUT2 DISK TEST DUMP A (RECFM F BLOCK 516 LRECL 516 XTENT 62500
FILEDEF SYSPRINT PRINTER
FILEDEF SYSIN DISK DYPAUSE CARD A
FILEDEF SYSUT3 DISK WORK FILE A (RECFM U BLOCK 545 LRECL 545
```

DYPAUSE CARD A contains the PAUSE statement. When using the statement from a file, insert a blank character before the statement to accommodate the *symbol*.

Issue the FILEDEF statements given in the example; then run the following:

```
IFLSVEP 0B8
```

The following appears at the operator's console:

```
IFV501A - REPLY WITH DESIRED FUNCTION OR 'END'
```

The operator then enters the following commands (indicated in bold type) and receives the following responses; the information in parentheses defines the purpose of each command:

```
option 4373023            (Activates SIT,
                          line data, level 2, and level 3
                          trace activity for channel
                          adapter 3 on subchannel 23.)

   IFV503I  FUNCTION COMPLETED - 00
   IFV501A - REPLY WITH DESIRED FUNCTION OR 'END'

dy dynamic                (Starts the transmission of
                          trace entries to the host module;
                          then it places the line trace entries
                          in the SYSUT2 work file and
                          both line and SIT entries in the
                          SYSUT3 work file.)

IFV521I ENTER ATTENTION INTERRUPT TO STOP TRACE
```

```
IFV508I SIT   BLOCK
1 WRITTEN AT 13:27:54
IFV508I TRACE BLOCK
1 WRITTEN AT 13:27:56
IFV508I SIT   BLOCK
200 WRITTEN AT 13:28:20
IFV508I TRACE BLOCK
200 WRITTEN AT 13:28:37
```

If the Enter key is pressed here, the following message appears:

```
IFV505D - REPLY S TO STOP TRACE OR C TO CONTINUE
```

The operator then enters and receives the following:

```
s                          (Stops the transfer of trace
                           blocks to the host module.)

IFV506I  STOP COMMAND ACKNOWLEDGED
IFV508I  TRACE BLOCK   219 WRITTEN AT 13:29:53
IFV508I  SIT   BLOCK   382 WRITTEN AT 13:29:57
IFV503I  FUNCTION COMPLETED - 00
IFV501A - REPLY WITH DESIRED FUNCTION OR 'END'

print start=13:25:00       (Causes a printout of only
                           those trace blocks written to
                           the SYSUT2 work file after 13:25.)

IFV503I FUNCTION COMPLETED - 00
IFV501A - REPLY WITH DESIRED FUNCTION OR 'END'

option 4343123             (Halts trace activity
                           on channel adapter 3, subchannel 23.)

IFV503I FUNCTION COMPLETED - 00
IFV501A - REPLY WITH DESIRED FUNCTION OR 'END'
```

LINECOUNT Parameter on the IFLSVEP Command

LINECOUNT is one parameter the dynamic dump utility recognizes. This parameter specifies a decimal number from 10 to 99, which represents the number of lines on each page printed by the dumper utility. If the LINECOUNT parameter is omitted or given incorrectly, the default is 55 lines on each page.

You can include the LINECOUNT parameter on the IFLSVEP command in one of two formats:

```
IFLSVEP  cuu linecount nn
         cuu lc nn
```

Example: To specify that the dynamic dump utility print 40 lines on each page of printed output, call the dynamic dump utility as follows:

```
IFLSVEP 0B8 LC 40
```

Sample VM Procedure for Running Dynamic Dump Utility

A sample procedure for running the dynamic dump utility under VM is included on your licensed program tape. The file name of the sample is DYNDMPVM SMPLEXEC. This procedure is provided to help you create and tailor the FILEDEFs in your VM environment.

Dynamic Dump Utility in VSE

The following section discusses how to use the dynamic dump utility in VSE.

Host Processor and Communication Controller Requirements

The host processor module of the dynamic dump utility can run in any host processor that accommodates VSE. The VSE dynamic dump utility operates in a minimum virtual region. Residence requirements are 15 blocks for the core-image library and 82 blocks for the relocatable library.

NCP, SSP, and EP Resource Definition Reference shows the valid ways the DYNADMP keyword on the BUILD definition statement is used to specify subchannels for the transfer of dynamic dump data to the host processor.

Requirements for Installing the Dynamic Dump Utility

The controller physical link unit block must specify a communication controller for SVC 27 (HALT I/O) to work. This can be accomplished by specifying 3720, 3725, or 3745 on the ADD command. The EP subchannel address for SYS011 must be specified as an IBM 3720, 3725, or 3745.

If the dynamic dump modules of the host processor section of the utility are cataloged as object code in the sublibrary, the following JCL statements can be used for link-editing them into phases in the sublibrary:

```
// JOB       LINKEDIT
// LIBDEF    OBJ,SEARCH=(SSPLIB.DUMPFORM)
// LIBDEF    PHASE,CATALOG=(SSPLIB.DUMPFORM),PERM
// OPTION    CATAL
   INCLUDE   IFUDYN
// EXEC      LNKEDT
//
```

Utility Control Statements

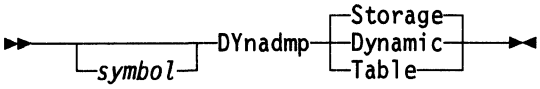
With the dynamic dump utility control statements, you can:

- Get a full or partial storage dump
- Display a section of storage
- Print the work file to be sent to the output file
- Request a line trace or SIT
- Allow the selection of available channel adapters

- Allow control statements to be entered after the PAUSE control statement
- End a job and stop the program after the trace output is printed
- Cause control statements to be read from the input stream.

DYNADMP Control Statement

The DYNADMP control statement requests a dump of the entire communication controller storage or a specified section. The communication controller does not become idle and does not require reloading.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

Dynamic specifies that the line or SIT tables are to be dumped dynamically as entries are made. This type of dump requires operator intervention to stop the trace. Before starting a dynamic trace dump, start a trace on a communication line using the control panel of the communication controller or using the dynamic dump utility (the OPTION control statement).

Storage specifies that the entire contents of communication controller storage are to be dumped. NCP execution continues both during the operation and after the storage contents have been dumped. Storage is the default.

Table specifies that only the trace table section of communication controller storage is to be dumped.

DISPLAY Control Statement

The DISPLAY control statement displays a section of the communication controller storage on the operator's console at the host processor.

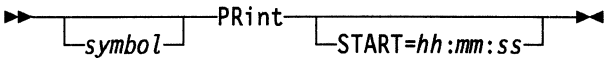
symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

hhhhhh specifies the beginning address, in hexadecimal, of the storage to be displayed.

n specifies the number of lines (16 bytes of storage on each line) to be displayed. The maximum number of lines you may specify is 9. If *n* is omitted, 1 is the default.

PRINT Control Statement

The PRINT control statement requests that a printout (32 bytes of storage per line) of the complete work file (SYS010) be sent to the SYSLST device (the output file).



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

START=hh:mm:ss (hours:minutes:seconds) specifies that only those trace blocks written to the work file after time *hh:mm:ss* are to be printed.

hh:mm:ss specifies a time that is both later than (or equal to) the time stamp associated with the first trace block and earlier than (or equal to) the time stamp associated with the last trace block that was written to the work file. Otherwise, message IFU510I is issued to show that no trace blocks that satisfied the PRINT command were found.

Example 1: Assume that the first trace block is recorded at 09:05:00 (9:05 a.m.) and the last is recorded at 09:20:00 a.m. The statement PRINT START=09:17:30 prints trace blocks recorded between 9:17:30 a.m. and 9:20 a.m.

The print function correctly interprets a postmidnight time stamp (for a last-written trace block) as later than a premidnight time stamp (for a first-written trace block), even though the numeric value of hh:mm:ss is lower for the postmidnight time (for example, the values 23:55:00 and 00:02:00 could represent the 7-minute interval from 11:55 p.m. to 12:02 a.m.).

Example 2: Assume that a trace is started just before midnight. If the first trace block was written to the work file at 23:25:23 (11:25 p.m.) and the last was written at 00:40:57 (12:40 a.m. the following day), then either of the following PRINT statements produces the intended results:

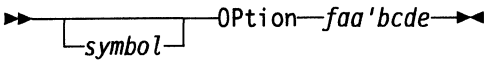
```
PRINT           START=23:40:00   (Trace entries written to work file
                                  between 11:40 p.m. and 12:40 a.m.
                                  are printed.)

PRINT           START=00:20:00   (Trace entries written to work
                                  file between 12:20 a.m.
                                  and 12:40 a.m. are printed.)
```

If you omit the START keyword, the complete work file is printed.

If you specify the START keyword and there are storage dumps in the work file with the trace blocks, these storage dumps are also printed regardless of whether they satisfy the START constraint. Storage dumps are not time stamped.

OPTION Control Statement

The OPTION control statement requests a line trace or SIT and allows the selection of any of the available channel adapters for the communication controller. Also, the OPTION control statement starts, stops, or alters the program interrupt levels being traced. OPTION traces level 2 interrupts (line data), level 3 interrupts (time-out complete or channel data such as initial selection, data, and status), or both. OPTION continuously traces level 1 error log entries after a level 3 trace is started.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

faa'bcde specifies the trace functions desired: the start trace or stop trace, the channel adapter to trace, the SIT options and the line trace data options, the program level to trace, and the subchannels to trace. The values for *f, a, a', bc,* and *de* and their meanings are as follows:

f	a	a'	bc	de	Meaning (L=level)
4	*n*[1]	4	00	xx	Start SIT without line data on subchannel xx.
4	*n*[1]	6	00	xx	Start SIT with line data on subchannel xx.
4	*n*[1]	4	01	xx	Stop SIT on subchannel xx.
4	*n*[1]	0	10	xx	Start L2 trace without line data on subchannel xx.
4	*n*[1]	1	10	xx	Start L2 trace with data on subchannel xx.
4	*n*[1]	4	10	xx	Start SIT without line data on subchannel xx. Start L2 trace without line data on subchannel xx.
4	*n*[1]	5	10	xx	Start SIT without line data on subchannel xx. Start L2 trace with data on subchannel xx.
4	*n*[1]	6	10	xx	Start SIT with line data on subchannel xx. Start L2 trace without line data on subchannel xx.
4	*n*[1]	7	10	xx	Start SIT with line data on subchannel xx. Start L2 trace with data on subchannel xx.
4	*n*[1]	0	11	xx	Stop L2 trace on subchannel xx.
4	*n*[1]	4	11	xx	Stop SIT on subchannel xx. Stop L2 trace on subchannel xx.
4	*n*[1]	0	20	xx	Start L3 trace on subchannel xx.
4	*n*[1]	4	20	xx	Start SIT without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	6	20	xx	Start SIT with line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	0	21	xx	Stop L3 trace on subchannel xx.
4	*n*[1]	4	21	xx	Stop SIT on subchannel xx. Stop L3 trace on subchannel xx.

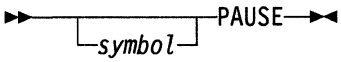
f	a	a'	bc	de	Meaning (L=level)
4	*n*[1]	0	30	xx	Start L2 trace without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	1	30	xx	Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	4	30	xx	Start SIT without line data on subchannel xx. Start L2 trace without data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	5	30	xx	Start SIT without line data on subchannel xx. Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	6	30	xx	Start SIT with line data on subchannel xx. Start L2 trace without line data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	7	30	xx	Start SIT with line data on subchannel xx. Start L2 trace with data on subchannel xx. Start L3 trace on subchannel xx.
4	*n*[1]	0	31	xx	Stop L2 trace on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	4	31	xx	Stop SIT on subchannel xx. Stop L2 trace on subchannel xx. Stop L3 trace on subchannel xx.
4	*n*[1]	0	70	00	Start L3 trace on defined subchannel.
4	*n*[1]	0	71	00	Stop L3 trace on defined subchannel.
4	*n*[1]	0	70	FF	Start L3 trace on all subchannels.
4	*n*[1]	0	71	FF	Stop L3 trace on all subchannels.

[1] Channel adapter:

Number 1–2 for the IBM 3720
Number 1–6 for the IBM 3725
Logical address 0–F for the IBM 3745.

PAUSE Control Statement

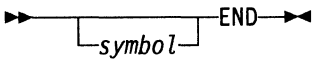
The PAUSE control statement allows control statements to be entered at the console of the host processor after the PAUSE statement is read from the input job stream or entered from the console.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

END Control Statement

The END control statement specifies the end of job and stops the program after the trace output has been printed.



symbol specifies a name, 1 to 8 characters long, beginning with an alphabetical character. Do not use a name if you enter statements from the console. If you enter statements in a file, leave a blank if you have not defined a symbol.

This control statement does not end the trace. You must stop the trace from the console. Establish operator communication with the host processor for a background partition by pressing the console Interrupt key. Reply 'MSG Fx' to the attention routine for foreground partition Fx.

SYSIN Control Statement

The SYSIN control statement causes control statements to be read from the input stream.

Obtaining a Dynamic Dump of Trace Entries

To dynamically dump the EP line trace table entries or SIT records, first start the traces on the desired range of EP subchannels using the OPTION control statement. Then, to begin the transfer of trace entries (trace blocks) to the dynamic dump utility host module, enter the DYNADMP DYNAMIC control statement. The operator's console receives message IFU505E, which requires a response. Reply *S* to this message to stop the transfer of trace blocks to the host module.

The trace blocks can be written to two different work files, depending on which traces are active. If only the line trace is active, the trace blocks are written to SYS010. If only SIT is active, the trace blocks are written to SYS012. If both the line trace and SIT are active, both line trace and SIT records are written to SYS012, but only line trace records are written to SYS010.

Each trace block received by the host module is time-stamped before being written to the work file. The time stamp, in the format hh:mm:ss (hours:minutes:seconds), shows the time when the host module received the trace block. Periodically, message IFU508I informs the operator of these time stamps. Typical IFU508I messages are:

```
IFU508I SIT   BLOCK   200 WRITTEN AT 13:28:20
IFU508I TRACE BLOCK   200 WRITTEN AT 13:28:37
```

Stopping Trace Activity

To stop a trace running in a background partition, press the External Interrupt key on the host processor. To stop a trace running in a foreground partition, press the console Interrupt Request key and enter 'MSG Fx' (x represents the number of the partition desired). This action halts the transfer of trace blocks to the work file when the next trace block is received from the communication controller and placed on the work file.

If you are dynamically dumping the SIT or communication controller line entries, and the controller's DYNADMP module has stopped sending trace blocks to the host module, start a line trace on an active line from the MOSS console. This allows you to get a last trace block and allows the host module to end the DYNADMP DYNAMIC session.

To stop the trace activity in the controller, which was started by the OPTION control statement, enter a second OPTION statement with the appropriate parameters specified. You can also start and stop the trace at the MOSS keyboard. Do not stop the trace at the MOSS keyboard until the response to message IFU505E is given and accepted.

See the operating guide for your communication controller for information on EP or PEP line and SIT.

Printing the Trace

When the trace activity is completed, you can get a readable output listing of the trace blocks. Print the EP line trace blocks in SYS010 using the PRINT command. Use ACF/TAP to format the SIT blocks in SYS012. (See the *NCP, SSP, and EP Trace Analysis Handbook* for information on using ACF/TAP.) If both SIT and line trace are written to the SYS012 data file, ACF/TAP formats only the SIT records and prints line trace blocks in unformatted hexadecimal records.

The PRINT command formats and prints the complete SYS010 work file. Suppose, however, that you want to print only the last section of the trace blocks to trap a sporadic line error. The trace stops when the line error occurs, and a printout of the last section of the trace blocks is required. To get this printout, enter a PRINT command such as the following:

```
PRINT START=13:40:00
```

This command prints only those trace blocks written to the work file after 1:40 p.m. Also, refer to the IFU508I time-stamp message when you print the work file.

Note: Two hundred trace blocks are equivalent to about 72 pages of printed output (assuming 55 lines on each page).

JCL Statements

The VSE JCL statements:

- Execute or invoke the dynamic dump utility
- Define the output file, the control statement file, the work file, and the communication controller.

Work file requirements for SYS010 depend on the storage size of the controller whose storage is being dumped. The work file for SYS010 and SYS012 must be a tape unit under VSE.

The following JCL statements invoke the dynamic dump utility.

```
// JOB                              Initiates the job.

// LIBDEF   PHASE,SEARCH=(SSPLIB.DUMPFORM),TEMP
                                    Specifies the location of the
                                    SSP dump formatter utility program.

// ASSGN    SYSLST                  Defines the output file.

// ASSGN    SYS011                  Defines the communication controller
                                    subchannel over which the dynamic
                                    dump utility communicates with the host
                                    processor.

// ASSGN    SYS010                  Defines a temporary tape work file;
                                    the contents of communication controller
                                    storage are written to this file.

// ASSGN    SYS012                  Defines the required tape work
                                    file for SIT data.

// DLBL     MCDUMP

// ASSGN    SYSIPT                  Defines the control statement file.

// EXEC     IFUSVEP                 Specifies the job step IFUSVEP.

(Control statements)

/*
//
```

Note: See the description of the DYNADMP keyword on the BUILD or LINE definition statement in *NCP, SSP, and EP Resource Definition Reference* for requirements for selecting a subchannel for the dynamic dump function.

Dynamic Dump Examples

This section contains an example of JCL and dynamic dump utility statements as well as examples of the statements required to dynamically dump trace entries.

Example of JCL and Dynamic Dump Utility Statements: The following example shows the statements required to dynamically dump to the work file, the entire contents of the communication controller, with a subchannel address of 001. After the dump is completed, the work file contents are transferred to the output file and printed. The job ends without operator intervention.

```
// JOB        SEVP
// LIBDEF     PHASE,SEARCH=(SSPLIB.DUMPFORM),TEMP
// ASSGN      SYSLST [...Parameters defining output file]
// ASSGN      SYS010,X'280'
// ASSGN      SYS011,X'001'
// EXEC       IFUSVEP
   DYNADMP    STORAGE
   PRINT
   END
/*
//
```

Example of Statements to Dynamically Dump Trace Entries: This example shows the statements required to dynamically dump the trace entries as they are created. The entries are placed in the SYS010 and SYS012 work files until operator communication is established. The SYS010 work file contents are transferred to the output file and sent to the printer. The job ends when the print operation ends. (Format the contents of the SYS012 work file using ACF/TAP.)

```
// JOB      SEVP
// LIBDEF   PHASE,SEARCH=(SSPLIB.DUMPFORM),TEMP
// ASSGN    SYSLST          (Parameters defining the output file.)
// ASSGN    SYS010,X'280'   (X'280' represents a device address.)
// ASSGN    SYS011,X'001'   (X'001' represents the controller subchannel address.
// ASSGN    SYS012,X'281'   (X'281' represents a device address.)
// EXEC     IFUSVEP
   PAUSE                   (Allows operator to enter control
                           statements from the console.)
```

The following appears at the operator's console:

```
BG 000 IFU501A - REPLY WITH DESIRED FUNCTION OR 'END'
```

The operator then enters the following commands (indicated in bold type) and receives the following responses; the information in parentheses defines the purpose of each command:

```
0 OP 4173020              (Activates SIT, line data,
                          level 2, and level 3
                          trace activity for channel
                          adapter 1 on subchannel 20.)

BG 000 IFU503I  FUNCTION COMPLETED - 00
BG 000 IFU501A - REPLY WITH DESIRED FUNCTION OR 'END'
```

```
0 DYNADMP DYNAMIC          (Starts the transmission of
                           trace entries to the host module,
                           and places the line trace entries
                           in the SYS010 work file and
                           both line and SIT entries in the
                           SYS012 work file.)

BG 000 IFU505E OC EXIT TO FORCE STOP

BG 000 IFU508I SIT   BLOCK      1 WRITTEN AT 15:12:48
BG 000 IFU508I TRACE BLOCK      1 WRITTEN AT 15:12:51
BG 000 IFU508I SIT   BLOCK    200 WRITTEN AT 15:13:12
BG 000 IFU508I TRACE BLOCK    200 WRITTEN AT 15:13:12

MSG BG                    (Stops the transfer of trace
                           blocks to the host module.)

BG 000 IFU506I  FORCE STOP ACKNOWLEDGED
BG 000 IFU508I  SIT   BLOCK   1,226 WRITTEN AT 15:14:27
BG 000 IFU503I  FUNCTION COMPLETED - 00
BG 000 IFU501A - REPLY WITH DESIRED FUNCTION OR 'END'

0 END                      (Stops the dynamic dump job.)

BG 000 EOJ DYNADUMP  MAX.RETURN CODE=0008
/*
//
```

Chapter 11. Using SSP CLISTs in MVS

You can use SSP command lists (CLISTs) to display selected NCP dump information online without formatting or printing the dump. By specifying a particular CLIST, you can indicate which NCP dump data you wish to view, such as registers, directly addressable storage, internal traces, and various other control blocks and storage areas.

This chapter discusses how to display sections of the SSP dumper utility online using SSP CLISTs.

Requirements for Using SSP CLISTs

To use SSP CLISTs to display NCP dumps, you must have two additional programs installed in the same MVS used to process the dumps: the Interactive Problem Control System (IPCS) and the Interactive System Productivity Facility (ISPF). For information about these programs, see the *MVS Interactive Problem Control System User's Guide and Reference* and *Interactive System Productivity Facility/Program Development Facility (MVS) Guide.*

In addition to having IPCS and ISPF, you must begin the SSP CLIST session with a *raw* (or *unformatted*) NCP dump. A raw dump has not been formatted by the SSP dump formatter utility and is still in hexadecimal. If you are using the SSP dumper utility, you prevent the SSP dump formatter utility from formatting the raw data by executing the IFLREAD program with the PARM=NOFORMAT option:

```
DUMPSTEP  EXEC  PGM=IFLREAD,PARM=NOFORMAT
```

The only DD statements you need to code when using this option are SYSUT1 (which communication controller is to be dumped) and SYSUT2 (which data set is to receive the dump). For information about the SSP dumper utility, see Chapter 7, "Using the SSP Dump Utilities in MVS" on page 201.

You can also invoke raw dump data by using the access method dumper facility. For more information about the access method facility, see "Using Access Method Dump Commands" on page 213.

The raw dump must be loaded prior to using SSP CLISTs. A *loaded* dump is a raw dump that has been reorganized to work properly with IPCS commands (used within the SSP CLISTs). The IFWILJCL CLIST is a JCL sample provided to invoke the IFWILOAD CLIST, the dump loading program. This loading program copies the raw dump and reorganizes it while keeping the original raw dump unchanged. IFWILJCL also provides a way to name the new loaded NCP dump.

IPCS requires that a dump directory be allocated for each dump being analyzed. Since SSP CLISTs do not make any provision for allocating such a data set, you are responsible for providing this data set for NCP dumps in the same format as is provided for other dumps processed with IPCS. Once you have a loaded dump and an allocated dump directory, the full set of SSP CLISTs is available for use.

For more information, see "Customizing the Program Invocation" on page 280.

Before using SSP CLISTs, the following limitations should be noted:

- If you would like to change an SSP CLIST, create a new CLIST instead of modifying one of the SSP CLISTs.
- Often the problem occurs with the NCP dump, not the SSP CLIST. When storage areas in the NCP dump are overlaid with meaningless data, the processing SSP CLIST may be unable to find or format the requested data.
- Dynamic dumps often contain incomplete or incorrect chains or pointers. For this reason, the following SSP CLISTs are not recommended for use with dynamic dumps:

  IFWINAU
  IFWIDISP
  IFWIBUSE
  IFWIEPCB
  IFWIREGS.

Customizing SSP CLISTs

SSP CLISTs should be customized for each MVS environment. They are provided as source code, so they can be altered. Although functional changes are not required, you are encouraged to evaluate the CLIST functions being provided and improve existing CLISTs or create new ones. Samples are provided for each CLIST that needs this customization, but it is your responsibility to determine the final format and content of each sample. You should be knowledgeable of IPCS, MVS, and JCL before attempting SSP CLIST customization.

Table 11 summarizes the CLISTs that you can review and alter. Any alterations to other CLISTs are considered to be unsupported changes (see "Problems to Consider When Customizing SSP CLISTs" on page 280).

Table 11 (Page 1 of 2). SSP CLISTs to Customize

CLIST	Description
IFWINCP	Begins the SSP CLIST session from the READY prompt. Calls IFWIALOC and IFWISET to allocate and initialize the dump data set.
IFWIALOC	Allocation routine called by IFWINCP to allocate data sets containing SSP CLISTs.
IFWINCP2	Sample menu invoked by IFWINCP0.
IFWINCP3	SSP CLIST menu used to access SSP CLISTs (Menu 1 of 2).
IFWIBATC	Submits jobs for batch processing. This CLIST does not appear on any menu and is called by IFWIDTRC, IFWILOCL, IFWILOAD, IFWIBTRC, and IFWIDTRC.[1]
IFWILOCL	Builds and submits local print jobs. This CLIST is called by several CLISTs.[1]
IFWILJCL	Sample JCL used to invoke IFWILOAD and prepare dump for use with IPCS.
IFWILPRS	JCL include file used by IFWILOCL to reroute output.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

Table 11 (Page 2 of 2). SSP CLISTs to Customize

CLIST	Description
IFWILPRT	Display panel called by IFWILOCL to accept JCL job card input.
IFWIBTRC	Builds the job card, calls IFWIBTRP, includes code from IFWIBTRS, and calls IFWIBTRA to create the trace. This CLIST is the driving program for the batch job branch trace and is called by IFWITRAC.[1]
IFWICTRC	Builds the job card, calls IFWICTRP, includes code from IFWICTRS, and calls IFWICTRA to create the trace. This CLIST is the driving program for the batch job CA IOH trace and is called by IFWITRAC.[1]
IFWIDTRC	Builds the job card, calls IFWIDTRP, includes code from IFWIDTRS, and calls IFWIDTRA to create the trace. This CLIST is the driving program for the batch job dispatcher trace and is called by IFWITRAC.[1]
IFWIBTRP	Displays JCL job card information. This CLIST is called by IFWIBTRC.[1]
IFWICTRP	Displays JCL job card information. This CLIST is called by IFWICTRC.[1]
IFWIDTRP	Displays JCL job card information. This CLIST is called by IFWIDTRC.[1]
IFWIBTRS	JCL to be included by IFWIBTRC as it creates a batch job.
IFWICTRS	JCL to be included by IFWICTRC as it creates a batch job.
IFWIDTRS	JCL to be included by IFWIDTRC as it creates a batch job.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

Besides describing each CLIST or JCL file that needs to be reviewed, the sections that follow discuss these topics concerning customization:

- CLIST data sets
- Customizing dump data set names
- Customizing sample menus
- JCL job card contents
- Customizing the program invocation
- Problems to consider when customizing CLISTs.

CLIST Data Sets

Code must be stored in allocated data sets. You need to establish the code so that typing a CLIST name (not the entire data set, just the member name) at the READY prompt causes the CLIST to be located and executed. It is recommended that you create and maintain a separate data set for the CLISTs to facilitate maintenance and customization efforts.

When shipped and installed, the SSP CLIST code is stored in three data sets:

SSPOBJ	Compiled object code
ASSPCLS1	CLISTs and associated panels
ASSPSRC1	Source code for corresponding compiled object code.

Before using SSP CLISTs, you must store two of them in an allocated data set: IFWINCP, the invocation routine, and IFWIALOC, the allocation routine. These two CLISTs need to be stored so they are found when typed at the READY prompt. IFWINCP begins the session from the READY prompt and invokes IFWIALOC to allocate data sets needed during your IPCS session. If the data sets that contain the CLISTs, panels, and object code are not allocated for implicit execution, you

must edit IFWIALOC to indicate the appropriate data set names. The sample provided includes data set allocations your site may not have. Therefore, you must carefully review IFWIALOC and add or delete allocations as necessary. You may also choose to allocate the CLIST data sets without using IFWIALOC. If so, edit IFWINCP and remove the call to IFWIALOC.

Customizing Dump Data Set Names

At the beginning of the SSP CLIST session, you enter IFWINCP at the READY prompt and display the Analyze NCP Dumps (IFWINCP) panel. This panel prompts you for the dump data set name. The code supplied assumes the dump data set name that begins with "IPCS." is followed by a 7-digit alphanumeric entry and ends with "DUMP" followed by a single character, as in the following example:

```
IPCS.P090338.DUMPC
```

This supplied code enforces some restrictions and provides a default feature for the final character. The specifics of the restrictions and default are described within the code, and you should review them when customizing dump data set names. You are not required to follow this convention; however, if you wish to change it, you must customize the prompt and verification code to provide a proper data set name to the remainder of the CLIST.

IFWINCP also contains the name of the dump directory file. This name is hard coded and should be reviewed or edited as needed. The dump directory is required by IPCS, but the name may be in any valid format.

For more information on this data set naming convention and the Analyze NCP Dumps (IFWINCP) panel, see "The SSP CLIST Session" on page 281.

Customizing Sample Menus

You can customize the two sample menus available in an SSP CLIST session: the Sample ISPF/PDF Primary Option Menu (IFWINCP0) and the Sample IPCS Primary Option Menu (IFWINCP2). Since both of these panels are sample menus, provided as examples, they are not required.

The Sample ISPF/PDF Primary Option Menu (IFWINCP0) appears after you have entered the dump data set name in the Analyze NCP Dumps panel (IFWINCP). This Sample ISPF/PDF Primary Option Menu lists available ISPF and PDF options and allows you to select an IPCS option, which invokes the Sample IPCS Primary Option Menu (IFWINCP2). If you wish, you may edit the IFWINCP CLIST to bypass this Sample ISPF/PDF Primary Option Menu and invoke either the IPCS Primary Option Menu or the first SSP CLIST Menu (IFWINCP3).

The Sample IPCS Primary Option Menu (IFWINCP2) is also a sample menu; you may choose to customize it by altering or bypassing it and invoking the first SSP CLIST Menu (IFWINCP3). However, since many of the IPCS options on this menu might be useful in an SSP CLIST session, such as the COMMAND option that allows you to enter a CLIST name or IPCS command on a command line instead of making a menu selection, you should consider carefully before eliminating it from the session.

For more information on these menus, see "Sample ISPF/PDF Primary Option Menu (IFWINCP0)" on page 282 and "Sample IPCS Primary Option Menu (IFWINCP2)" on page 283.

JCL Job Card Contents

Job card information is pulled in by several CLISTs from the user profile and is used for executing batch jobs or for routing CLIST output to printers or other resources. Table 12 shows JCL-related CLISTs.

Table 12. JCL-Related SSP CLISTs

CLIST	Description
IFWIBATC	Submits jobs for batch processing. This CLIST does not appear on any menu and is called by IFWIDTRC, IFWILOCL, IFWILOAD, IFWIBTRC, and IFWIDTRC.[1]
IFWILOCL	Builds and submits local print jobs. This CLIST is called by several CLISTs.[1]
IFWIBTRC	Builds the job card, calls IFWIBTRP, includes code from IFWIBTRS, and calls IFWIBTRA to create the trace. This CLIST is the driving program for the batch job branch trace and is called by IFWITRAC.[1]
IFWIBTRS	JCL to be included by IFWIBTRC as it creates a batch job.
IFWIBTRP	Displays JCL job card information. This CLIST is called by IFWIBTRC.[1]
IFWICTRC	Builds the job card, calls IFWICTRP, includes code from IFWICTRS, and calls IFWICTRA to create the trace. This CLIST is the driving program for the batch job CA IOH trace and is called by IFWITRAC.[1]
IFWICTRS	JCL to be included by IFWICTRC as it creates a batch job.
IFWICTRP	Displays JCL job card information. This CLIST is called by IFWICTRC.[1]
IFWIDTRC	Builds the job card, calls IFWIDTRP, includes code from IFWIDTRS, and calls IFWIDTRA to create the trace. This CLIST is the driving program for the batch job dispatcher trace and is called by IFWITRAC.[1]
IFWIDTRS	JCL to be included by IFWIDTRC as it creates a batch job.
IFWIDTRP	Displays JCL job card information. This CLIST is called by IFWIDTRC.[1]

[1] To access this SSP CLIST, enter the name of the CLIST that it is called by.

[2] This SSP CLIST is not recommended for use in viewing dynamic dumps.

Besides altering JCL-related CLISTs, you should check the following:

- The information in the job card (to ensure that the cards produced are compatible with your MVS environment)
- Prompts for node names, identifications, and message class
- The location of the object code being invoked (to ensure the named data set is where you have stored the code).

Customizing the Program Invocation

You must begin an SSP CLIST session with a *raw* (or *unformatted*) NCP dump. A raw dump has not been formatted by the SSP dump formatter utility and is still in hexadecimal. This raw dump must be loaded before using SSP CLISTs. A *loaded* dump is a raw dump that has been reorganized to work properly with IPCS commands (used within the SSP CLISTs). IFWILJCL is a JCL sample provided to invoke IFWILOAD, the dump loading program. This loading program copies the raw dump and reorganizes it while keeping the original raw dump unchanged. IFWILJCL also provides a way to name the new loaded NCP dump. IFWILJCL contains several items that you must alter:

- Job card
- Location of compiled code (IFWILOAD)
- Name of raw dump data set
- Name of destination (loaded) dump data set.

For more information about IFWILJCL, see "Requirements for Using SSP CLISTs" on page 275.

Once loaded, the dump is available for use with other CLISTs.

Problems to Consider When Customizing SSP CLISTs

Changes to the CLISTs produced by IBM (for instance, PTFs or new release changes) arrive in the form of new, replacement CLISTs. If you have altered an existing CLIST, left it in the installation data set, and not changed the name, the new CLIST will replace the old one and your changes will be lost. Therefore, you are urged to protect any changes you have made by creating backup copies of the affected CLISTs and by renaming or moving them so they will not be replaced. Renaming is probably the more difficult option since calling routines (if any) must also be changed.

IBM supports only those CLISTs that are provided as samples. If you change sample CLIST code, you are then responsible for support of the code. If you wish to change code other than sample code, consider copying the original code and then altering and running the copy. If a problem occurs, the original can be executed to check for the same problem. If the problem persists with the original code, support is provided through the IBM Support Center. In fact, IBM encourages you to report your needs and problems so that IBM can make enhancements beneficial to all users.

Finally, you are cautioned to keep careful records of customization changes to facilitate upgrades and to assist in any service-related problems. You should also keep the original raw dump since it may be required by the IBM Support Center, especially if the loading routines (IFWILCJL and IFWILOAD) are suspected in a problem call. Once you no longer need the dump loaded on IPCS, you can remove both the raw and loaded dumps.

The SSP CLIST Session

The SSP CLIST session consists of five panels:

Analyze NCP Dumps (IFWINCP) panel	Provides access to the dump you wish to display.
Sample ISPF/PDF Primary Option Menu (IFWINCP0)	Displays a sample menu of ISPF and parallel data field (PDF) options; provides access to the SSP CLIST menus.
Sample IPCS Primary Option Menu (IFWINCP2)	Displays a sample menu of IPCS options; provides access to the SSP CLIST menus.
SSP CLIST Menu 1 (IFWINCP3) SSP CLIST Menu 2 (IFWINCP4)	Displays two menus for selecting SSP CLISTs to view NCP dump data.

Using the SSP CLIST Session

To begin the SSP CLIST session, enter IFWINCP from the READY prompt. The IFWINCP CLIST invokes the first of five panels, Analyze NCP Dumps (IFWINCP), shown in Figure 29.

Invalid Data and IPCS Message: If you enter invalid data after the promt, ===> you receive the following IPCS information message: `IKJ56545I THIS STATEMENT HAS AN EXPRESSION WITH A CHARACTER DATA ITEM USED NUMERICALLY.` For example, if you enter, –5 for a selection instead of 5, you would recieve the IPCS message and you do not receive the requested output.

```
*****************************************************************
*                      Analyze NCP Dumps                        *
* IFWINCP:                                                      *
*                                                               *
* Dumps are located in the IPCS.* data set.  Enter the specific *
* data set name in one of two formats:                          *
*                                                               *
*    Enter       To Analyze                                     *
*                                                               *
*   NNNNNNN     'IPCS.NNNNNNN.DUMP?' - use dump last selected   *
*                                      for this data set name   *
*                                      (code replaces ?)        *
*                                                               *
*   NNNNNNN*    'IPCS.NNNNNNN.DUMP*' - * is any letter used     *
*                                      to identify a dump       *
*                                                               *
*    X to EXIT                                                  *
*                                                               *
*****************************************************************

Enter Data Set Name ===>
```

Figure 29. Analyze NCP Dumps (IFWINCP) Panel

All dumps are located in the IPCS data set. In order to load and open an NCP dump, you must enter its complete IPCS data name in one of two formats. The Analyze NCP Dumps panel displays these formats: NNNNNNN or NNNNNNN*.

The program fills in "IPCS." before your 7-digit alphanumeric entry and ".DUMP*" after your entry (replacing the * with a letter), as shown in this example:

```
IPCS.P090338.DUMPC
```

Although you can use any valid data set name, you cannot use a dump name being used in another IPCS session because the dump directory and analysis file are currently allocated to that dump name. For information on customizing these data set names, see "Customizing Dump Data Set Names" on page 278.

MVS/ESA: If you have an MVS/ESA system, an additional prompt displays:

```
BLS18099D  Treat input only as trace data?
Enter Y for Yes, N for full initialization.
```

Answer this prompt by entering N. If you enter any other response, the SSP CLISTs are unable to locate stored data. The MVS/ESA system allows nondump data sets. The NCP dump requires full initialization and is not a trace data set.

Sample ISPF/PDF Primary Option Menu (IFWINCP0)

After you enter the dump data set name in the Analyze NCP Dumps panel, the Sample ISPF/PDF Primary Option Menu (IFWINCP0), shown in Figure 30, is displayed.

```
------------------  *SAMPLE* ISPF/PDF PRIMARY OPTION MENU  ------------------
OPTION  ===>
                                                          USERID   -
   0 ISPF PARMS  - Specify terminal and user parameters   DATE     -
   1 BROWSE      - Display source data or output listings JULIAN   -
   2 EDIT        - Create or change source data           TIME     -
   3 UTILITIES   - Perform utility functions              PREFIX   -
   4 FOREGROUND  - Invoke foreground language processors  TERMINAL -
   5 BATCH       - Submit job for language processing     PF KEYS  -
   6 COMMAND     - Enter TSO command or CLIST             PROC     -
   7 DIALOG TEST - Perform dialog testing
   8 LM UTILITIES- Perform library administrator utility functions
   9 IBM PRODUCTS- Additional IBM program development products
   C CHANGES     - Display summary of changes for this release
   D PROBLEM UTIL- Utility functions for problem analysis
   I IPCS        - IPCS problem analysis services
   R RACF        - RACF administration
   RM RMDSVIEW   - RMDS TSO Viewer
   S SDSF        - Spool Display and Search Facility
   T TUTORIAL    - Display information about ISPF/PDF
   X EXIT        - Terminate ISPF using log and list defaults

Enter END command to terminate ISPF.
```

Figure 30. Sample ISPF/PDF Primary Option Menu (IFWINCP0)

This sample menu lists available ISPF and PDF options, such as displaying output listings or editing source data. It also provides access to the Sample IPCS Primary Option Menu (IFWINCP2). To display this menu, select option I (IPCS—IPCS problem analysis services) from the ISPF and PDF options.

You can customize the SSP CLIST session to bypass the Sample ISPF/PDF Primary Option Menu (IFWINCP0) since it is a sample menu. For information on customizing your session, see "Customizing Sample Menus" on page 278.

Sample IPCS Primary Option Menu (IFWINCP2)

When you select the IPCS option from the Sample ISPF/PDF Primary Option Menu, the IFWINCP2 CLIST is invoked. The IFWINP2 CLIST displays the Sample IPCS Primary Option Menu, shown in Figure 31.

```
------------------ *SAMPLE* IPCS PRIMARY OPTION MENU ----------------------
OPTION  ===>
                                                      ********************
   0  DEFAULTS    - Specify default dump and options    * USERID  -
   1  BROWSE      - Browse dump data set                * DATE    -
   2  ANALYSIS    - Analyze dump contents               * JULIAN  -
   3  UTILITY     - Perform utility functions           * TIME    -
   4  COMMAND     - Enter IPCS subcommand or CLIST      * PREFIX  -
   5  VTAM        - VTAM analysis commands              * TERMINAL-
                                                        * PFKEYS  -
   6  NCP         - NCP analysis commands               * PROC    -
                                                        ********************
   7  NMP         - NMP analysis commands
   T  TUTORIAL    - Learn how to use the IPCS dialog
   X  EXIT        - Terminate using log and list defaults

Enter END command to terminate IPCS dialog
```

Figure 31. Sample IPCS Primary Option Menu (IFWINCP2)

The Sample IPCS Primary Option Menu (IFWINCP2) provides two options that enable you to invoke the SSP CLISTs you need. If you already know the SSP CLIST you wish to invoke or if you need to enter an IPCS command, enter option 4 (COMMAND—Enter IPCS subcommand or CLIST). After selecting this option, you will see a command line on the panel on which you can enter the CLIST name or command. However, if you would prefer to display an SSP CLIST menu with a list of some (not all) of the CLISTs available to you and a brief description of what they do, select option 6 (NCP—NCP analysis commands). When you select this option, the first panel of the SSP CLIST menus (IFWINCP3) is displayed.

Besides providing these options to enable you to access SSP CLISTs, the Sample IPCS Primary Option Menu (IFWINCP2) provides many other useful IPCS options. For instance, if you select 0 (DEFAULTS—Specify default dump and options), you can view the name of the currently active dump data set and set the default dump data set name.

You can customize the SSP CLIST session to substitute, alter, or bypass the Sample IPCS Primary Option Menu (IFWINCP2) since it is a sample menu. For information on customizing your session, see "Customizing Sample Menus" on page 278.

SSP CLIST Menu 1 (IFWINCP3) and Menu 2 (IFWINCP4)

SSP CLIST Menu 1 (IFWINCP3) and its second page, SSP CLIST Menu 2 (IFWINCP4), are shown in Figure 32 and Figure 33, respectively.

```
------------------------- SSP CLIST MENU 1 of 2 -----------------------------

  1    - IFWILEVL - NCP & SSP version and release, dump date & name, etc.
  2(p) - IFWIREGS - Level 1, 2, 3, 4 and 5 registers
  3(p) - IFWIDIR  - Direct addressable control blocks
  4(p) - IFWIBUSE - Addresses of the buffers in use
  5(p) - IFWIBNN  - Boundary network node control blocks
  6(p) - IFWICA   - Channel adapter control blocks
  7(p) - IFWIERP  - Error recovery information (L1B, L1X)
  8    - IFWIFIND - Sub-menu / search for value or display address
  9    - IFWINAU  - Resource control blocks for lines, PUs, LUs
 10    - IFWIPATH - Sub-menu / all control blocks by network or by subarea
 11    - IFWISAVE - Save areas for a specified level
 12(p) - IFWISESS - Session control and physical services control blocks
 13(p) - IFWISLOW - Information on NCP slowdown / buffers, thresholds
 14    - IFWIVRB  - Virtual route vector table and assigned VRBs

   F              - Forward to SSP CLIST MENU 2

 For screen display enter the selection number    (e.g.  2   ).
 To print, enter selection number followed by p   (e.g.  2p  ).
Select CLIST ===>
-------------------------------------------------------------------------
```

Figure 32. SSP CLIST Menu 1, IFWINCP3

```
------------------------- SSP CLIST MENU 2 of 2 -----------------------------

   1(p) - IFWIEPCB - Emulation Program (EP) control blocks
   2(p) - IFWIAVB  - Token Ring / Frame Relay - AVB, PLBAT, LLBAT, SNAP
   3(p) - IFWISSNP - NPSI snap trace
   4(p) - IFWISNAU - Sub-menu / NPSI resource control blocks
   5(p) - IFWIDISP - Dispatch priority table
   6(p) - IFWIHARD - Adapter information table, line and channel adapters
   7(p) - IFWIMAP  - Load map - written to a data set (or printed)
   8(p) - IFWIMOSS - Maintenance and operator subsystem (MOSS) control blocks
   9    - IFWITRAC - Sub-menu / selection of internal traces
  10    - IFWIMOD  - Locate a specified module in storage
  11    - IFWIWHER - Translate hex address into module name and offset
  12(p) - IFWILIMS - ODLC Adapter resources
  13(p) - IFWISNAP - NCP snap trace table
  14    - IFWIPOOL - Sub-menu / select free pool to view
  15    - IFWIIP   - Sub-menu / select IP related control blocks
     B  - Back to SSP CLIST MENU 1

  For screen display enter the selection number    (e.g.  2   ).
  To print, enter selection number followed by p   (e.g.  2p  ).

 Select CLIST ===>
```

Figure 33. SSP CLIST Menu 2, IFWINCP4

These menus list CLISTs that enable you to obtain dump information (such as version and release numbers), display or print sections of the dump (such as specified registers or control blocks), or access other submenus (such as menus for control blocks by network).

To display the selected dump data online, enter a selection number from SSP CLIST Menu 1 or 2. See "SSP CLIST Descriptions" on page 285 for definitions of all SSP CLISTs. To print the selected dump data, enter a selection number followed by a **p**. For instance, if you enter **6p** on the command line in SSP CLIST Menu 1, you invoke the IFWICA CLIST, which prints all the channel adapter control blocks in your NCP dump. If you just enter **6**, you view this information online.

To move forward from SSP CLIST Menu 1 to SSP CLIST Menu 2, enter **f**; to return to SSP CLIST Menu 1 from SSP CLIST Menu 2, enter **b**.

Ending the SSP CLIST Session

To exit SSP CLIST Menu 1 or 2 and return to the previous menu level, press **F3**. From this menu level, enter **x** to return to the ISPF/PDF Primary Option Menu (IFWINCP0). When you exit IFWINCP0, IFWINCP frees the dump directory and analysis file.

SSP CLISTs

This section provides a description of each SSP CLIST (Table 13) and tells which CLISTs to use to locate specific information such as control blocks (Table 14 on page 294), chains and pointers (Table 15 on page 298), and specific functions or requests (Table 16 on page 299).

SSP CLIST Descriptions

Table 13 lists the SSP CLISTs you can use to view NCP dumps and describes each SSP CLIST.

Table 13 (Page 1 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWIALOC	Allocates data sets containing SSP CLISTs. This CLIST is called by IFWINCP.
IFWIAVB	Displays the AVB, PLBAT, LLBAT, SNAP, and LLT for NTRI and 3745 frame-relay resources.
IFWIBATC	Submits jobs for batch processing. This CLIST does not appear on any menu and is called by IFWIDTRC, IFWILOCL, IFWILOAD, IFWIBTRC, and IFWICTRC.[1]
IFWIBLU	Displays the control blocks for BNN logical unit.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 2 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWIBNN	Displays the control blocks related to the boundary network node. A print option is provided because of the quantity of output. The control blocks include: BCT BSB for dependent SSCP-LU sessions BSB for independent LU sessions BXI for dependent LUs BXI for independent LUs CBB CUB for dynamic reconfiguration CXI CX2 CXB LDA LNB LND LTX LUB LUX NNT QAB QAX QPB SCE SSB
IFWIBNPU	Displays the control blocks for BNN logical unit.
IFWIBTRA	Builds a branch trace as a batch job. Assembler routine called indirectly by IFWIBTRC.
IFWIBTRC	Builds the job card, calls IFWIBTRP, includes code from IFWIBTRS, and calls IFWIBTRA to create the trace. This CLIST is the driving program for the batch job branch trace and is called by IFWITRAC.[1]
IFWIBTRP	Displays JCL job card information. This CLIST is called by IFWIBTRC.[1]
IFWIBTRS	JCL to be included by IFWIBTRC as it creates a batch job.
IFWIBUFS	Checks several queues to count the buffers in use and returns the information to IFWISLOW (calling CLIST).[1]
IFWIBUSE[2]	Lists the number of buffers in use and the address of each buffer. Lists the buffers currently being used for dynamic control blocks. This CLIST takes several minutes to execute.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 3 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWICA	Displays the channel adapter control blocks: CAVT CAVT CAB pointers CAVT CER pointers. Displays the control blocks for each channel: ACB AXB CAB CABEXT CAP CBB CER GCBB LGT LKB PUV SCB SXB. A print option is provided because of the quantity of output. This CLIST calls IFWICAB.
IFWICAB	Lists CAB and related control blocks. This CLIST is called by IFWICA.[1]
IFWICTRA	Builds a CA IOH trace as a batch job. Assembler routine called indirectly by IFWICTRC.
IFWICTRC	Builds the job card, calls IFWICTRP, includes code from IFWICTRS, and calls IFWICTRA to create the trace. This CLIST is the driving program for the batch job CA IOH trace and is called by IFWITRAC.[1]
IFWICTRP	Displays JCL job card information. This CLIST is called by IFWICTRC.[1]
IFWICTRS	JCL to be included by IFWICTRC as it creates a batch job.
IFWIDIR	Displays the NCP direct addressable control blocks: DTG FAX HWE HWX NTI NTT NTW XDA XDB XDH.
IFWIDISP[2]	Displays and expands the dispatch priority table (DPT).

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 4 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWIDTRA	Builds a dispatcher trace as a batch job Assembler routine called indirectly by IFWIDTRC.
IFWIDTRC	Builds the job card, calls IFWIDTRP, includes code from IFWIDTRS, and calls IFWIDTRA to create the trace. This CLIST is the driving program for the batch job dispatcher trace and is called by IFWITRAC.[1]
IFWIDTRP	Displays JCL job card information. This CLIST is called by IFWIDTRC.[1]
IFWIDTRS	JCL to be included by IFWIDTRC as it creates a batch job.
IFWIEPCB[2]	Displays the EP control blocks: CAVT CCB CER CHCB CHVT NSCCB.
IFWIERP	Displays error recovery information: ABN, L1B, and L1X control blocks GES control block Level 1, 2, 3, 4, and 5 registers.
IFWIFIND	Provides a menu that allows you to search storage for a specified value, and designate how to display that information. The six options on the menu are: • Display one complete buffer • Find the specified value in the buffer pool and display the buffer • Find the specified value outside the buffer pool and display X'100' bytes • Find the specified value within a given area and display a specified amount of data • Display storage starting at a specified address and ending at a specified length • Search only at a specified offset of each buffer for a specified value.
IFWIHARD	• Displays and expands the adapter information table (AIT) showing line and channel adapters. • Displays the CDS control block. • Displays the CST control block.
IFWIHLP1	Displays help information for panels IFWINCP3 and IFWINCP4.
IFWIHLP2	Displays help information for panel IFWIREGP.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 5 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWIIP	Displays the: • HRT, HRE and associated RIBs • SRT, SRE and associated RIBs • NRT, NRE and associated RIBs • LAT, LAE and associated RIBs • RDA, RDF and associated RIBs • IPS, IPX, IPC • IDQ • IP snap trace table.
IFWILEVL	Displays the: • NCP version and release numbers • SSP version and release numbers • Machine type • CCU serial number and hardware model • NCP subarea number • Date and time NCP was generated • Date and time NCP dump occurred.
IFWILIMS	Displays CSS adapter related control blocks.
IFWILJCL	Sample JCL used to invoke IFWILOAD and prepare dump for use with IPCS.
IFWILOAD	Copies and reformats the raw dump, preparing it for use with SSP CLISTs (creating a loaded dump). Only the header record is reformatted.
IFWILOCL	Builds and submits local print jobs. This CLIST is called by several CLISTs.[1]
IFWILPRS	JCL include file used by IFWILOCL to reroute output.
IFWILPRT	Display panel called by IFWILOCL to accept JCL job card input.
IFWIMAP[3]	Creates a load map and places it in a data set that can be viewed with standard TSO utilities or prints it (depending on your choice of options).
IFWIMOD[3]	Locates a specified module in storage and displays its: • Beginning and ending addresses • Hexadecimal length • The historical job number (HJN) or, if fixes have been made to that module, the program temporary fix (PTF).

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 6 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWIMOSS	Displays the MOSS control blocks: CPIT MBXIN MBXOUT MIF MTF Expansion of the CRP.
IFWINAU[2]	Serves as the driver for displaying control blocks related to a particular resource. Displays the resource control blocks for lines, physical units, logical units, clusters, and terminals. On a menu, you specify one of the following: • Element address • LNVT entry address (also known as BAR) • Relative line number (RLN) • Resource name.
IFWINAUR	Lists the network addressable unit (NAU) control blocks for an NAU. May also display NTO, SMMF, or gateway NAU control blocks.
IFWINCP	Begins the SSP CLIST session from the READY prompt. Calls IFWIALOC and IFWISET to allocate and initialize the dump data set.
IFWINCP0	Sample menu invoked by IFWINCP.
IFWINCP2	Sample menu invoked by IFWINCP0.
IFWINCP3	SSP CLIST menu used to access SSP CLISTs (Menu 1 of 2).
IFWINCP4	SSP CLIST menu used to access SSP CLISTs (Menu 2 of 2).
IFWINET	Displays path control blocks for a given network. This CLIST is called by IFWIPATH[1] and does not work as a stand-alone CLIST. This CLIST calls IFWISA and IFWIVRSA.
IFWINPS	Displays the NCP physical service and NCP session control blocks.
IFWINPU	Displays the control blocks for an INN physical unit.
IFWIPATH	Provides a menu to obtain control blocks by network, by subarea, or by both. The options on the menu are: • All control blocks • Control blocks for a given network • Control blocks for a given subarea. This CLIST calls IFWINET.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 7 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWIPOOL	Provides a menu that allows you to select a resource pool and displays the GPA and any free chains of control blocks in that pool. This CLIST calls IFWISGPA. These control blocks include: BSB for dependent LU sessions — NIB BSB for independent LU sessions — NIX BSB for dependent SSCP-LU sessions — NLB BXI for dependent LUs — NLX BXI for independent LUs — NNT CBB — NQE CUB — NQX CXB — NRE CXI — NSB CX2 — NSC FCT — NSX HRE — NVT ODLC LAN — RVT LDA — SCE LKE — SRE LLB for token-ring — SSB LLB for frame relay — TGB LNB — TRT LND — VAT LTX — VTS LUB — VVT LUX
IFWIPSNA	Displays the line control blocks for a pre-SNA line.
IFWIPSTM	Displays the control blocks for a pre-SNA terminal and its cluster, if it has one.
IFWIPUV	Calculates the length of the PUV.
IFWIREGP	Register display panel called by IFWIREGS to display registers 0-7.
IFWIREGS	Displays the level 1, 2, 3, 4, and 5 registers.
IFWISA	Lists control blocks for a given NCP subarea. This CLIST is called by IFWINET[1] and calls IFWITGB.
IFWISAVE	Displays the save areas for a specified level. You specify which level and how many save areas to display.
IFWISAVT	Locates the NPSI AVT control block. This CLIST is called by IFWISSNP and IFWISNAU.[1]
IFWISCBL	Lists the MKB control blocks associated with a given MKB. This CLIST is called by IFWISPTH.[1]

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 8 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWISELE	Obtains the address of MKB that corresponds to an element address. This CLIST is called by IFWISPTH.[1]
IFWISESS	Displays the physical services and session control blocks: PSB PSI SNPs VTS.
IFWISET	Initializes dump and establishes the direct addressable. This CLIST is called by IFWINCP and IFWILEVL.[1]
IFWISGPA	Displays the addresses of items queued to the specified generic pool anchor block (GPA). This CLIST is called by IFWIPOOL.[1]
IFWISLOW	When NCP is in slowdown, this CLIST displays: • Count of buffers queued • Total buffers allocated • Current count of free buffers • Slowdown entry and exit thresholds. This CLIST calls IFWIBUFS and takes several minutes to execute.
IFWISNA	Displays the line control blocks for an SDLC line and the PLX for NTRI resources.
IFWISNAP	Displays the NCP snap trace table.
IFWISNAU	Displays resource control blocks for NPSI resources. You enter an element address or resource name and select which NPSI control blocks you want to see: MKB VCB. This CLIST calls IFWISPTH.
IFWISPTH	Provides a menu of NPSI control block selections. This CLIST is called by IFWISNAU[1] and calls IFWISCBL, IFWISELE, IFWISRSN, and IFWISVCB.
IFWISRSN	Determines the element address from a specified resource type (line, physical unit, or logical unit) and name. This CLIST is called by IFWISPTH.[1]
IFWISSNP	Displays or prints the X.25 NCP Packet Switching Interface (NPSI) snap trace. This CLIST calls IFWISAVT.
IFWISVCB	Lists the virtual control blocks related to a given MKB. This CLIST is called by IFWISPTH.[1]
IFWITGB	Lists the DCL control blocks related to a given transmission group control block. This CLIST is called by IFWISA.[1]

[1] To access this SSP CLIST, enter the name of the CLIST that it is called by.

[2] This SSP CLIST is not recommended for use in viewing dynamic dumps.

[3] The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Table 13 (Page 9 of 9). SSP CLISTs for Analyzing and Manipulating NCP Dumps

CLIST	Description
IFWITRAC	Provides a menu to access internal trace information. The nine options on the menu are: • Port swap trace table • GPT control block • Channel adapter (CA) trace table • Address trace table • Unformatted dispatcher trace table • Formatted dispatcher trace table • Unformatted branch trace table • Formatted branch trace table • Formatted channel adapter input/output halfword (CAIOH) trace. This CLIST calls IFWIBTRC, IFWICTRC, and IFWIDTRC.
IFWIVIRT	Displays the line control blocks for an SDLC virtual line. This line may be an NPA, an NTO, or an NRF line.
IFWIVRB	Displays the virtual route vector table and all currently assigned virtual route control blocks (VRBs). You can select the VRBs by: • Origin subarea • Virtual route number • Origin subarea and virtual route number.
IFWIVRSA	Lists the virtual route control blocks. This CLIST is called by IFWINET.[1]
IFWIVTLU	Displays the logical unit control blocks for an SDLC virtual logical unit. This logical unit may be an NPA, an NTO, or an NRF logical unit.
IFWIVTPU	Displays the physical unit control blocks for an SDLC virtual physical unit. This physical unit may be an NPA, an NTO, or an NRF physical unit.
IFWIWHER[3].	Given an address, this CLIST returns: • Module name • Offset into that module • Level and HJN or PTF number.

1 To access this SSP CLIST, enter the name of the CLIST that it is called by.

2 This SSP CLIST is not recommended for use in viewing dynamic dumps.

3 The length and starting address of some modules may be inaccurate because:

- Unused storage between the module delimiter ($$$$*module_name*) and the beginning of the next module that must begin on a 4KB alignment boundary is added to the length of the next module
- Any storage occupied by a control block that precedes a module is added to the length of the next module.

Locating Specific NCP Dump Information with SSP CLISTs

Besides using the IFWIFIND CLIST (see page 288) to search for and display specific sections of storage, you can select or execute SSP CLISTs to display specific information. This section contains three tables that tell you which SSP CLISTs to use to display specific information:

Table 14 lists CLISTs used to display control blocks.

Table 15 on page 298 lists CLISTs used to display chains and pointers.

Table 16 on page 299 lists CLISTs used to display information about a specific function such as an abend or trace.

Control Blocks

Table 14 shows the CLISTs you can use to display and analyze a specific control block. NTRI, NPSI, and EP control blocks are not displayed if those resources were not used in the NCP being dumped.

Table 14 (Page 1 of 5). CLISTs for Locating Control Blocks

Control Block	CLIST
ABN (abend control block)	IFWIERP
ACB (adapter control block)	IFWICA, IFWINAU
AIT (adapter information table)	IFWIHARD
ARE (address resolution protocol entry)	IFWIIP
ART(address resolution protocol table)	IFWIIP
ATT (ACB trace table)	IFWINAU
AVB (address vector control block)	IFWIAVB
AVX (address vector control block extension)	IFWIAVB
AXB (adapter control block extension)	IFWICA, IFWINAU
BCT (BFSESSINFO PIU control table)	IFWIBNN
BSB (boundary session block)	IFWINAU, IFWIBNN
BXI (BSB extension)	IFWINAU, IFWIBNN
CAB (channel adapter control block)	IFWICA
CAP (channel adapter parameter table)	IFWICA
CAVT (channel adapter vector table)	IFWIEPCB, IFWICA
CBB (committed buffers block)	IFWICA, IFWINAU, IFWISNA, IFWIBNN
CCB (character control block)	IFWIEPCB
CDS (configuration data set)	IFWIHARD
CER (channel adapter ERP control block)	IFWIEPCB, IFWICA
CHCB (channel control block)	IFWIEPCB
CHVT (channel vector table)	IFWIEPCB
CPIT (control program information table)	IFWIMOSS
CRP (check record pool)	IFWIMOSS
CST (CSS status table)	IFWIHARD

Table 14 (Page 2 of 5). CLISTs for Locating Control Blocks

Control Block	CLIST
CUB (common physical unit block)	IFWINAU
CUB (physical unit) pool anchor	IFWIBNN, IFWIPOOL
CXB (common physical unit block extension)	IFWINAU, IFWIBNN
CXI (common physical unit block extension for embedded blocks)	IFWINAU, IFWIBNN
CX2 (peripheral physical unit block extension 2)	IFWINAU, IFWIBNN
DPT (dispatch priority table)	IFWIDISP
DTG (date and time generation control block)	IFWIDIR
DVB (device base control block)	IFWINAU
FAX (fullword direct addressable extension)	IFWIDIR
GCB (group control block)	IFWINAU
GCBB (group control block for channel links)	IFWICA
GES (get error status table)	IFWIERP
GPA (generic pool anchor block)	IFWIBNN, IFWIPOOL
Free HRE (host route entry)	IFWIPOOL
HRE (host route entry)	IFWIIP
HRT (host route table)	IFWIIP
HSH (token-ring hash table)	IFWISNA
HWE (extended halfword direct addressables)	IFWIDIR
HWX (extended halfword direct addressables extension)	IFWIDIR
IDQ (internet protocol datagram queue control block)	IFWIIP
IPC (internet protocol congestion)	IFWIIP
IPS (internet protocol router statistics)	IFWIIP
IPX (internet protocol router statistics control block extension)	IFWIIP
LACB (processor-NCP ODLC adapter control block)	IFWISNA, IFWILIMS
LAE (local address entry)	IFWIIP
LAT (local address entry table)	IFWIIP
LCB (line control block (BSC/SS))	IFWINAU
LDA (logical unit block extension data area)	IFWIBNN
LDP (processor-NCP dynamic PSA control block)	IFWISNA, IFWILIMS
LGT (line group table (NCP))	IFWICA, IFWINAU
LIB (level-1 control block)	IFWIERP
LIT (line interface table)	IFWINAU
LIX (L1B control block extension)	IFWIERP
LKB (line control block (SDLC))	IFWICA, IFWINAU
LKE (LKB ODLC extension)	IFWISNA
LLBAT (logical link block address table)	IFWINAU
LLT (logical line timer table)	IFWIAVB

Table 14 (Page 3 of 5). CLISTs for Locating Control Blocks

Control Block	CLIST
LMB (LIM control block)	IFWILIMS
LME (LMB extension)	IFWILIMS
LNB (logical unit network address control block)	IFWINAU
LNK (NCST LINK session control block)	IFWINAU
LPSA (processor-NCP PSA control block)	IFWISNA, IFWILIMS
LRB (logical unit routing block)	IFWINAU
LTX (logical unit terminal node extension)	IFWINAU
LUB (logical unit pool anchor block)	IFWIBNN
LUV (logical unit vector table)	IFWINAU
LUX (logical unit block extension)	IFWINAU
MBXIN (MOSS mailbox IN)	IFWIMOSS
MBXOUT (MOSS mailbox OUT)	IFWIMOSS
MIF (MOSS interface control block)	IFWIMOSS
MKB (multichannel link block)	IFWISNAU
MTF (mailbox trace facility)	IFWIMOSS
NAB (NSC pool anchor block)	IFWIBNN, IFWIBLU
NACB (NCP-LIM ODLC anchor control block)	IFWISNA, IFWILIMS
NDP (NCP-LIM dynamic PSA control block)	IFWISNA, IFWILIMS
NIB (network interconnect control block)	IFWINAU
NLB (programmed resource logical unit block)	IFWINAU
NNT (network names table)	IFWIBNN
NPB (physical unit block)	IFWINAU
NPSA (NCP-LIM PSA control block)	IFWISNA, IFWILIMS
NPU (NTO PU control block)	IFWINAU
NRE (network router entry)	IFWIIP
NRT (network router entry table)	IFWIIP
NSC (NPA session counters control block)	IFWINAU, IFWIBLU
NSCCB (native subchannel CCB)	IFWIEPCB
PLB (physical link control block)	IFWINAU
PLBAT (physical link block address table)	IFWIAVB
PLUA (physical link adapter control block)	IFWISNA
PLX (physical link block extension)	IFWISNA
PNK (session control block for PUs)	IFWINAU
PRB (physical unit routing block)	IFWINAU
PSA (parameter/status area control block)	IFWINAU
PSB (physical services block)	IFWISESS, IFWINAU
PSI (product set identifier)	IFWISESS
PUV (physical unit vector table)	IFWICA, IFWINAU

Table 14 (Page 4 of 5). CLISTs for Locating Control Blocks

Control Block	CLIST
QAB (queue anchor block)	IFWIBNN
QAN (queue anchor block for a network)	IFWIBNN
QAX (queue anchor block extension)	IFWIBNN
QPB (queue pointer block)	IFWIBNN
RCB (resource connection block)	IFWINAU
RDA (routing data area)	IFWIIP
RDF (routing data area for fragmentation control block)	IFWIIP
RDM (routing data area for fragment reassembly)	IFWIIP
RDO (routing data area for options processing)	IFWIIP
SCB (station control block)	IFWICA, IFWINAU
SCE (SCB extension)	IFWIBNPU
SEB (search element control block)	IFWINAU
SHB (search tree header control block)	IFWINAU
SLB (ESCA link control block)	IFWISNA
SNAP (snap trace table (ODLC))	IFWISNAP
SNP (SSCP-NCP session control block)	IFWISESS, IFWINAU
SPC (session path control block)	IFWINAU
SRE (subnetwork route entry)	IFWIPOOL
SRT (subnetwork route entry table)	IFWIPOOL
SSB (ESCA station control block)	IFWIBNPU
SXB (station control block extension)	IFWICA, IFWINAU
SX2 (subarea physical block extension 2	IFWICA, IFWIINPU
TLB (token ring physical line control block)	IFWISNA
TRA (ALT trace ACB)	IFWILIMS
TRB (ALT trace LKB)	IFWILIMS
TRE (ALT trace LKE)	IFWILIMS
TRX (ALT trace AXB)	IFWILIMS
TSB (token ring station control block)	IFWIBNPU
VAT (virtual route access table)	IFWIBNN
VCB (virtual circuit block)	IFWISNAU
VLB (programmed resource virtual line block)	IFWINAU
VLU (NTO line control block)	IFWINAU
VRB (virtual route control block)	IFWIVRB
VTS (vector table of SNPs)	IFWISESS, IFWINAU
VVT (virtual route vector table)	IFWIVRB, IFWIBNN
XDA (word direct addressable storage)	IFWIDIR
XDB (byte direct addressable storage)	IFWIDIR
XDH (halfword direct addressable storage)	IFWIDIR

Table 14 (Page 5 of 5). CLISTs for Locating Control Blocks

Control Block	CLIST
XUA (physical link adapter control block extension)	IFWINAU

Chains and Pointers

Table 15 shows SSP CLISTs used to locate and analyze chains and pointers, and locate generic pool anchor blocks (GPA).

Table 15 (Page 1 of 2). CLISTs for Locating GPAs, Chains, and Pointers

GPA, Chain, or Pointer	CLIST
BSB	IFWIPOOL, IFWIBNN
BXI	IFWIPOOL, IFWIBNN
CBB	IFWIPOOL, IFWIBNN
CUB	IFWIPOOL, IFWIBNN
CXB	IFWIPOOL, IFWIBNN
CXI	IFWIPOOL, IFWIBNN
CX2	IFWIPOOL, IFWIBNN
FCT	IFWIPOOL
HRE	IFWIPOOL
ODLC LAN	IFWIPOOL
LDA	IFWIPOOL
LKE	IFWIPOOL
LLB	IFWIPOOL
LNB	IFWIPOOL
LND	IFWIPOOL
LTX	IFWIPOOL
LUB	IFWIPOOL
LUX	IFWIPOOL
NIB	IFWIPOOL
NIX	IFWIPOOL
NLB	IFWIPOOL
NLX	IFWIPOOL
NNT	IFWIPOOL
NQE	IFWIPOOL
NQX	IFWIPOOL
NRE	IFWIPOOL
NSB	IFWIPOOL
NSC	IFWIPOOL
NSX	IFWIPOOL
NVT	IFWIPOOL
RVT	IFWIPOOL

Table 15 (Page 2 of 2). CLISTs for Locating GPAs, Chains, and Pointers

GPA, Chain, or Pointer	CLIST
SCE	IFWIPOOL
SRE	IFWIPOOL
SSB	IFWIPOOL
TRT	IFWIPOOL
TGB	IFWIPOOL
VAT	IFWIPOOL
VTS	IFWIPOOL
VVT	IFWIPOOL
Buffer in use pointer	IFWIBUSE
CAB pointers	IFWICA
CER pointers	IFWICA

Specific Functions or Requests

Table 16 shows the SSP CLISTs you can use to obtain information about a specific function or request, such as an abend or a trace.

Table 16. CLISTs for Locating Specific Functions

Function or Request	CLIST
All control blocks	IFWIPATH
Load map	IFWIMAP
Module address	IFWIMOD
NPSI	IFWISSNP, IFWISNAU
Register contents	IFWIREGS
Save areas	IFWISAVE
Slowdown information	IFWISLOW
Traces	IFWITRAC

Chapter 12. Using NDF Diagnostic Aids

This chapter describes the diagnostic aids that are available with the NCP/EP definition facility (NDF), which is part of SSP. This chapter also describes the operation of NDF under MVS, VM, and VSE.

Note: To run NDF under VM, you must be in the CMS environment.

The NDF diagnostic aids consist of three program-controlled diagnostic aids:

- NDF messages
- Procedure tracebacks
- Storage dumps.

NDF also includes user-controlled diagnostic aids, which are invoked using the OPTIONS definition statement:

- Procedure traces
- Parameter traces
- Data traces
- Data printing
- Global traces (MVS and VM).

The examples of NDF output are extracted from the NDF generation definition report.

Program-Controlled Diagnostic Aids

NDF produces diagnostic information automatically whenever there is an abnormal condition during program execution. The following sections discuss the sources of this information.

NDF Messages

Each NDF execution produces a generation definition report that presents the system definition input information, together with messages, parameter default/inheritance information, and error summary information.

All NDF message numbers begin with ICN. You can locate messages easily by searching your generation definition messages for this string.

Each error message in the generation definition report is followed immediately by a two-digit severity level (see Figure 34 on page 303). See *NCP, SSP, and EP Messages and Codes* for an interpretation of the messages.

The severity codes, together with user responses, are as follows:

00—User informational. NDF generates user informational messages (severity 0) to alert you to conditions that may require your attention. Most informational messages tell you that NDF changed, ignored, deleted, or added a keyword. The condition is not serious enough to stop the generation definition process, but you should read the message and determine whether you want to accept the change made by NDF or make your own change to your generation definition.

Other informational messages tell you what calculations NDF performed.

04—User warning. NDF generates user warning messages for errors found when processing the generation definition. Severity-04 messages cause NDF to terminate table source generation. NDF assumes a value for the keyword that is in error and continues generation definition validation. NDF uses the assumed keyword value in later validation processing. However, you must correct the error in your generation definition and run it again.

08—User error. NDF generates user error messages when NDF encounters an unrecoverable error in the generation definition. Examples of user errors include unrecognizable lines in the generation definition, and required keywords that are coded with improper values when NDF cannot find an appropriate default value. User errors terminate NDF table source generation. NDF continues to validate the remainder of the generation definition. You must correct the error in your generation definition and run it again.

10—User error. NDF generates level 10 user errors when NDF can no longer perform significant functions. These errors usually mean insufficient file space or insufficient virtual memory. Most level 10 errors are recoverable user errors and are not related to the generation definition. NDF terminates generation immediately with an error message. No dump is provided. You must correct the parameter identified in the message and resubmit the generation.

12—Severe NDF error. NDF generates severe NDF error messages when it detects an internal problem. See *NCP, SSP, and EP Messages and Codes* for help in interpreting the message.

16—Fatal system error. A fatal system error message shows that NDF cannot perform any further useful processing. Level 16 errors are typically generated when NDF traps an abend situation. You should take the same action as for a level 12 message.

Figure 34 on page 303 is an example of a severity-04 code, and the message that was issued with it.

```
SSP VxRx  12/11/91 10:06:32  DEFINITION SPECIFICATION     PAGE 9

 LINE #                STATEMENT

    203  LN32711  LINE  ADDRESS=008,                          *5
    204                 SPEED=2400,                           *
    205                 CLOCKNG=WRONG,                        *
    206                 CODE=EBCDIC,                          *
    207                 POLLED=YES,                           *
    208                 SESSION=6,                            *
    209                 SERVPRI=OLD,                          *
    210                 PAUSE=255,                            *
    211                 NEGPOLP=5,                            *
    212                 POLIMIT=(255,QUEUE),                  *
    213                 RETRIES=(7,4,3)
                      G             TYPE=NCP
                       * * * NCP * * *
 *WARNING*  ICN001I  04  CLOCKNG=WRONG INVALID, EXT IS ASSUMED
                              FOR STATEMENT KEYWORD VALIDATION
                      D             CLOCKNG=EXT
                      D             DUPLEX=HALF
                      D             LPDATS=NO
                      D             DATRATE=LOW
                      D             SPDSEL=NO
                      D             ETRATIO=30
                      D             CHNLZ=NO
                      D             SERVLIM=HALF THE NUMBER OF
                                            ENTRIES IN THE SOT
                      D             DIALALT=NONE
                      D             TRANSFR=6
                      D             CUTOFF=NO
                      D             AVGPB=212
```

Figure 34. Sample NDF Error Message

Procedure Tracebacks

NDF contains logic that can detect internal program errors. Internal or system errors that generate a severity level 12 or level 16 error message produce procedure tracebacks in the generation definition report. A procedure traceback gives the routine name, the entry point for the routine, and, if possible, the current location counter within that routine for each procedure active at the time NDF detected the error.

Figure 35 on page 304 shows the first 5 characters of the procedure (entry) name identifying the subcomponent involved. Figure 36 on page 305 presents a sample procedure traceback that NDF produced. This traceback shows the names of the procedures that were active at the time of the error.

```
ICNCR:  Cross reference
ICNCV:  Consistency and validity checking
ICNER:  Error processor
ICNIO:  Input/output
ICNIP:  Input processor
ICNLE:  Link edit
ICNMN:  Main processor
ICNND:  New generation definition utilities
ICNOB:  Object generation
ICNOT:  Options processor
ICNRP:  Report generation
ICNSM:  String manipulation
ICNST:  Storage manager
ICNSY:  Symbol table
ICNTC:  Type conversion
ICNUS:  Usergen utilities
ICNUT:  Operating system utilities
ICNxx:  NCP statement/keyword validation
ICNAL:  Automatic line generation utilities
```

Figure 35. Subcomponent Prefixes

Note: If procedures occur in the traceback with subcomponent codes other than those listed, they refer to NCP statement keyword processing procedures and are included under the ICN*xx* subcomponent.

Once you identify the subcomponents related to the error, you can use the traces available through the OPTIONS statement to gather additional information. See "Procedure Traces" on page 307 for a description of this process.

In Figure 36 on page 305, the procedure causing the traceback is ICNIORDP. The two following procedures, ICNERPTX and ICNERPBX, are error-processing procedures that NDF invokes because of the error.

```
                    D             ER4(4)=5000
                    D             ER4(5)=5000
                    D             ER4(6)=20000
                    D             ER5(3)=5000
                    D             ER5(4)=5000
                    D             ER5(5)=5000
                    D             ER5(6)=20000
                    D             ER6(3)=5000
                    D             ER6(4)=5000
                    D             ER6(5)=5000
                    D             ER6(6)=20000
                    D             ER7(3)=5000
                    D             ER7(4)=5000
                    D             ER7(5)=5000
                    D             ER7(6)=20000
  558  *-------------------------------------------------------------------* NTO02220
  559  *          G E N E N D    D E L I M I T E R                         * NTO02230
  560  *-------------------------------------------------------------------* NTO02240
  561  *                                                                   * NTO02250
  562               GENEND  INIT=(CXNNINI),                                 XO02260
  563                       INCINIT=(CXNMINCI),                             XNTO02280
  564                       ORDINIT=(CXNMORDI),                             XNTO02280
  565                       INCHI=(CXNMINC),                                *
  566                       ORDHI=(CXNMORD),                                *
  567                       INCL2LO=(LOW2C),                                XNTO02310
  568                       ORDL2LO=LOW2D,                                  XNTO02310
  569                       KEY0INC=(LOW2E),                                XNTO02310
  570                       KEY0ORD=LOW2F,                                  XNTO02310
  571                       INCLO=LOW2G,                                    XNTO02310
  572                       ORDLO=LOW2H,                                    XNTO02310
  573                       SRCLO=(LOW2Y),                                  XNTO02310
  574                       SRCHI=(NTOLIB)                                  XNTO02310
                         D              BUILD.TRANSFR=9
                         D              TMRTICK=()
                         D              INCL2HI=()
                         D              ORDL2HI=()
*ERROR*    ICN621I  08  ICNIOGET: I/O ERROR ACCESSING FILE SYSLIB          MEMBER CXNMORDI
*SEVERE*   ICN624I  12  ICNIORDP: ERROR IN GET FOR READ PDS MEMBER SYSLIB(CXNMORDI)-FILE CLOSED
* PROCEDURE TRACEBACK *
  ENTRY NAME    ENTRY LOC    OFFSET       SAVE AREA
  ICNRTNDP      00020000     00000108     000204C0
  ICNMNMAN      00020B08     000000EE     00020CF4
  ICNIPMAN      0003ECA8     000000A6     0003EE10
  ICNIPDSP      00038770     000003D6     00038D60
  ICN05EPI      0014C838     000001D4     0014CBD0
  ICNS4N5E      00175AC0     00001EBA     00178728
  ICNXNGDL      00190088     00000236     00190354
  ICNIORDP      00036F18     000001F8     00037260
  ICNERPTX      0002A0A8     0000026E     0002A3C0
  ICNERPBX      00026A80     00000394     00026EC8
   575           END                                                    NTO02320
```

Figure 36. Sample NDF Procedure Traceback

Storage Dumps

A standard storage dump is produced when NDF traps an abend condition.

MVS: If there is an abend, invoke a storage dump with an ABEND job control language (JCL) statement. You must also code a DD statement defining a dump data set. The name of the DD statement must be either SYSABEND, SYSMDUMP, or SYSUDUMP.

VM: In CMS, control is returned to you when the abend occurs. If necessary, you can then invoke a manual storage dump.

VSE: NDF does not detect abends. The standard system response to an abend will be taken.

For additional information, consult the system control manual for your operating system.

User-Controlled Diagnostic Aids

If a system error occurs, NDF produces an error message with severity level 12 or 16, and a procedure traceback in the NDF generation definition report. Also, NDF may print an interrupt code (see "Procedure Tracebacks" on page 303). Report these errors to IBM along with diagnostic information gathered with the user-controlled diagnostic aids described here.

System errors identify the NDF subcomponents active at the time of the error. Use this information as a guide in selecting the appropriate debugging options. The procedure traceback prints 8-character procedure names, as shown in Figure 36 on page 305. The first five of these characters identify the subcomponent involved. This subcomponent is one of those defined in "Procedure Tracebacks" on page 303.

Also, the error message printed in the generation definition report will be associated with one of the subcomponents shown in Figure 35 on page 304. Adding the OPTIONS definition statement to your generation definition causes NDF to print useful debugging information in the generation definition report. This process is described in the following sections.

OPTIONS Definition Statement

Use the OPTIONS definition statement to cause NDF to print debugging information in its generation definition report. The output you request with the OPTIONS definition statement appears in the generation definition report interspersed with normal output. You can code keywords on the OPTIONS definition statement to specify which debugging information you want. TRPROC, TRPARM, and TRDATA activate debugging trace information or print specific data structures. NOTRPROC, NOTRPARM, and NOTRDATA terminate the specified traces. TRSNAP provides a one-shot dump of key data structures of a selected component. TRGLOB activates a trace for specified global variables. (TRGLOB must be used in conjunction with TRPROC.) NOTRGLOB terminates tracing of specified global variables.

The debugging process is as follows:

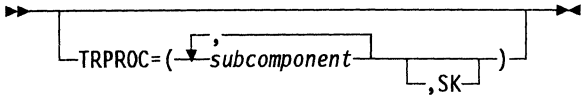
1. If the errors are of severity level 12 or 16, refer to *NCP, SSP, and EP Messages and Codes*, which provides an interpretation of the message, identifies the associated subcomponent, and shows which diagnostics should be run.
2. Using the information given in *NCP, SSP, and EP Messages and Codes*, determine the appropriate programmer action. See specific descriptions of keywords below for explanations of parameters allowed on each keyword.
3. Re-execute NDF. Debugging information appears in the generation definition report.

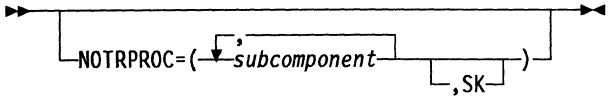
The debugging output appears in readable form. For tracing options, the debugging output lists the routine name and whether the routine is being entered or exited. For data printing options, the debugging output lists the data name, any subscript, and the data value converted to numeric, character, bit or pointer format as appropriate.

The following sections describe keywords and parameters on the OPTIONS definition statement. Code these keywords in any order in the generation definition.

Procedure Traces

The TRPROC and NOTRPROC keywords on the OPTIONS definition statement control procedure tracing within NDF. Specify TRPROC or NOTRPROC if you suspect flow control problems, or if your IBM support representative instructs you to run a procedure trace for diagnostic purposes.





Specifies the subcomponent or statement and keyword routines for which the procedure entry and exit trace is to be activated or deactivated.

subcomponent
Controls entry and exit tracing for all procedures whose names start with the given prefix. For example, if you specify TRPROC=(ICNSM,ICNSY), the entry and exit trace is activated for all modules in the SM and SY subcomponents. If you specify NOTRPROC=(ICNSM,ICNSY), the entry and exit trace is deactivated for all modules in the SM and SY subcomponents. See Figure 35 on page 304 for a list of valid subcomponent values.

SK
Controls entry and exit tracing for NDF statement and keyword routines.

Figure 37 on page 308 identifies the flow of control into and out of each module in the designated subcomponent. Use indentation levels, + and –, in the output to show the calling hierarchy between modules. This example shows only the trace output lines, rather than the full report.

Note: Tracing continues after the NOTRPROC statement is printed. NDF continues tracing until it has processed the statement.

```
Input:

*************************************************************************
*************************************************************************
         OPTIONS TRPROC=ICNIP
M10      HOST  INBFRS=10,          NCP BUFFERS ALLOCATION             X
               MAXBFRU=25,         UP TO 25 VTAM BUFFERS SHIPPED      X
               UNITSZ=152,         VTAM IO BUFFERS SIZE               X
               BFRPAD=0,           BUFFER PAD (MANDATORY FOR ACF)     X
               SUBAREA=(10)        CHANNEL ATTACHED HOSTSA
         OPTIONS NOTRPROC=ICNIP



OUTPUT:
       45  ************************************************************
       46  ************************************************************
       47           OPTIONS TRPROC=ICNIP
 ++ENTERING ICNIPGKI
 ++++ENTERING ICNIPFND
 ----EXITING ICNIPFND
 --EXITING ICNIPGKI
 ++ENTERING ICNIPGKI
 ++++ENTERING ICNIPFND
 ----EXITING ICNIPFND
 --EXITING ICNIPGKI
 ++ENTERING ICNIPGKI
 ++++ENTERING ICNIPFND
 ----EXITING ICNIPFND
 --EXITING ICNIPGKI
 ++ENTERING ICNIPGKI
 ++++ENTERING ICNIPFND
 ----EXITING ICNIPFND
 --EXITING ICNIPGKI
 ++ENTERING ICNIPGKI
       |       |
       |       |
       |       |
       |       |
       |       |
 ++++ENTERING ICNIPGKI
 ++++++ENTERING ICNIPFND
 ------EXITING ICNIPFND
 ----EXITING ICNIPGKI
 --EXITING ICNIPDSP
 ++ENTERING ICNIPPRS
 ++++ENTERING ICNIPGNT
 ++++++ENTERING ICNIPGCD
     53           OPTIONS NOTRPROC=ICNIP
 ------EXITING ICNIPGCD
 ----EXITING ICNIPGNT
 ++++ENTERING ICNIPGNT
 ----EXITING ICNIPGNT
 ++++ENTERING ICNIPPKV
```

Figure 37. NDF Procedure Trace Example

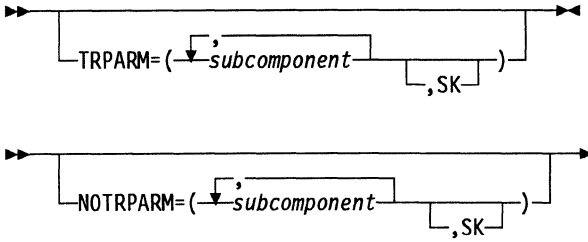
Figure 38 lists modules that are not traced because of recursion.

ICNERCST	ICNRPMSX	ICNRTDTC
ICNERSPI	ICNRPPAG	ICNRTNDP
ICNERSPX	ICNRPPBT	ICNRTPCL
ICNERSTA	ICNRPPCH	ICNRTPOP
ICNIOINI	ICNRPPCX	ICNRTPPR
ICNIOPCL	ICNRPPFX	ICNRTSUM
ICNIOPOP	ICNRPPHX	ICNSMALX
ICNIOPPR	ICNRPPLN	ICNSMPLX
ICNIOSYN	ICNRPPNM	ICNTCGET
ICNMNCLS	ICNRPPRM	ICNTCPUT
ICNMNINI	ICNRPTIM	ICNTCPUX
ICNMNMAN	ICNRPTIT	ICNUTABD
ICNRPFMT	ICNRPTRC	ICNUTDMP
ICNRPINI	ICNRTAUX	
ICNRPMSG	ICNRTDEV	

Figure 38. Modules not Traced by Procedure and Parameter Traces

Parameter Traces

The TRPARM and NOTRPARM keywords on the OPTIONS definition statement control parameter tracing within NDF. Specify TRPARM or NOTRPARM if your IBM support representative instructs you to run a parameter trace for diagnostic purposes.



Specifies the subcomponent or statement and keyword routines for which the I/O parameter trace is activated or deactivated.

subcomponent
Controls I/O parameter tracing for all procedures with names beginning with the given prefix. For example, if you specify TRPARM=(ICNSM,ICNSY), the I/O trace is activated for all modules in the SM and SY subcomponents. If you specify NOTRPARM=(ICNSM,ICNSY), the I/O trace is deactivated for all modules in the SM and SY subcomponents. See Figure 35 on page 304 for a list of valid subcomponent values.

SK
Controls I/O parameter tracing for NDF statement and keyword routines.

Figure 38 lists the modules that TRPARM does not trace.

Figure 39 shows the NDF parameter trace. This example shows only the trace output lines, rather than the full report.

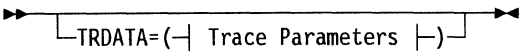
Note: Tracing continues after the NOTRPARM statement is printed. NDF continues tracing until it processes the statement.

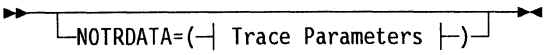
```
   34           OPTIONS TRPARM=SK
DISPATCHING KEYWORD=NOTRPARM%
STATUS='80010000'X
STMT NAME=OPTIONS%
KEYWORD VALUE=%
VALUE LENGTH=0
SUBCOUNT=0
XVT LENGTH=34
DISPATCHING KEYWORD=TRDATA%
STATUS='80010000'X
      |              |
      |              |
      |              |
      |              |
      |              |
      |              |
      |              |
   36           OPTIONS NOTRPARM=SK
DISPATCHING KEYWORD=#SYMBOL%
STATUS='80010000'X
STMT NAME=OPTIONS%
KEYWORD VALUE=%
VALUE LENGTH=0
SUBCOUNT=0
XVT LENGTH=34
      |              |
      |              |
      |              |
      |              |
      |              |
      |              |
      |              |
      |              |
      |              |
   35  STMT3    HOST  BFRPAD=28,INBFRS=3,MAXBFRU=16,SUBAREA=1,UNITSZ=84
DISPATCHING=PROLOG%
STATUS='80010000'X
STMT NAME=HOST%
XVT SIZE=34
VERSION & RELEASE=V3  %
STATUS='80010000'X
MAC=HOST%
```

Figure 39. NDF Parameter Trace Example

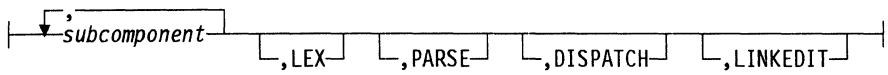
Data Traces

The TRDATA and NOTRDATA keywords on the OPTIONS definition statement control the tracing of data structures within NDF. Specify TRDATA or NOTRDATA if your IBM support representative instructs you to run a data trace for diagnostic purposes.





Trace Parameters:



Specifies the subcomponent or data areas for which the data trace is activated or deactivated.

subcomponent
Controls data tracing for all procedures with names beginning with the given prefix. For example, if you specify TRDATA=(ICNIO,ICNOB), the data trace is activated for all modules in the IO and OB subcomponents. If you specify NOTRDATA=(ICNIO,ICNOB), the data trace is deactivated for all modules in the IO and OB subcomponents. The valid subcomponent values are the following:

- ICNIO
- ICNIP
- ICNLE
- ICNOB
- ICNOT
- ICNST
- ICNUT.

LEX
Enables or disables the printing of each lexical token, length, and type as soon as it is known.

PARSE
Enables or disables the printing of the parsed representation for each definition statement as soon as it is known.

DISPATCH
Enables or disables the printing of an identifying message for each routine in the keyword vector table (KVT) that is called.

LINKEDIT
Enables or disables tracing of the generation of the linkage editor control cards.

Figure 40 shows the NDF data trace. The output of this trace varies with the subcomponent or data area identified. This example shows only the trace output lines, rather than the full report.

Note that tracing continues after the NOTRDATA statement has been printed. NDF continues tracing until it has processed the statement.

Input:

```
         OPTIONS TRDATA=LEX
M12      HOST  INBFRS=10,          NCP BUFFERS ALLOCATION            X
               BFRPAD=0,          BUFFER PAD (MANDATORY FOR ACF)    X
               MAXBFRU=30,        UP TO 30 VTAM BUFFERS SHIPPED     X
               SUBAREA=(12),      CHANNEL ATTACHED HOSTSA           X
               UNITSZ=132         VTAM IO BUFFERS SIZE FOR TPNS
         OPTIONS NOTRDATA=LEX
*
```

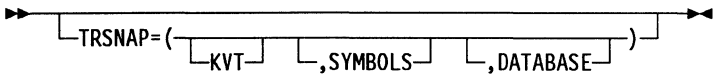
Output:

```
   62  *
   63           OPTIONS TRDATA=LEX
   64  M12      HOST  INBFRS=10,          NCP BUFFERS  ALLOCATION          X
  OUT_TYPE=2
  OUT_SPELLING=M12%
  OUT_LENGTH=4
  OUT_TYPE=1
  OUT_SPELLING=HOST%
  OUT_LENGTH=5
  OUT_TYPE=1
  OUT_SPELLING=INBFRS%
  OUT_LENGTH=7
  OUT_TYPE=3
  OUT_SPELLING==%
  OUT_LENGTH=2
  OUT_TYPE=1
  OUT_SPELLING=10%
  OUT_LENGTH=3
  OUT_TYPE=4
  OUT_SPELLING=,%
  OUT_LENGTH=2
   65                BFRPAD=0,           BUFFER PAD (MANDATORY FOR ACF)    X
  OUT_TYPE=1
  OUT_SPELLING=BFRPAD%
  OUT_LENGTH=7
  OUT_TYPE=3
  OUT_SPELLING==%
      |        |
      |        |
  OUT_TYPE=1
  OUT_SPELLING=132%
  OUT_LENGTH=4
  OUT_TYPE=7
  OUT_SPELLING=%
  OUT_LENGTH=1
                    D              TIMEOUT=420.0
                    D              DELAY=0
   69           OPTIONS NOTRDATA=LEX
  OUT_TYPE=1
  OUT_SPELLING=OPTIONS%
      |        |
      |        |
```

Figure 40. NDF Data Trace Example

Data Printing

Dump major data structures within NDF using the TRSNAP keyword on the OPTIONS definition statement.



Specifies which data structures NDF is to print in a readable format.

KVT
Specifies that NDF is to print all keyword vector tables (KVTs).

SYMBOLS
Specifies that NDF is to print the symbol table.

DATABASE
Specifies that NDF is to print the storage manager control structures and data sets.

Figure 41 is an example of the NDF data printing. This example shows only the trace output lines, rather than the full report.

Input:

```
*
         OPTIONS TRSNAP=SYMBOLS
P14042   PU    MAXOUT=7,           UP TO 7 PIUS BEFORE REQUEST RESPONSEX
               PASSLIM=7,          UP TO 7 PIUS CAN BE SENT AT ONCE    X
               PUTYPE=4,           PHYSICAL UNIT IS A 37xx             X
               SUBAREA=19,         SUBAREA ADDRESS = 19                X
               TGN=5,              TRANSMISSION GROUP 5                X
               ISTATUS=INACTIVE    (V) VTAM
*
```

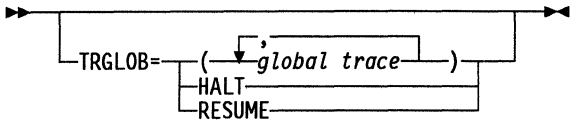
Output:

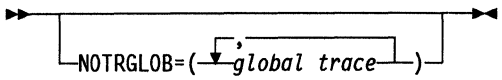
```
                    SYMBOL TABLE DUMP
                    ------ ----- ----

  SYMBOL TABLE RECORD 1
    SY_TABLE
      SY_NAME: BUILD
      SY_TYPE: 1
      SY_NAME_LINK: 0
      SY_TYPE_LINK: 2
    SY_STMT
       |       |
       |       |
       |       |
       |       |
       |       |
  SYMBOL TABLE RECORD 6
    SY_TABLE
      SY_NAME: OPTIONS
      SY_TYPE: 1
      SY_NAME_LINK: 0
      SY_TYPE_LINK: 7
    SY_STMT
      SY_ST_KVT_PTR: 0014CD90
      SY_ST_RESERVED: 0
```

Figure 41. NDF Data Printing Example

Global Traces (MVS and VM)

The TRGLOB and NOTRGLOB keywords on the OPTIONS definition statement control global tracing within NDF. Specify TRGLOB or NOTRGLOB if your IBM support representative instructs you to run a global trace for diagnostic purposes.





Specifies the global variables for which the global trace is to be activated or deactivated.

You may activate a trace for a maximum of 24 global traces at one time on one or more OPTIONS definition statements. TRGLOB must be coded in conjunction with TRPROC to activate the trace activity.

Code TRGLOB=HALT or TRGLOB=RESUME to halt or resume the printing of trace data at any time.

Note: When specifying an array name for globals, braces {} must be used.

Figure 42 is an example of the NDF global trace option.

Input:

```
       OPTIONS TRPROC=SK,TRGLOB=SISFTRC{603}
GENV5R3 BUILD VERSION=V5R3,TYPSYS=MVS,                          *
       |      |
       |      |
       |      |
       OPTIONS NOTRGLOB=SISFTRC{603}
```

Output:

```
    19          OPTIONS TRPROC=SK,TRGLOB=SISFTRC{603}
       |      |
       |      |
       |      |
++ENTERING ICNN1VER

   SISFTRC{603}=%

--EXITING  ICNN1VER

 SISFTRC{603}=V5R3%

++ENTERING ICN01LBL

   SISFTRC{603}=V5R3%

--EXITING  ICN01LBL

 SISFTRC{603}=V5R3%
       |      |
       |      |
       |      |
    51          OPTIONS NOTRGLOB=SISFTRC{603}
       |      |
       |      |
       |      |
++++ENTERING ICNX0SEQ

----EXITING  ICNX0SEQ

--EXITING  ICN11PRO

++ENTERING ICN11LBL

--EXITING  ICN11LBL
```

Figure 42. NDF Global Trace Option Example

Chapter 13. Using the Configuration Report Program

The configuration report program (CRP) is a utility program that creates three types of configuration reports: the Cable Selection Report (IBM 3725), the VTAM Network Configuration Report, and the NCP Configuration Report. These reports include information on network resources and resource attributes for a network with NCP, EP/PEP, or VTAM as well as a copy of the generation definition and the node cross-reference list.

The content of each report is as follows:

- Cable Selection Report (IBM 3725). This report prints an entry for every line statement coded in the generation definition. The report lists the line name, the line interface card (LIC) type, the line address, and the cable group number.
- VTAM Network Configuration Report. This report prints resource names, generation definition statements, line addresses, and type (SNA or non-SNA) for VTAM network resources.
- NCP Configuration Report. This report prints resource names, generation definition statements, various keyword values, and partial or full-line comments for NCP or EP/PEP network resources.

To use CRP, you must first enter CRP utility control statements in your generation definition. These control statements allow you to specify which network resources are included in the configuration report (NCP, EP/PEP, or VTAM), the type of configuration report you wish to view (NCP, VTAM, or Cable Selection), and whatever resource attributes you want omitted from the report (such as line information). These control statements also let you specify the number of lines to print on each page of the report and whether you will include partial or full-line comments.

To invoke CRP to process this network resource and generation definition information, you code specified job control language (JCL) statements for MVS or VSE, or file definitions (FILEDEFs) for VM. Since CRP does not check the generation definition for completeness, it is recommended that you verify the validity of the generation definition you are using before running CRP.

Note: Code NEWDEFN=YES on the OPTIONS definition statement if your NCP generation definition has one or more of the following conditions:

- Contains NTRI, frame-relay, or Internet resources
- Uses NDF standard attachment facility (SAF)
- Has the AUTOLINE keyword coded on the LINE definition statement.

Use the output from the NCP generation, found in the file specified by the NEWDEFN ddname, as input to CRP.

After processing and formatting the input, CRP moves the utility control statement and keyword information to direct-access files SYSUT1 and SYSUT2. CRP places the reports, a copy of the generation definition, and any diagnostic messages on a sequential output data set (SYSPRINT) and prints reports when requested. CRP also prints a cross-reference table when you request VTAM, NCP, EP, or PEP reports.

Note: You must use the IBM sort/merge program, or its equivalent, to run CRP. The CRP interface to the sort/merge program is as follows:

MVS: SORT FIELDS=(1,8,CH,A,12,5,CH,A) (cross reference)
RECORD TYPE=F,LENGTH=(133)
SORT FIELDS=(21,4,BI,A) (cable report)
RECORD TYPE=F,LENGTH=(133)

VM: The necessary SORT routines are provided.

VSE: SORT FIELDS=(1,8,CH,A,12,5,CH,A),WORK=0 (cross reference)
SORT FIELDS=(21,4,BI,A),WORK=0 (cable report)

This chapter discusses the following information about CRP:

- CRP features
- The JCL (for MVS or VSE) or FILEDEF (for VM) coding needed to run CRP
- The meaning and format of the four utility control statements entered in your generation definition
- The descriptions and examples of CRP output: generation definition, Cable Selection Report (IBM 3725), VTAM Network Configuration Report, NCP Configuration Report, and node cross-reference list.

CRP Features

The following lists some of the features of the configuration report program:

- The listing header contains a statement that the USGTIER keyword is placed after the ERLIMIT keyword on the BUILD definition statement.
- Adds "ENET" in the LINE CNTL column for a logical or physical Ethernet-type subsystem (ESS) line.
- Adds "NTRI" in the LINE CNTL column for a logical or physical NTRI line.
- Adds "FRLY" in the LINE CNTL column for 3745 frame-relay lines.
- For LU definition statements ignored by NDF because GENILU=NO is specified on the BUILD definition statement:
  - Displays blanks in the ELMT ADDR column
  - Displays the word "IGNORED" in the COMMENTS/NOTES column.
- Adds the PHYS RES REFERENCE column to the VTAM Network Configuration Report and moves the CA address to precede the physical unit type.
- Adds the following information to the list of SNA devices in the NCP Configuration Report:
  - All lines attached to the 3746 Model 900
  - Whether these lines are attached to an ESCON processor (ESCP) or a token-ring processor (TRP).
- Add information to the VTAM Network Configuration Report to identify each line as either a physical or logical line. Identify the physical resource with which the logical line is associated.
- Includes 3746 Model 900-attached SDLC, frame-relay, and token-ring lines in the NCP Configuration Report.

Running CRP under MVS

A sample procedure for running CRP under MVS is included on your licensed program tape. The data set name of the sample, found in the ASSPSAMP library on the tape, is CRPJCL. This procedure is provided to help you create and tailor the JCL in your MVS environment.

To run CRP under MVS, provide the following JCL:

//jobname	JOB	Initiates the job.
//	EXEC	Specifies the program PGM=IFLCRP, or the name of a procedure that contains the job control statements.
//SYSPRINT	DD	Defines a sequential data set to be sent to the SYSOUT device.
//SYSUT1	DD	Defines a DASD data set to be used as intermediate storage for the NCP Configuration Report.
//SYSUT2	DD	Defines a DASD data set to be used as intermediate storage for the VTAM Network Configuration Report.
//SORTIN	DD	Defines the DASD data set to be used as input to the MVS sort routine.
//SORTOUT	DD	Defines the DASD data set to be used as output from the MVS sort routine.
//SORTLIB	DD	Specifies the data set that contains the CRP sort routine.
//SORTWK01	DD	Defines the working data set to be used by the sort routine.
//SYSOUT	DD	Defines the SORT/MERGE message data set. this is required by the sort/merge program.
//SYSIN	DD	Specifies the data set that contains the CRP control statements and the generation definition statements.

The following is an example of the JCL needed to run CRP under MVS.

```
//CRP      JOB (account info),'name'
//CRP      PROC OUT='*',UNITNME=sysda,SSPLIB='sys1.ssplib',
//             SORTLIB='sys1.sort.sortlib',SORTWK='sortwk'
//*********************************************************************
//*********************************************************************
//**                                                                 **
//**     PROCEDURE:  CRP                                             **
//**                                                                 **
//**     FUNCTION:   RUN CONFIGURATION REPORT PROGRAM                **
//**                                                                 **
//**     NOTE:                                                       **
//**        CHANGE ALL LOWER CASE CHARACTERS TO VALUES               **
//**        SUITABLE FOR YOUR INSTALLATION.                          **
//**                                                                 **
//**     SYMBOLIC PARMS:                                             **
//**     OUT      :  SYSOUT CLASS                                    **
//**     UNITNME  :  UNITNAME FOR TEMPORARY DATA SETS                **
//**     SSPLIB   :  LIBRARY CONTAINING IFLCRP ROUTINE               **
//**     SORTLIB  :  LIBRARY CONTAINING MVS SORT ROUTINE             **
//**     SORTWK   :  UNIT NAME FOR SORT ROUTINE                      **
//**                                                                 **
//**     FOR MORE INFORMATION ABOUT THIS JCL SEE NCP/SSP/EP          **
//**     DIAGNOSIS GUIDE, FORM NUMBER LY43-0033                      **
//**                                                                 **
//**    ACTIVITY:                                                    **
//**    ---------------------------------------------------------    **
//**                                                                 **
//**    NONE                                                         **
//**                                                                 **
//*********************************************************************
//CRPRUN   EXEC  PGM=IFLCRP
//*********************************************************************
//**  LIBRARY CONTAINING IFLCRP ROUTINE                              **
//*********************************************************************
//STEPLIB  DD  DSN=&SSPLIB,DISP=SHR
//*********************************************************************
//**  DIAGNOSTIC OUTPUT                                              **
//*********************************************************************
//*SYSUDUMP DD  SYSOUT=&OUT
//*SYSABEND DD  SYSOUT=&OUT
//*********************************************************************
```

```
//*********************************************************************
//**  CRP REPORTS                                                    **
//*********************************************************************
//SYSPRINT DD  SYSOUT=&OUT
//*********************************************************************
//**  INTERNAL DATASETS USED BY CRP                                  **
//*********************************************************************
//SYSUT1   DD  DSN=&&SPOOL1,UNIT=&UNITNME,SPACE=(CYL,(10,5)),
//             DISP=(NEW,DELETE)
//SYSUT2   DD  DSN=&&SPOOL2,UNIT=&UNITNME,SPACE=(CYL,(10,5)),
//             DISP=(NEW,DELETE)
//*********************************************************************
//**  DATASETS USED FOR SORTING                                      **
//*********************************************************************
//SORTIN   DD  DSN=&&SPOOL5,UNIT=&UNITNME,SPACE=(CYL,(10,5)),
//             DISP=(NEW,DELETE)
//SORTOUT  DD  DSN=&&SPOOL6,UNIT=&UNITNME,SPACE=(CYL,(10,5)),
//             DISP=(NEW,DELETE)
//*********************************************************************
//**  LIBRARY CONTAINING MVS SORT ROUTINE                            **
//*********************************************************************
//SORTLIB  DD  DSN=&SORTLIB,DISP=SHR
//*********************************************************************
//**  WORKING DATASET USED BY SORT ROUTINE                           **
//*********************************************************************
//SORTWK01 DD  DSN=&&TEMP1,DISP=(NEW,DELETE),UNIT=&SORTWK,
//             SPACE=(CYL,(5,2),,CONTIG)
//*********************************************************************
//**  SORT/MERGE MESSAGE DATASET                                     **
//*********************************************************************
//SYSOUT   DD  SYSOUT=&OUT
//*********************************************************************
//PROCEND  PEND
//STEP1    EXEC CRP
//*********************************************************************
//**  GENERATION DEFINITION WITH CRP CONTROL STATEMENTS              **
//*********************************************************************
//SYSIN    DD  *
*REPORT=(NCP,VTAM)  --- this or similar CRP control statement is
                        required  (see NCP/SSP/EP Diagnosis Guide,
                        PUBLICATION # LY43-0033, FOR MORE DETAILS)


    generation definition goes here

/*
```

Note: Immediately after *REPORT=(NCP,VTAM), you insert the generation definition statements.

Running CRP under VM

A sample procedure for running CRP under VM is included on your licensed program tape. The file name of the sample is CRPVM SMPLEXEC. This procedure is provided to help you create and tailor the FILEDEFs in your VM environment.

To run CRP under VM, provide the following FILEDEFs:

SYSIN Defines a file containing the CRP control statements and generation definition statements.

SYSPRINT Defines a sequential file used to store CRP output.

SYSUT1 Defines a DASD file used as intermediate storage for the NCP Configuration Report.

SYSUT2 Defines a DASD file used as intermediate storage for the VTAM Network Configuration Report.

SORTIN Defines a temporary file used as input for sorting.

SORTOUT Defines a temporary file used as output for sorting.

The following are sample FILEDEFs:

```
FILEDEF SYSIN DISK SYSGEN DECK A (RECFM F LRECL 80
FILEDEF SYSPRINT DISK CRP OUTPUT A (RECFM F LRECL 133 DISP MOD
FILEDEF SYSUT1 DISK SYSUT1 DATASET A (RECFM F LRECL 154
FILEDEF SYSUT2 DISK SYSUT2 DATASET A (RECFM F LRECL 154
FILEDEF SORTIN DISK CRP$SIN TEMPCRP A (RECFM F LRECL 133
FILEDEF SORTOUT DISK CRP$SOT TEMPCRP A (RECFM F LRECL 133
```

After issuing the FILEDEFs, issue the command:

```
IFLCRP
```

Running CRP under VSE

To run CRP under VSE, provide the following JCL (the input records to CRP must be 80 bytes long):

```
// JOB       jobname                  Initiates the job.
// LIBDEF    OBJ,SEARCH=(SSPLIB.CRP)

// DLBL      SORTIN1                  Defines the DASD file to be
                                      used as input to the VSE
                                      sort routine.

// EXTENT    SYS002
// ASSGN     SYS002

// DLBL      SORTOUT                  Defines the DASD file to be
                                      used as output from the VSE
                                      sort routine.

// EXTENT    SYS001
// ASSGN     SYS001

// DLBL      SPOLODT                  Defines the DASD file to be
                                      used as intermediate storage for
                                      the NCP Configuration Report.

// EXTENT    SYS003
// ASSGN     SYS003

// DLBL      VTMSODT                  Defines the DASD file to be
                                      used as intermediate storage for
                                      the VTAM Network Configuration Report.

// EXEC                               Specifies the IFUCRP program or
                                      the name of the procedure that contains
                                      the JCL.
```

The following is an example of the JCL needed to run CRP under VSE:

```
// JOB IFUCRP
// LIBDEF OBJ,SEARCH=(SSPLIB.CRP)
// DLBL SORTIN1,'SORT.INPUT',0,SD
// EXTENT SYS002,XXXXXX,1,0,12,36
// ASSGN SYS002,351
// DLBL SORTOUT,'SORT.OUTPUT',0,SD
// EXTENT SYS001,XXXXXX,1,0,48,36
// ASSGN SYS001 ,351
// DLBL SPOLODT,'NCP.TEMP.REPORT',0,SD
// EXTENT SYS003,XXXXXX,1,0,84,36
// ASSGN SYS003,351
// DLBL VTMSODT,'VTAM.TEMP.REPORT',0,SD
// EXTENT SYS004,WK1SYS,1,0,120,36
// ASSGN SYS004,351
// EXEC IFUCRP
/*
/&
```

Note: Immediately after the // EXEC IFUCRP statement, you enter the generation definition containing the utility control statements.

CRP Utility Control Statements

CRP uses four utility control statements to invoke program options. To use these CRP control statements, add them to your generation definition. These control statements are:

```
*REPORT          To select the type of output report
*OPTION          To omit resources from the report
*LINECNT         To specify the number of lines per page
*/L and */C      To include comments within the report
```

Note: The * for these statements is always in column 1, except for the */C, which may be embedded within a SYSGEN statement.

*REPORT Control Statement

The *REPORT control statement lets you select the type of configuration report (NCP, VTAM, or Cable Selection) you want to process. Entering the report type designates which network resources (NCP, EP/ PEP, or VTAM) will be contained in the report. Selecting NCP generates a report for NCP, EP, and PEP network resources; selecting VTAM generates one for VTAM network resources; and selecting CABLE generates the cable specifications for the IBM 3725 line adapters.

The *REPORT control statement is required and must precede the first BUILD definition statement in the generation definition. The control statement format is:

```
*REPORT=(report name, report name, ...)
```

where *report name* represents the type of configuration report to be processed and printed. Valid parameters for this statement are NCP, VTAM, or CABLE.

You can specify the reports in any combination or order. Use a comma to delimit multiple values and enclose the values in parentheses:

```
*REPORT=(NCP,VTAM)
```

However, the reports always print in the order determined by your operating system.

*OPTION Control Statement

The *OPTION control statement specifies the resources to be omitted from the configuration report. This control statement only applies to NCP, EP, and PEP resources. The *OPTION control statement must appear before the first BUILD definition statement in the input data set. If you code the *OPTION control statement, it affects all NCPs coded in the definition, not just those following the statement.

The parameters for the *OPTION control statement are NCP generation definition statement names or NODECK, which inhibits the printing of the generation definition or specified generation definition statements. Any definition statement specified is omitted from the configuration report. The control statement format is:

```
*OPTION=(name,name,...)
```

where *name* is the NCP definition statement that is omitted from the configuration report. Delimit the definition statement names with a comma. Do not code blanks. If you specify only one parameter, do not code parentheses.

Note: To continue parameters on the *OPTION control statement, code a continuation character in column 72 and start the next parameter in column 16 on the continuation statement. Do not split a parameter between the *OPTION control statement and the continuation statement.

The following NCP definition statement names are valid parameters for the *OPTION control statement.

CLUSTER	LINE	NCPNAU	SERVICE
COMP	LU	PATH	TERMINAL
GROUP	LUDRPOOL	PU	
GWNAU	LUPOOL	PUDRPOOL	

For example, if you do not want the GROUP and SERVICE definition statements included in the configuration report, code the *OPTION control statement as follows:

```
*OPTION=(GROUP,SERVICE)
```

Code NODECK on the *OPTION control statement to inhibit the printing of the generation definition. For example:

```
*OPTION=NODECK
```

You can code NODECK with definition statement names to inhibit printing of the generation definition and the definition statements in the NCP report. For example:

```
*OPTION=(GROUP,NODECK,LU)
```

*LINECNT Control Statement

Use the *LINECNT control statement to specify the number of lines printed on each page in the generation definition listing, and for the VTAM, NCP, and CABLE reports. The format of the *LINECNT statement is:

```
*LINECNT=nnn
```

The value specified can be 1 to 999. The default value is 52.

The *LINECNT control statement does not apply to the printing of the cross-reference table.

*/L and */C Control Statements

Use the */L and */C control statements to insert comments into the configuration report. The */L control statement inserts full-line comments, while the */C is the partial-line comment control statement. You can insert these control statements, with their respective comment text, throughout the generation input. Because CRP ignores assembler comments, use the */L and */C control structures to distinguish areas of interest in the generation definition.

The */L control structure designates a CRP full-line comment. Begin the */L in column 1 of the generation definition followed by one or more spaces, and then comment text up to 68 characters long. CRP puts the prefix "===*/L===>" in front of the comment text to distinguish it from other CRP output. If CRP places the */L comment within the continuation of a generation statement, CRP prints the comment immediately preceding the generation statement. Otherwise, the comment appears in the CRP output as it appeared in the generation input.

```
*/L ********************************************************************
*/L * Building SNA devices                                              *
*/L ********************************************************************
```

The */C control statement shows a partial-line comment, which applies to a specific generation statement within the generation input definition. CRP places the partial-line comment under the Comments heading on that specific statement's output line in the configuration report. The */C must appear within a generation statement as follows:

```
LINE1           LINE ADDRESS=000, */C First line of generation def.   *
```

or

```
LINE1           LINE ADDRESS=000,                                     *
*/C First line of generation definition
```

If the */C comment is on the same line as the definition statement, as in the first example above, the */C comment must begin after column 16. You can also code the */C comment between two generation statements where the second generation statement is not a continuation of the first statement. The */C must be followed by

one or more spaces, and then the comment text. For either an SNA or a non-SNA device, the comment text may be 27 characters long. Except for a PATH definition statement, each statement is allowed only one partial-line comment. For the PATH definition statement, you can use up to eight partial-line comments. The actual number of comments printed is the number of ER keywords coded. If you code eight comments, but only five ER keywords, the first five comments are printed, and the last three comments are ignored.

CRP Output

Use the *REPORT control statement to request CRP output. The following output is available from CRP:

- Copy of the generation definition
- Cable Selection Report (IBM 3725)
- VTAM Network Configuration Report
- NCP Configuration Report
- Cross-reference table.

Generation Definition

The generation definition output produces a list of all input and any comment statements submitted to CRP. CRP automatically prints the list when the configuration report prints, unless you code NODECK on the *OPTION control statement. If you code NODECK, all CRP-generated messages except IFW300I are printed before the first specified report. The generation definition listing contains the page number, the report creation date, and page titles. Figure 43 is an example of part of a generation definition listing from a report.

```
DATE: 08/29/92          CONFIGURATION REPORT PROGRAM                PAGE     1

*REPORT=(NCP,VTAM)
         OPTIONS NEWDEFN=(YES,PACK),USERGEN=(CXNNTO,X25NPSI,CXRNRF)
*      OPTIONS NEWDEFN=YES,USERGEN=(CXNNTO,X25NPSI,CXRNRF,FNMNDFGN)     00000300
AH1      PCCU AUTODMP=NO,AUTOIPL=NO,AUTOSYN=YES,DUMPDS=VTAMDUMP,MAXDATA*
               =4096,SUBAREA=1,VFYLM=YES,NETID=NETA,GWCTL=ONLY
*                                                                        00001400
AH2      PCCU AUTODMP=NO,AUTOIPL=NO,AUTOSYN=YES,DUMPDS=VTAMDUMP,MAXDATA*
               =4096,SUBAREA=2,VFYLM=YES
*                                                                        00002400
AH10     PCCU AUTODMP=NO,AUTOIPL=NO,AUTOSYN=YES,DUMPDS=VTAMDUMP,MAXDATA*
               =4096,SUBAREA=10,NETID=NETA,GWCTL=ONLY
*                                                                        00003300
```

Figure 43 (Part 1 of 2). Example of a CRP Section in a Generation Definition

```
NCP431   BUILD ADDSESS=200,AUXADDR=200,X25.MAXPIU=64K,X25.MCHCNT=4,X25.*
               SNAP=YES,X25.PREFIX=X,X25.MWINDOW=7,MEMSIZE=2048,       *
               SUBAREA=4,SALIMIT=255,SESSACC=(YES,ALL,10,200,100,10),  *
               ERLIMIT=8,TYPGEN=PEP,BACKUP=5,BRANCH=200,BFRS=124,CA=(  *
               TYPE5-TPS,TYPE5-TPS,TYPE5-TPS),CANETID=NETA,CATRACE=(YES*
               ,255),CSMHDR=27F5C8,CSMSG=C3D9C9E3E2C9E340D4C5E2E2C1C7C5*
               40C6D9D6D440C1C5D5E5F4D9F1,DELAY=(0.2),DSABLTO=6.5,DYNAD*
               MP=(YES,2F),ENABLTO=6.5,HICHAN=(3F,3F),HSBPOOL=100,LOADL*
               IB=NCPLOAD,LOCHAN=(20,20),MAXSSCP=4,MXRLINE=2,MXVLINE=6,*
               NAMTAB=120,MAXSESS=250,NCPCA=(ACTIVE,ACTIVE,ACTIVE),NPA=*
               YES,MODEL=3725,NUMHSAS=4,PRTGEN=GEN,SLODOWN=12,         *
               TIMEOUT=(180),TRACE=(YES,256),NEWNAME=NCP431,           *
               TWXID=(E8D6E4C3C1D3D311,C2C9C7D5C3D7C3C1D3D325),        *
               TYPSYS=VM,VERSION=V5R4,NETID=NETA,                      *
               VRPOOL=2
*                                                                      00006700
         SYSCNTRL OPTIONS=(BACKUP,BHSASSC,DLRID,DVSINIT,LNSTAT,MODE,NAK*
               LIM,RCNTRL,RCOND,RDEVQ,RECMD,RIMM,SESINIT,SESSION,SSPAUS*
               E,STORDSP,XMTLMT,ENDCALL)
*
NTONCP   NCPNAU NOTIFY=1,NTO.TRACEML=YES,NTO.TRCTABL=2000,VIROWNER=CXNN*
               TO,TYPE=SSCP,NAUCB=NTOSSCP,NAUFVT=CXNFVTN
*
         GWNAU NAME=T1M,NETID=NETT,NUMSESS=3
*                                                                      00007400
         GWNAU NUMADDR=50
*                                                                      00007600
         HOST BFRPAD=(0),INBFRS=3,MAXBFRU=24,SUBAREA=(1),UNITSZ=172
*
         HOST BFRPAD=(0),INBFRS=3,MAXBFRU=24,SUBAREA=(2),UNITSZ=172
*
         HOST BFRPAD=(35),INBFRS=3,MAXBFRU=24,SUBAREA=(3),UNITSZ=180
*
         HOST BFRPAD=(0),INBFRS=3,MAXBFRU=24,SUBAREA=(10),UNITSZ=172
*                                                                      00008900
         PATH DESTSA=1,ER0=(1,1),ER1=(1,1),ER2=(1,1),ER3=(2,1),ER4=(2,1*
```

Figure 43 (Part 2 of 2). Example of a CRP Section in a Generation Definition

Cable Selection Report (IBM 3725)

To use the Cable Selection Report for the cabling of the IBM 3725 Communication Controller, specify the CABLE parameter on the *REPORT control statement. Specify the LIC keyword on the LINE definition statement to make the cable selection. Only CRP uses the LIC keyword. NDF ignores it. Code the appropriate value in the generation definition for each line as defined by the following table. Table 17 lists the proper names of telephone services and facilities by LIC type.

Table 17. Telephone Services and Facilities by LIC Type

LIC=1	LIC=2	LIC=3	LIC=4
V.25	WIDEBAND 8751	V.35 DCE	X.21 DCE
RS366	WIDEBAND 8801	V.35 DIRECT	X.21 DIRECT
AUTOCALL	WIDEBAND 8803 303		
RS232C			
V.24 Direct			
X.21 Bis			

CRP prints the Cable Selection Report (IBM 3725) when you code CABLE on the *REPORT statement. CRP prints an entry for every LINE definition statement in the generation definition in hexadecimal numerical order by line address. If the LIC keyword is valid, CRP prints the cable numbers under the following categories:

- US
- UK
- Japan
- France
- Belgium
- Other.

If you do not code the LIC keyword or if you code an invalid value, CRP prints a message with asterisks in the columns under the US heading. Figure 44 is an example of a Cable Selection Report (IBM 3725).

```
SSP VxRx                                CONFIGURATION REPORT PROGRAM
DATE: 08/14/92                          3725 CABLING INSTRUCTIONS                    PAGE     3

                          CABLE GROUP NUMBER
                        ***********************************************
   LINE      LIC    LINE     US      UK     JAPAN    FRENCH  BELGIUM   ALL
   NAME      TYPE   ADDRESS                                           OTHER
   ****      ****   *******  ****    ****   *****    *******  *******  *****
 L04002      1        002    080     092      081      080      092      080
 L04003               003    ***                                              IFW313I  NO VALID LIC TYPE SPECIFIED
 L04009      2        009    086     086      086      086      086      086
 L04010      4        010    089     089      089      089      089      089
 L04011               011    ***                                              IFW313I  NO VALID LIC TYPE SPECIFIED
 L04012      3        012    087     087      087      095      087      087
 L05008      2        008    086     086      086      086      086      086
                             ************************************
                             * END CABLE SELECTION REPORT       *
                             ************************************
```

Figure 44. Example of a Cable Selection Report (IBM 3725)

VTAM Network Configuration Report

The VTAM Network Configuration Report prints an entry for all VTAM and generation definition statements that have labels in columns 1 through 8 of the generation definition. When you code VTAM on the *REPORT statement, the following entries are printed:

- Resource name (label)
- Resource level (definition statement name)
- SNA or non-SNA determination (for definition statements easily categorized)
- Physical or logical address (LINE definition statements only)
- Channel adapter (CA) address
- Physical unit type
- Logical unit local address
- Logical unit physical resource reference.

Figure 45 on page 330 is an example of a VTAM Network Configuration Report.

```
SSP VxRx                                CONFIGURATION REPORT PROGRAM
DATE: 07/14/92                              ACF / VTAM NETWORK                    PAGE    15

        RESOURCE      RESOURCE     SNA/     LINE  ADDR     CA        PU      LU     PHYS  RES
          NAME         LEVEL     NON-SNA   PHYS | LOG   ADDRESS    TYPE   LOCADDR  REFERENCE
        PU1088          PU        SNA
        LU1088           LU       SNA
        GPHYB         GROUP       SNA
        LN1089         LINE       SNA      1089
        PU1089          PU        SNA                              1
        LU1089           LU       SNA
        GPHYI2        GROUP       SNA
        LN1092         LINE       SNA      1092
        PU1092          PU        SNA
        LU1092           LU       SNA
        GPHYB2        GROUP       SNA
        LN1093         LINE       SNA      1093
        PU1093          PU        SNA                              1
        LU1093           LU       SNA
        GLOGB         GROUP       SNA
        GLOGB2        GROUP       SNA
        LLN93L0        LINE       SNA
        LPU93L0         PU        SNA                              2.1
        PRIMNTI       GROUP       SNA
        SECDNTI       GROUP       SNA
        GLOGI         GROUP       SNA
        LLN88L0        LINE       SNA
        LPU88           PU        SNA                              4
        GLOGI2        GROUP       SNA
        LLN92L0        LINE       SNA
        LPU92           PU        SNA                              4
        DLANG9        GROUP       SNA                                        L2080PU
        L2080LLN       LINE       SNA
        L2080LPU        PU        SNA                              4
        DLANGA        GROUP       SNA                                        L3040PU
        L3040LLN       LINE       SNA
        L3040LPU        PU        SNA                              4
        GSNA2         GROUP       SNA
        CA0            LINE       SNA                    00
        PUCHAN0         PU        SNA                              5
        CA1            LINE       SNA                    01
        PUCHAN1         PU        SNA                              5
        CA2            LINE       SNA                    02
        PUCHAN2         PU        SNA                              5
        CA8            LINE       SNA                    08
        PUCHAN8         PU        SNA                              5
        PHYSGRP       GROUP       SNA
        S2432LN        LINE       SNA      2432
SSP VxRx                                CONFIGURATION REPORT PROGRAM
DATE: 07/14/92                              ACF / VTAM NETWORK                    PAGE    16

        RESOURCE      RESOURCE     SNA/     LINE  ADDR     CA        PU      LU     PHYS  RES
          NAME         LEVEL     NON-SNA   PHYS | LOG   ADDRESS    TYPE   LOCADDR  REFERENCE
        S2432PU         PU        SNA                              1
        S2816LN        LINE       SNA      2816
        S2816PU         PU        SNA                              1
        LOGGRP1       GROUP       SNA                                        S2432PU
        S2432LLN       LINE       SNA            1
        S2432LPU        PU        SNA                              5
        LOGGRP2       GROUP       SNA                                        S2816PU
        S2816LLN       LINE       SNA            1
        S2816LPU        PU        SNA                              2
        GENEND        GENEND
```

Figure 45. Example of a VTAM Network Configuration Report

NCP Configuration Report

When you code NCP on the *REPORT statement, CRP prints the NCP Configuration Report and prints an entry for any of the following definition statements:

NCPNAU	PUDRPOOL	SERVICE	COMP	GWNAU
LUDRPOOL	GROUP	CLUSTER	PU	PATH
LUPOOL	LINE	TERMINAL	LU	NETWORK

CRP prints labels, definition statement names, keyword values, and CRP partial- and full-line comments (*/L and */C type comments). The NCP Configuration Report is divided into the following parts:

- Report header box
- Non-SNA device pages
- SNA device pages
- PATH definition statement pages
- Resource pool report
- GWNAU definition statement pages
- Modem report section
- Non-native network header box.

The following are descriptions of the NCP Configuration Report parts.

Header Box

Use the BUILD definition statement to print the NCP Configuration Report header box. The information in the header box includes the following information:

- RUN DATE and RUN TIME refer to the date and time of the CRP run. The time printed is Greenish mean time (GMT).
- SYSTEM is the value of the TYPSYS keyword on the BUILD definition statement.
- MODEL is the value of the MODEL keyword on the BUILD definition statement.
- TYPGEN is the value of the TYPGEN keyword on the BUILD definition statement.
- VERSION is the value of the VERSION keyword on the BUILD definition statement.
- AUXADDR is the value of the AUXADDR keyword on the BUILD definition statement.
- NAMTAB is the value of the NAMTAB keyword on the BUILD definition statement.
- NCP LOAD MODULE NAME is the name of the NEWNAME keyword on the BUILD definition statement. However, if you omit the NEWNAME keyword, CRP generates a name.
- NATIVE NETWORK NAME is the name coded on the NETID keyword on the BUILD definition statement.
- SALIMIT is the value of the SALIMIT keyword on the BUILD definition statement.
- ERLIMIT is the value of the ERLIMIT keyword on the BUILD definition statement.

- USGTIER is the value of the USGTIER keyword on the BUILD definition statement.
- MAXSUBA is the value of the MAXSUBA keyword on the BUILD definition statement.
- SUBAREA is the value of the SUBAREA keyword on the BUILD definition statement.
- SLOWDOWN is the value of the SLODOWN keyword on the BUILD definition statement.
- CWALL is the value of the CWALL keyword on the BUILD definition statement.

Figure 46 shows an example of a NCP Configuration Report header box.

```
************************************
*==================================*
* NCP CONFIGURATION REPORT PROGRAM  *
*==================================*
*                                  *
* RUN DATE ..............  08/14/92  *
* RUN TIME ..............  16:15 (GMT)*
* SYSTEM   ..............  OS        *
* MODEL    ..............  3745      *
* TYPGEN   ..............  NCP       *
* VERSION  ..............  V6        *
* AUXADDR  ..............  0         *
* NAMTAB   ..............            *
* NCP LOAD MODULE .......  LULBNO    *
* NATIVE NETWORK NAME ...  NETC      *
* SALIMIT ...............  255       *
* ERLIMIT ...............  8         *
* USGTIER  ..............  5         *
*                                    *
* MAXSUBA  = 255     SUBAREA =  6    *
* SLOWDOWN =  12     CWALL   =   26  *
************************************
```

Figure 46. Example of an NCP Configuration Report Header Box

Non-SNA Device Pages

CRP puts a complete list of the non-SNA devices in the NCP Configuration Report. The following list explains the non-SNA device column headings:

RESOURCE NAME	Symbol
RESOURCE LEVEL	Definition statement type
ELMT ADDR	Computed by CRP
LINE CNTL	LNCTL keyword value
LINE SPEED	SPEED keyword value
CU TYPE	CUTYPE keyword value
DX	DUPLEX keyword value
CLK	CLOCKNG keyword value
TERM TYPE	TERM keyword value
LINK TYPE	TYPE keyword value
DIAL	DIAL keyword value
POLL/GPOLL	POLL or GPOLL keyword value
ADDRESS	ADDRESS keyword value

COMMENTS/NOTES — Area for */C comments. If COMPACB=YES is on the GROUP definition statement, "COMPATIBLE UACB" appears in this column; if COMPACB=NO is on the GROUP definition statement, "INCOMPATIBLE UACB" appears.

Figure 47 shows the non-SNA device page.

```
SSP VxRx                        CONFIGURATION REPORT PROGRAM                          PAGE    12
DATE: 08/14/92                       NON-SNA DEVICES
                                  LOAD MODULE - LULBNO
```

RESOURCE NAME	RESOURCE LEVEL	ELMT ADDR	LINE CNTL	LINE SPEED	CU TYPE	D X	CLK	TERM TYPE	LINK TYPE	DIAL	POLL/ GPOLL	ADDRESS	COMMENTS/NOTES
GTWX	GRP		SS						NCP	NO			
NCPTWX	LINE	0001	SS	110		F	INT	TWX	NCP			029	
TWXTERM	TERM	0002						TWX					
G3271	GRP		BSC						NCP	NO			
LN32760	LINE	0003	BSC	4800		F	EXT		NCP			065	
T32760	SRV												
C32760													
C32760	CLUS	0004			3271						40407F7F		
T32760	TERM	0005						3277			40404040	60604040	
LN3276B	LINE	0006	BSC	2400		F	EXT		NCP			032	
T3276B	SRV												
C3276B													
C3276B	CLUS	0007			3271						C3C37F7F		
T3276B	TERM	0008						3277			C3C34040	41414040	
LN3276C	LINE	0009	BSC	9600		F	EXT		NCP			034	
T3276C	SRV												
C3276C													
C3276C	CLUS	000A			3271						C1C17F7F		
T3276C	TERM	000B						3277			C1C14040	61614040	
LN3276D	LINE	000C	BSC	2400		F	EXT		NCP			033	
T3276D	SRV												
C3276D													
C3276D	CLUS	000D			3271						C2C27F7F		
T3276D	TERM	000E						3277			C2C24040	62624040	

Figure 47. Example of a Non-SNA Device Page

SNA Device Pages

CRP prints a complete list of the SNA devices in the NCP configuration report. The counters for the SNA devices appear immediately after the list of the SNA devices. The following explains the SNA device column headings:

RESOURCE NAME — Symbol

RESOURCE LEVEL — Definition statement type

ELMT ADDR — Computed by CRP

LINE CNTL — LNCTL keyword value or one of the following words:

- "ENET" for Ethernet-type subsystem (ESS) lines
- "NTRI" for NTRI lines
- "FRLY" for 3745 frame-relay lines
- "ESCA" for Enterprise Systems Connection (ESCON) lines
- "TRA" for ODLC token-ring lines
- "OSDLC" for 3746 Model 900 SDLC lines

LINE SPEED — SPEED keyword value

DX — DUPLEX keyword value

DM	DATMODE keyword value
CLK	CLOCKNG keyword value
NRZI	NRZI keyword value
DIAL/ADDR	DIAL, ADDRESS, or ADDR keyword value
PU TYPE	PUTYPE keyword value
TGN	TGN keyword value
SUB AREA	SUBAREA keyword value
VIR	VIRTUAL keyword value
VIRTUAL OWNER	VIROWNER keyword value
LINK OWNER	LNKOWNER keyword value
BATCH/MOD	BATCH keyword value or MODULO keyword value
NETID/RESSCB	NETID keyword value or RESSCB keyword value
COMMENTS/NOTES	Area for */C comments. If GENILU=NO on the BUILD definition statement, the word "IGNORED" appears in this column for independent logical units. The word "INDEPENDENT" appears for other independent logical units. If COMPACB=YES is on the GROUP definition statement, "COMPATIBLE UACB" appears in this column; if COMPACB=NO, "INCOMPATIBLE UACB" appears.

Figure 48 is an example of an SNA device page.

```
SSP VxRx                          CONFIGURATION REPORT PROGRAM                    PAGE    26
DATE: 11/14/92                          SNA DEVICES
                                  LOAD MODULE - MAIN621
```

RESOURCE NAME	LEVEL	ELMT ADDR	LINE CNTL SPEED	DX	DM	CLK	NRZI	DIAL/ ADDR	PU TYPE	TGN	SUB AREA	VIR	VIRTUAL OWNER	LINK OWNER	BATCH /MOD	NETID/ RESSCB	COMMENTS/NOTES
LLN93L0	LINE	0025	SDLC														
LPU93L0	PU	0026							2.1								
PRIMNTI	GRP							NO							8		
SECDNTI	GRP							NO							8		
GLOGI	GRP							NO							8		
LLN88L0	LINE	0027	SDLC							36							
LPU88	PU	0028							4	36							ADDR=04400000000034
GLOGI2	GRP							NO							8		
LLN92L0	LINE	0029	OSDLC					2112									
LPU92	PU	002A															
DLANG9	GRP							NO							8		
L2080LLN	LINE	002B	TRA														
L2080LPU	PU	002C							4								ADDR=04400000000030
DLANG9	GRP							NO							8		
L2084LLN	LINE	002D	TRA														
L2084LPU	PU	002E							4								ADDR=04400000000030
GSNA2	GRP							NO							8		
CA0	LINE	002F	CA					00									
PUCHAN0	PU	0030							5	1							
CA1	LINE	0031	CA					01									
PUCHAN1	PU	0032							5	1							
CA2	LINE	0033	CA					02									
PUCHAN2	PU	0034							5	1							
CA8	LINE	0035	CA					08									
PUCHAN8	PU	0036							5	1							
PHYSGRP	GRP							NO							8		
S2432LN	LINE	0037	ESCA 1800000					2432									
S2432PU	PU	0038							1								
S2816LN	LINE	0039	ESCA 4000000					2816									
S2816PU	PU	003A							1								
LOGGRP1	GRP							NO							8		
S2432LLN	LINE	003B	ESCA 1800000														
S2432LPU	PU	003C						01	5	1							

Figure 48. Example of an SNA Device Page

PATH Definition Statement Pages

CRP generates two report sections for each PATH definition statement. The first section has three headings:

RESOURCE LEVEL	Definition statement type
RESOURCE NAME	Symbol
DESTINATION SUBAREAS	DESTSA keyword value.

The second section for each PATH definition statement includes the following:

- ER keyword value
- VRPWS keyword value
- VR keyword value
- */C comments.

Note: You can have up to eight */C comments for each PATH definition statement:

Figure 49 is an example of a PATH definition statement page.

```
SSP VxRx                          CONFIGURATION REPORT PROGRAM
DATE: 08/14/92                         PATH DEFINITION                                    PAGE     9
                                     LOAD MODULE - LULBNO

RESOURCE RESOURCE
 LEVEL    NAME        DESTINATION SUBAREAS
PATH                 16
                                        TG THRESHOLDS          | VRPWS   MIN MAX |
                    ER# ADJSA TGN  LO     MED    HI    TOTAL  | VR#/TPF  WD  WD | VR# ER#|      COMMENTS/NOTES
                     1  16    1   5000   5000   5000   20000 |                 |  1   1 |
                     2  16    1                               |                 |  2   1 |
                     3  16    1                               |                 |  3   1 |
                     4  16    1                               |                 |  4   4 |
                     5  16    1                               |                 |  5   5 |
                     7  16    1                               |                 |  7   7 |
```

Figure 49. Example of a PATH Definition Statement Page

Resource Pool Report

The following items appear in the resource pool report shown in Figure 50 on page 336:

- ADDSESS is the value of the ADDSESS keyword on the BUILD definition statement.
- MAXSESS is the value of the MAXSESS keyword on the BUILD definition statement.
- RESOURCE NAME is the statement label.
- RESOURCE LEVEL is the definition statement type.
- NUMBER OF UNITS IN POOL is the value of the PUDRPOOL or LUDRPOOL definition statement.
- NUMTYP1 is the value of the NUMTYP1 keyword on the LUDRPOOL definition statement.
- NUMTYP2 is the value of the NUMTYP2 keyword on the LUDRPOOL definition statement.

- FRSEDRPU is the value of the FRSEDRPU keyword on the PUDRPOOL definition statement.
- **NCP V4R1 and NCP V4R2:** MAXLU is the value of the MAXLU keyword on the PUDRPOOL or LUDRPOOL definition statement.

```
SSP VxRx                        CONFIGURATION REPORT PROGRAM
DATE: 07/14/92                      RESOURCE POOL REPORT                    PAGE    23
                                  LOAD MODULE - MAIN601

| ADDSESS | MAXSESS |  RESOURCE   | NUMBER OF UNITS |        |         |         |
| 0-65535 | 0-65535 | NAME  LEVEL |    IN POOL     |        | NUMTYP1 | NUMTYP2 | FRSEDRPU |
0       0      65535

                        PUPOOL  |PUDR|      3
                        LUL001  |LUDR|                          1       2
```

Figure 50. Example of a Resource Pool Report

GWNAU Definition Statement Pages

The GWNAU definition statement page has information for two types of GWNAU definition statements, the predefined GWNAU and dynamic pool GWNAU. The predefined GWNAU headings are as follows:

RESOURCE NAME	Symbol
RESOURCE LEVEL	Definition statement type
PRE-DEFINED NETID	NETID keyword value
NUMSESS	NUMSESS keyword value
ELEMENT ADDR	Computed by CRP
COMMENTS/NOTES	Area for */C comments.

The last line always contains the GWNAU dynamic pool definition statement information. The NUMADDR keyword value is printed for the dynamic-pool GWNAU.

Figure 51 is an example of the GWNAU definition statement report page.

```
SSP VxRx                CONFIGURATION REPORT PROGRAM
DATE: 08/29/92              GWNAU INFORMATION                   PAGE    47
                          LOAD MODULE - NCP431

|  RESOURCE   | PRE-DEFINED | NUM- | ELEMENT |      COMMENTS/NOTES      |
| NAME  LEVEL |    NETID    | SESS |  ADDR   |                          |
T1M       |GWN| NETT          3     0002
          |GWN| NUMADDR=    50(DYNAMIC POOL)

SSP VxRx                CONFIGURATION REPORT PROGRAM
DATE: 08/29/92              GWNAU INFORMATION                   PAGE    66
                          LOAD MODULE - NCP431

|  RESOURCE   | PRE-DEFINED | NUM- | ELEMENT |      COMMENTS/NOTES      |
| NAME  LEVEL |    NETID    | SESS |  ADDR   |                          |
A1M       |GWN| NETA          3     0001
A2M       |GWN| NETA          3     0002
A10M      |GWN| NETA          3     0003
          |GWN| NUMADDR=    50(DYNAMIC POOL)
```

Figure 51. Example of a GWNAU Definition Statement Page

Modem Report Section

The modem report section follows all SNA device pages but precedes the first non-native network header box. The heading definitions are:

RESOURCE NAME	Symbol
RESOURCE LEVEL	Definition statement type (always "LINE")
MODEM TYPE	3867 when LPDATS = (LPDA1,3867)
LPDATS	LPDATS keyword value
CORNUM	CORNUM keyword value
CHNLZ	CHNLZ keyword value
PORT/CHANLA	PORT keyword value or the letter "A" if CHANLA=YES is on the LINE definition statement
TAIL	TAILING keyword value
CLINES/CALINE	CLINES or CALINE keyword value
COMMENTS/NOTES	Area for */C comments.

Figure 52 is an example of a modem report section.

```
SSP VxRx                    CONFIGURATION REPORT PROGRAM
DATE: 08/14/92                 MODEM REPORT SECTION                    PAGE 16
                               LOAD MODULE - LULBNO
```

RESOURCE NAME	RESOURCE LEVEL	MODEM TYPE	LPDATS	CORNUM	CHNLZ	PORT/ CHANLA	TAIL	CLINES / CALINE	COMMENTS/NOTES
LN3276B	LINE		LPDA2	80	YES	B	NO		
LN3276C	LINE		LPDA2	12	YES	A	NO		
LN3276D	LINE		LPDA2	12	YES	B	YES		
LNHMP2	LINE		LPDA2	80	YES	D	YES		
LNHMM2	LINE		LPDA2	12	YES	C	YES		

Figure 52. Example of a Modem Report Section

Non-Native Network Header Box

The NETWORK definition statement causes the non-native network header box to print. The information in the header box includes the values of the NETID, MAXSUBA, SUBAREA, ERLIMIT, SALIMIT and COPIES keywords.

- RESOURCE DEFINITION FOR provides the NETID keyword value.
- MAXSUBA is the value of the MAXSUBA keyword used for the NETWORK definition statement.
- SUBAREA is the value of the SUBAREA keyword used for the NETWORK definition statement.
- **NCP V5R4 and Later:** ERLIMIT is the value of the ERLIMIT keyword used for the NETWORK definition statement.
- SALIMIT is the value of the SALIMIT keyword used for the NETWORK definition statement.
- **NCP V5R4 and Later:** COPIES is the value of the COPIES keyword used for the NETWORK definition statement.

Figure 53 is an example of a non-native network header box when COPIES is not specified.

```
***********************
* RESOURCE DEFINITION *
*     FOR NET 4       *
*                     *
*   MAXSUBA = 15      *
*   SUBAREA = 6       *
*   SALIMIT = 511     *
*   ERLIMIT = 8       *
***********************
```

Figure 53. Example of a Non-Native Network Header Box (NCP V5R4 and NCP V6R1 and Later)

Figure 54 is an example of a non-native network header box when COPIES is specified and NETID is not (NCP V5R4 and NCP V6R1 and later).

```
***********************
* RESOURCE DEFINITION *
*  FOR MODEL NETWORK  *
*                     *
*   MAXSUBA= 127      *
*   SUBAREA= 7        *
*   SALIMIT= 255      *
*   ERLIMIT= 8        *
*   COPIES = 3        *
***********************
```

Figure 54. Example of a Non-Native Network Header Box When COPIES Is Specified and NETID Is Not (NCP V5R4 and NCP V6R1 and Later)

Node Cross-Reference List

The node cross-reference list prints only when you request NCP or VTAM reports. CRP lists labels in alphabetical order, vertically. For each occurrence of a label, its page numbers are listed to the right. Labels are now cross-referenced to the generation definition listing.Figure 55 shows a node cross-reference list.

```
SSP VxRx                CONFIGURATION REPORT PROGRAM
DATE: 08/14/92           NODE CROSS REFERENCE LIST                    PAGE 18
```

NODENAME	PAGE	NODENAME	PAGE	NODENAME	PAGE
CA0	4,14	LU3276C1	4,14	P3767A	3,13
CA1	4,14	LU3276C2	4,14	P3767H1	4,13
CA10	4,15	LU3276M1	4,14	TWXTERM	3,12
CA11	4,15	LU3276M2	4,14	T3276B	3,12
CA12	5,15	LU3276N1	4,14	T3276C	3,12
CA13	5,15	LU3276N2	4,14	T3276D	3,12
CA14	5,15	LU3276Q1	3,13	T32760	3,12
CA15	5,15	LU3276Q2	3,13		
CA2	4,14	LU3767A	3,13		
CA3	4,14	LU3767Q	3,13		
CA4	4,14	L3276A1	3,13		
CA5	4,14	L3276A2	3,13		
CA6	4,14	L3767A	3,13		
CA7	4,14	L3767H2	4,14		
CA8	4,14	NCPTWX	3,12		
CA9	4,14	NPALN	3,13		
C3276B	3,12	NPALU	3,13		
C3276C	3,12	NPAPU	3,13		
C3276D	3,12	PUCHAN0	4,14		
C32760	3,12	PUCHAN1	4,14		
GENEND	5,9	PUCHAN10	4,15		
GNPA	3,13	PUCHAN11	4,15		
GSNA	3,13	PUCHAN12	5,15		
GSNA1	4,14	PUCHAN13	5,15		
GTWX	3,12	PUCHAN14	5,15		
G3271	3,12	PUCHAN15	5,15		
HOST1	3	PUCHAN2	4,14		
LNFMP1	3,13	PUCHAN3	4,14		
LNFMQ1	3,13	PUCHAN4	4,14		
LNFP1	3,13	PUCHAN5	4,14		
LNHMM2	4,14,16	PUCHAN6	4,14		
LNHMP1	4,13	PUCHAN7	4,14		
LNHMP2	4,14,16	PUCHAN8	4,14		
LNHMQ1	4,14	PUCHAN9	4,15		
LN3276B	3,12,16	PUPOOL	3,10		
LN3276C	3,12,16	PU3276A	3,13		
LN3276D	3,12,16	PU3276B	4,13		
LN32760	3,12	PU3276C	4,14		
LULBNO	3	PU3276M	4,14		
LUL001	3,11	PU3276N	4,14		
LU3276A1	3,13	PU3276Q	3,13		
LU3276A2	3,13	PU3767A	3,13		
LU3276B1	4,13	PU3767Q	3,13		
LU3276B2	4,13	P3276A	3,13		

Figure 55. Example of a Node Cross-Reference List

Appendixes

Appendix A. Supplementary Network Flow Control Information

This appendix provides reference material about NCP network flow control that supplements the information in "Network Flow Control Error Procedure" on page 115. Although much of this material is also in the *NCP and EP Reference*, the emphasis in this appendix is on collecting reference material to *diagnose* network flow control problems.

This appendix is divided into the following sections:

- "Network Flow Control Mechanisms" gives an overview of network flow control and its terminology. It also discusses, in detail, virtual route pacing flow control.
- "Global Flow Control Mechanisms" discusses NCP global flow control mechanisms.
- "Local Flow Control Mechanisms" on page 346 discusses other flow control mechanisms used by NCP and VTAM.
- "Virtual Route State Information" on page 361 presents virtual route state information. This provides indications of network over-subscription and under-subscription.
- "Network Flow Control Variables" on page 363 lists NCP and VTAM flow control variables.

Network Flow Control Mechanisms

Network flow control mechanisms are categorized into global or local flow control. Local flow control consists of the mechanisms that regulate the entry and exit of data at one particular node. It holds data out of a node once congestion is detected at that node. This mechanism prevents users from entering new data in a congested boundary node or in a boundary node that feeds a congested virtual route.

Global flow control is a set of protocols and algorithms used to control data traffic on a route composed of hosts and NCPs. It is accomplished through the mechanism of virtual route pacing. Virtual route congestion indicators cause virtual route pacing changes and adjustments to network traffic through the local flow control mechanisms located at peripheral network nodes.

Global Flow Control Mechanisms

This section discusses the global flow control mechanism of virtual route pacing. The next section discusses local flow control mechanisms.

A virtual route is a bidirectional, logical pipe between two SNA subarea nodes. A virtual route defined between two subareas has a virtual route end point in each subarea node. Each virtual route end point consists of a virtual route sender and a virtual route receiver. Each virtual route communicates with its counterparts at the other virtual route end point. Figure 56 on page 344 shows the virtual route logical pipe. Virtual route pacing controls the rate of flow independently for each virtual route direction. The intermediate node shown in Figure 56 on page 344 is a trans-

port mechanism only, and has no knowledge of the virtual route mechanism. Virtual routes are used only to connect end points.

You can define up to 24 virtual routes between any two subarea nodes (eight virtual route numbers with three transmission priorities for each virtual route). At system generation time, each virtual route number is defined to flow over a particular explicit route. The host system definition parameters define the virtual routes that flow between VTAM and NCP. NCP system definition parameters define the virtual routes that flow between two NCPs.

Pacing on a virtual route operates on the concept of a dynamic window. A window is a set of path information units (PIUs). The amount of virtual route PIU traffic allowed to enter the network at any particular time is referred to as the window size. The window represents the amount of data allowed to be in transit on a virtual route in a given direction. The dynamic window algorithm operates a network at an optimum level by adjusting PIU traffic.

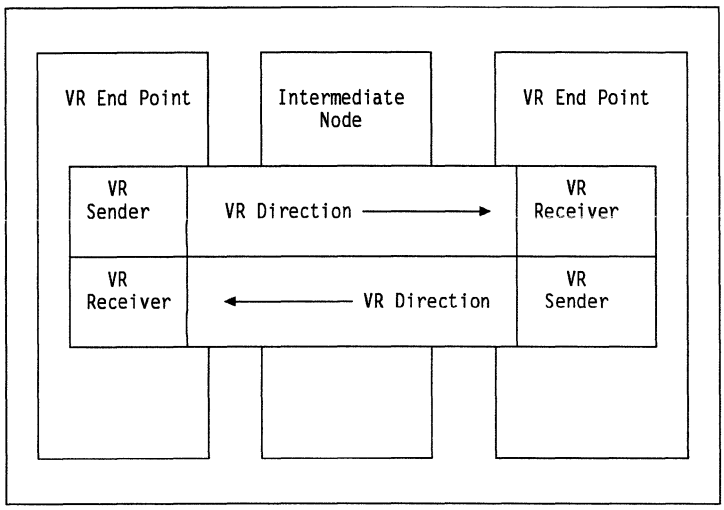


Figure 56. The Virtual Route Logical Pipe

The virtual route window size varies between a maximum and minimum size. These sizes are set at virtual route activation time by the virtual route activator. The window size is altered dynamically by the network in response to congestion. Congestion indicators in the PIU indicate whether you should adjust window size within the range of the maximum and minimum window size. Window size adjustments are based on the following situations:

Minor congestion:	Change window indicator (CWI) on. Decrement the current window size by one.
Severe congestion:	Reset window indicator (RWI) on. Set the current window size to the minimum value.
No congestion:	No indicators on. If the virtual route is held, increment window size by one when a you receive virtual route pacing response (VRPRS).

The window size will never be less than the minimum nor greater than the maximum. You may specify minimum and maximum window sizes on the VTAM and NCP PATH statement for each virtual route during system generation

(VRPWSnn keyword). If you do not do this, VTAM and NCP dynamically obtain these values based on the network topology. For further discussion about how window size is determined, see the section "Virtual Route Window Information" in the technical bulletin *VR Performance and Window Size Tuning*.

Beginning with a virtual route pacing request (VRPRQ), a virtual route transmitter may send the total PIU content of a window on a virtual route. A virtual route transmitter maintains a count that starts at the current window size and decrements it by one for each PIU transmitted on the virtual route. Counting begins with the PIU that carried the VRPRQ. Once the count reaches 0, the virtual route must stop transmitting unless it receives a VRPRS.

When the virtual route receives a VRPRS, the window count is set to the current window size, and transmission of the next window begins. If the virtual route has not received a VRPRS and the window count goes to 0, transmission on the virtual route stops until the virtual route receives a VRPRS in that direction. At this point, the virtual route is in a held state.

Window size modifications do not differ between NCP and VTAM. However, VTAM has a blocked state that is not included in NCP. PIUs that are waiting to be sent on a virtual route are queued on a virtual route transmit queue (NCP) or a virtual route hold queue (VTAM). With a VTAM virtual route end point, once the hold queue contains more than the total PIU content of one window, VTAM marks the virtual route as blocked, and limits the solicitation of data for the blocked virtual route.

A virtual route becomes held when the current pacing window expires at the virtual route sender. Usually when this occurs, the virtual route sender has data to send but does not have permission to send it. Common causes of an intermittently held virtual route in a virtual route sender are:

- Excessive network delay between the virtual route end points, such as transmission group queue congestion, link in error recovery, or intermediate subarea communication controller congestion.
- Excessive delay at the virtual route receiver. This can happen when a flow control mechanism attempts to prevent congestion for a cycle-constrained communication controller.
- Excessive error recovery values for single and multilink transmission groups or for peripheral links in gateway NCPs. In this case, delays occur only when a link error occurs. If a transmission group sequence number overflow occurs, link error recovery in a multilink transmission group may delay all transmission group links. A peripheral gateway NCP link that is in error recovery or is hung may cause the virtual route PIU pool of the virtual route in the network adjacent to this NCP to fill up. This causes the other end point of that virtual route to enter a held state. A temporary transmission group or gateway NCP peripheral link hangs due to excessive retries (RETRIES) or a high reply time-out (REPLYTO). See "Local Flow Control Mechanisms" on page 346 for more information on transmission groups and virtual route PIU pools.
- A low maximum virtual route window size value for the route used by the virtual route.

- Node failure. Hung network nodes can cause a held virtual route. Isolated VRPRSs are not numbered by virtual route sequence across a virtual route. If they are lost, a held virtual route results.
- Transmission group thresholds that are too small, causing congestion indicators. Congestion indicators decrease the virtual route window size and reduce the number of PIUs allowed into the network. A held virtual route results as the window size is constrained. In this case, the held virtual route is a symptom of a false congestion indication.
- A held virtual route in one network may cause held virtual routes in another network. This occurs if the virtual routes in one network feed a held virtual route in another network. Data backs up at the SNA network interconnection (SNI) network boundary, causing the virtual route PIU pool thresholds to be exceeded.
- Normal operation. This occurs when the route's "bottleneck transmission group" is at least one *hop* away from the virtual route sender. A *hop* is a single transmission group connection between two adjacent subarea nodes. This bottleneck normally occurs when a link feeding an intermediate node runs at a higher speed than the output link of that intermediate node. This results in normal data buffering within the intermediate node due to the difference in link speeds.

NCP transmits pacing information with 6 bits in the FID4 header of PIUs. Two bits request a pacing response or send a pacing request. The other 4 bits indicate network congestion. The virtual route block (VRB in NCP and VRBLK in VTAM) contains the virtual route status bits, congestion indicators, window sizes, and so on. One active virtual route block exists for each active virtual route. Inspect this block whenever diagnostic information is required for a virtual route. See "Network Flow Control Variables" on page 363 for more detailed information.

Local Flow Control Mechanisms

The local flow control part of network flow controls the amount of data in a peripheral network node. Primarily, the following local flow control mechanisms prevent users from entering new data into a congested boundary node. This section discusses the local flow control mechanisms used by NCP and VTAM.

NCP Buffer Slowdown Mechanism

The following section contains an overview of buffer management mechanisms related to the slowdown and CWALL thresholds. The NCP slowdown mechanism is a buffer resource protection scheme, which prevents severe congestion and reduces the possibility of deadlocks in network nodes.

Three main functions associated with buffer management are LEASE, PRELEASE, and COMMIT. Each of these has an important effect on the state of the NCP buffer pool. Depending upon how you use these functions and the number of free buffers available, four NCP buffer pool states occur. These are pseudo-slowdown, slowdown, pseudo-CWALL, and CWALL.

Pseudo-Slowdown State: NCP is in pseudo-slowdown when the free buffer count is less than the slowdown entry threshold plus the global committed buffer count. When NCP is in pseudo-slowdown, normal polling for peripheral lines is stopped.

Slowdown State: NCP enters slowdown when the free buffer count is less than the slowdown entry threshold. NCP exits slowdown when the free buffer count is greater than the slowdown exit threshold. The slowdown entry threshold is a certain percentage of the total number of buffers in NCP, specified on the BUILD definition statement during NCP system generation.

The slowdown exit threshold is a certain percentage of the slowdown entry threshold. While in slowdown, the following restrictions apply:

- Virtual route pacing responses are withheld on all virtual routes.
- Session pacing responses are withheld.
- Certain types of buffer requests are not satisfied.
- All restrictions for pseudo-slowdown state are also in effect.

When NCP enters and exits slowdown, it sends messages to all the hosts that are in session with NCP. It displays these messages on the network operator's console.

Pseudo-CWALL State: NCP is in pseudo-CWALL when the free buffer count is less than the CWALL threshold plus the global committed buffer count. When NCP is in pseudo-CWALL, normal polling for subarea links is stopped. All of the restrictions listed for slowdown are also in effect.

CWALL State: NCP is in CWALL when the free buffer count is less than the CWALL threshold. The CWALL threshold is a fixed number of buffers specified on the BUILD definition statement of the NCP generation definition. While in CWALL, the following restrictions are in effect:

- The channel and receiving lines cannot lease any buffers for incoming data.
- The channel gives an error status to all WRITEs attempted from the channel-attached hosts (CE,DE,UE).
- All the restrictions listed for pseudo-CWALL are also in effect.

NCP does not close the channel connection from a host to NCP when NCP enters slowdown. When NCP enters or exits slowdown, it sends entering or exiting slowdown notification to all its owning hosts. Its channel status will not change. At CWALL, NCP indicates a unit exception for host WRITE channel programs. NCP still honors channel programs that read (take data) from NCP. After exit from CWALL, NCP uses channel status bits to tell the host that it can write again. This is summarized as follows:

- (CE) + DE + UE:

  No buffers are available for host writes.

- (CE) + DE + UE + SM:

  Buffers are now available for host writes.

- (CE) + DE + ATTN + SM:

  A read is issued, and buffers are now available for host writes.

Lease Mechanism: After NCP and its control blocks are loaded in communication controller storage, some storage remains. NCP initialization formats the rest of available storage in buffers that are chained together in the free buffer pool. The XDA control block maintains the pointers to the first and last buffers in the free

pool. The BHBUFCHN field in the buffer prefix (BUFFER + X'0') chains the buffers themselves together. The LEASE mechanism removes buffers from the beginning of the free buffer chain and makes them available to lines, channels, or internal routines. The RELEASE mechanism replaces buffers on the end of the free buffer chain.

If the LEASE is satisfied, the current free buffer count is decremented by the number of buffers leased.
There are three types of buffer leases:

- CONDITIONAL
  - LEASE is satisfied if slowdown is not entered.
  - The conditional type of buffer is used when satisfying the lease is not critical and the lease may be delayed until some buffers are freed.
- CWALL
  - LEASE is satisfied if CWALL is not entered.
  - The CWALL type of lease is used by lines and channels.
- UNCONDITIONAL
  - LEASE is satisfied if there are enough buffers.
  - The unconditional type of lease is used only by internal routines when the leasing routine has some potential of causing deadlock if the LEASE were not satisfied.

Prelease Mechanism: Due to special processing considerations in NCP, buffers may be preleased to ensure future availability for level 5 tasks and critical processes. Tasks that expect to LEASE buffers will, at the beginning of the task, PRELEASE the number of buffers they need. If the PRELEASE is satisfied, the system PRELEASE count is incremented, and the current buffer count decremented by the number of buffers preleased.

There are two types of preleases:

- CONDITIONAL
  - PRELEASE is satisfied provided that the system does not enter slowdown.
  - The conditional type of prelease is used by noncritical level 5 tasks.
  - Unsatisfied conditional PRELEASEs may be queued on the conditional PRELEASE dispatch queue.
- UNCONDITIONAL
  - PRELEASE is satisfied if enough buffers exist.
  - The unconditional type of prelease is used by tasks that are critical to keeping data flow open and that have the likelihood of having more buffers released than leased if allowed to run.
  - Unsatisfied unconditional PRELEASEs may be queued on the unconditional PRELEASE dispatch queue.

Commit Mechanism: The COMMIT mechanism controls polling. COMMIT also assures that buffers will be available for messages received on the lines when the LEASEs are issued. Prior to sending a poll on a peripheral or subarea link, NCP issues a COMMIT for the expected number of buffers needed to contain the message that may be received in response to the poll. If the COMMIT is satisfied, the global committed buffer count is incremented by the number of buffers committed, and the line is polled in a normal fashion as receive ready (RR). If the COMMIT is not satisfied, the request may be queued on the commit request queue, and the line is polled as receive-not-ready (RNR).

There are two types of COMMIT:

- CONDITIONAL
  - COMMIT is satisfied if the system does not enter pseudo-slowdown.
  - The conditional type of COMMIT is used by peripheral network node links.
- CWALL
  - COMMIT is satisfied if the system does not enter pseudo-CWALL.
  - The CWALL type of COMMIT is used by subarea links.

NCP Slow Poll Mechanism

The slow poll mechanism works in cooperation with the global flow control mechanism of virtual route pacing. This helps prevent severe congestion or deadlock conditions at the peripheral node. NCP detects global congestion at a peripheral node by means of a held virtual route. A held virtual route causes NCP to restrict data from devices that feed the virtual route.

NCP can poll the RNRs of all physical units on the Synchronous Data Link Control (SDLC) lines that feed a held virtual route. For a binary synchronous communication (BSC) line containing a cluster, NCP can stop polling the devices that feed a held virtual route. As a result, physical units that have attached logical units feeding multiple virtual routes are RNR polled whenever any of the virtual routes becomes held. The slow poll mechanism prevents sessions that traverse other noncongested virtual routes, but share the same physical unit as the logical unit using the held virtual route, from becoming deadlocked. The slow poll mechanism affects only SDLC peripheral links.

Slow poll operates with the COMMIT logic when buffers are reserved for polling. Whenever a peripheral station feeds a held virtual route by means of one of its logical units, a no-poll bit is turned on in the committed buffers block (CBB). The CBB also maintains an RNR count, which it increments at every poll interval. When the count reaches 32, the no-poll bit is reset. Unless a PIU is received from a logical unit feeding a held virtual route, it remains off. Otherwise, the bit is turned on, and the count is incremented.

NCP BPOOL Mechanism

The destination boundary pool (BPOOL) mechanism sends information about local congestion at a peripheral node to the global flow control virtual route mechanism. This mechanism lets NCP control the rate at which it receives data from a virtual route. The BPOOL mechanism also feeds boundary devices physically connected to NCP. The BPOOL consists of the maximum number of buffers that incoming virtual route data, which feed physically attached devices, can occupy. The size of

the BPOOL is half of all buffers above the slowdown threshold. The other half of the buffers service subarea node traffic.

The BPOOL control block (BPB) maintains the BPOOL count. The virtual route receiver increments the count. The count is decremented when a PIU is moved to the channel-hold queue or to the link-outstanding queue, or when a PIU is released.
Changing window sizes on virtual routes ending in NCP slows virtual route traffic, depending upon the virtual route's priority and the level of buffers left in the BPOOL, as follows:

- For virtual routes with TPN=0:

  Set CWRI when BPOOL is at 62.5% threshold.
  Set RWI when BPOOL is at 75% threshold.

- For virtual routes with TPN=1:

  Set CWRI when BPOOL is at 75% threshold.
  Set RWI when BPOOL is at 87.5% threshold.

- For virtual routes with TPN=2:

  Set CWRI when BPOOL is at 87.5% threshold.
  Set RWI when BPOOL is full.

NCP IPPOOL and IPRATE Mechanism

This section applies to NCP V6R1 and later

The NCP Internet Protocol (IP) pool (IPPOOL) or rate (IPRATE) mechanism allows NCP to control congestion of Ethernet-type subsystem (ESS) lines independent of the NCP buffer slowdown mechanism. This mechanism prevents ESS lines from monopolizing NCP buffers since the interface between one Ethernet-type LAN and another executes at a lower level than other line interfaces. The Internet Protocol congestion control block (IPC) is used to maintain the Internet counters. The IPPOOL keyword on the BUILD definition statement specifies the percentage of the non-slowdown buffer pool that can be used for Internet traffic, and the IPRATE keyword on the BUILD definition statement specifies the maximum rate at which IP datagrams will be accepted from an Ethernet-type LAN. When either of these limits is exceeded, IP datagrams are discarded. See *NCP, SSP, and EP Resource Definition Guide* for more information on specifying the IPPOOL and IPRATE keywords. See *NCP and EP Reference Summary and Data Areas*, Volume 1, for more information on the IPC.

NCP Virtual Route End Point PIU Pool Mechanism

The NCP virtual route end point PIU pool was located in the peripheral node logic of every NCP. The NCP virtual route end point PIU pool worked in conjunction with BPOOL to prevent a single virtual route from monopolizing the BPOOL buffer pool. To do this, it either withheld virtual route pacing responses or, if congestion became severe enough, withheld the pacing responses and asked the virtual route sender to decrement the window size.

The data destined for devices physically attached to NCP is no longer considered part of the NCP virtual route end point PIU pool. Therefore, the NCP virtual route end point PIU pool functions mainly as an NCP gateway mechanism that prevents excess data accumulation at the SNI network boundary.

Traffic to the same network programmed resource logical unit block extension (NLX) still uses the NCP virtual route end point PIU pool mechanism. Examples of NLX are Network Terminal Option (NTO) traffic (see *NCP and SSP Customization Guide* and *NCP and SSP Customization Reference*) and system services control point (SSCP)-to-NCP physical unit traffic from the virtual route. Because the NCP virtual route end point PIU pool still affects NLXs and SSCP traffic, a complete description of how the mechanism previously worked is shown in Figure 57.

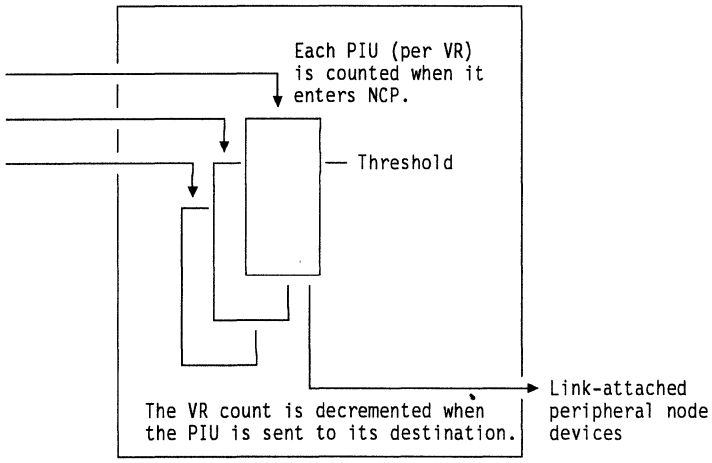


Figure 57. NCP Virtual Route End Point PIU Pool Located at a Peripheral Node NCP

NCP keeps a running count of the number of PIUs it receives over a given virtual route. When NCP receives the PIU, it increments the count. When NCP moves the PIU to either the channel-hold queue or link-outstanding queue, or when the PIU is released, NCP decrements the count. For BSC or start-stop devices, when NCP receives an ACK signifying that data was sent to the device, it decrements the count. NCP compares this count to a threshold that is kept for each virtual route. NCP does this only at a route end point for peripheral network nodes because virtual routes are known only at the end nodes.

If an SDLC link is not available, NCP does not schedule data destined to the link-outstanding queue. NCP does not decrement the virtual route PIU count. As new data arrives at the NCP destined for the unavailable link, the virtual route PIU pool threshold is reached. Once the threshold is reached, NCP withholds the virtual route pacing response and stops incoming traffic over the virtual route. A similar scenario occurs for unavailable BSC or start-stop links. By stopping the incoming traffic over the virtual route, the NCP virtual route end point PIU pool mechanism prevents continual acceptance and usage of NCP buffers for data arriving over a virtual route feeding an unavailable link.

If a virtual route feeds multiple peripheral node links, data to *all* these links from the virtual route stops if data cannot be scheduled to the link-outstanding queue of *any one* of the links. Therefore, depending on the logical and physical configuration, one link may affect the performance of several links.

Figure 58 on page 352 shows how NCP manipulates the virtual route PIU pool threshold count as the PIU is scheduled to the different NCP queues.

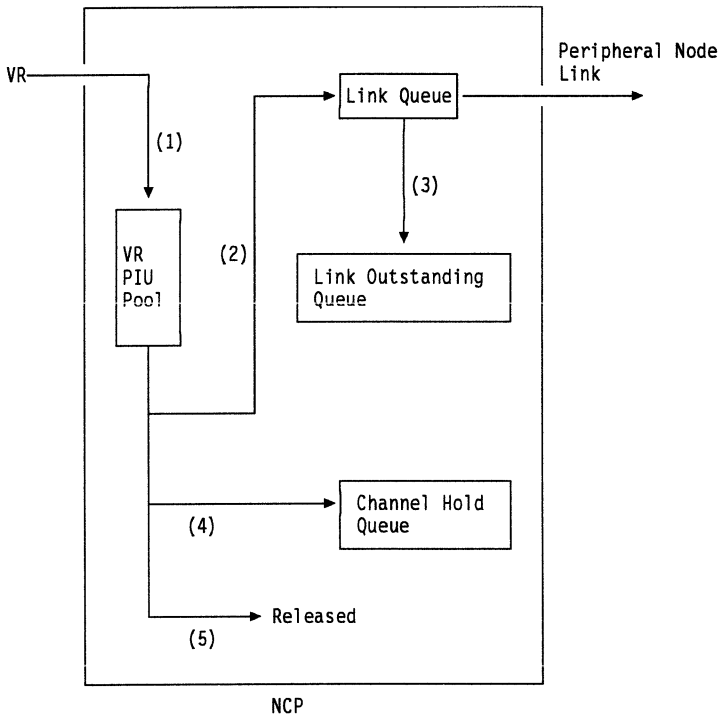


Figure 58. How the Virtual Route PIU Pool Threshold Is Determined

The following explanations refer to the notes in Figure 58.

1. When a PIU arrives on a virtual route, the virtual route PIU count is incremented by one. Each PIU on a particular virtual route is assigned a buffer associated with a particular virtual route PIU pool. PIUs destined for LUBs and DVBs are not counted.
2. The PIU is routed to the appropriate peripheral node link queue for transmission, at the link level, to an attached device.
3. The PIU is transmitted on the peripheral node link. A copy of the PIU is sent to the link-outstanding queue to await acknowledgment at the SDLC level. The virtual route PIU pool count is decremented by one when:
   - A copy of the PIU is sent to the link-outstanding queue.
   - The PIU is sent to the channel-hold queue when destined for a channel-attached host.
   - The PIU is released.
4. The threshold for each virtual route is determined as follows:
   - Initial (minimum) value is the greater of 9 or three times the minimum window size.
   - +1 for each active physical unit (CUB) that is attached to the virtual route.
   - +1 for each active physical unit (CUB) that has a logical unit attached to the virtual route.

- +1 for each active non-cluster DVB attached to the virtual route.
- +1 for each active non-gateway NLX attached to the virtual route.
- +1 for each active gateway NLX that represents a terminal attached to this virtual route ending in NCP.

The last two items above are supplied for completeness. They do not apply in non-gateway environments. This mechanism will not restrict the traffic flow from migration virtual routes.

5. The PIU is released.

You can take two possible actions when the number of PIUs from a virtual route exceeds its threshold:

- When the virtual route PIU count is greater than the threshold, withhold VRPRS on the virtual route.
- When the virtual route PIU count is greater than the threshold + 6, set CWRI to decrement the virtual route pacing window size. Decrementing the virtual route window is requested later than withholding the VRPRS. This prevents dramatic reductions in virtual route window sizes at the virtual route PIU pool thresholds.

A gateway NCP joins two (or more) network peripheral nodes in a common NCP. Cross-network sessions cross network boundaries in the gateway NCP; however, virtual routes end there. Two virtual route PIU pools control session data spanning a network boundary. Whenever the virtual route PIU pool threshold is exceeded, a held virtual route results at the other end point of the virtual route. Congestion and failures in an attached network can cause held virtual routes that end at a gateway NCP. Held virtual route symptoms can cascade through multiple networks. For example, if a virtual route in one network hangs, all virtual routes in attached networks that feed the hung virtual route may eventually hang. This is because the virtual route PIU pool thresholds may eventually be exceeded.

The following circumstances cause held virtual routes for virtual routes ending in a gateway NCP:

- Data arriving at the gateway NCP destined for another network by way of a transmission group that has failed or is in error recovery. (PIU is queued on the transmission group outbound queue.)
- Data arriving at the gateway NCP destined for another network using a virtual route that is in a held state. (PIU is queued on the virtual route transmit queue.)
- Data arriving at the gateway NCP from a non-native network destined for an unavailable physically attached terminal in the native network. (PIU is queued on the link-outbound queue.)

NCP Transmission Group Mechanisms

An SDLC transmission group is a collection of physically independent SDLC links that act as a single logical link. Links in a transmission group are logically sequenced in the order of their activation. Each link in a transmission group has its own SDLC protocol. You can add and delete links to accommodate capacity changes or multiple-link reliability. Failures of single links do not disrupt sessions using a multilink transmission group because session traffic is automatically routed over the remaining links in the transmission group. Whenever a link in a multilink

transmission group is busy, arriving PIUs are sent to the next available link in the transmission group. A PIU is sent to the first non-busy activated link. Deactivation and reactivation of a link causes the link to become the last activated. PIU traffic is scheduled for that link only if all other links of the transmission group are busy. (If monitor mode is used, links usually become active in the order defined by the NCP generation definition.) Remember, for any given NCP, all owners of the link must deactivate a link for it to become inactive.

NCP searches the transmission group to find an available link on a transmission group to schedule a PIU. If all links in the particular transmission group are busy, NCP queues the PIUs, by priority, on the transmission group outbound queue. This manipulation of PIUs is referred to as a multilink protocol.

This list applies to NCP V5R3 (VSE), NCP V5R4, and NCP V6R1 and later:

- In a casual connection environment, an adjacent link station's characteristics are unknown prior to the establishment of the switched connection. NCP assumes a negotiable role at system definition time for all switched SDLC lines, but you are given the option to specify that NCP is to assume a primary role during the contact sequence. A link station that has a negotiable role is a configurable link station. As a configurable link station, NCP enters SDLC role determination on switched connections during the contact sequence. During a successful contact sequence, NCP designates one station as primary and the other as secondary. For information about casual connection, refer to *NCP and EP Reference*.
- With the new token-ring adapter type 2, you do not need to define separate lines for the peripheral subarea functions.
- NTRI can load or dump over the line.

If NTRI contains both peripheral and subarea functions, define two separate lines.

The dynamic window mechanism works with subarea node functions by monitoring transmission group thresholds as shown in Figure 59. Session traffic flows through the network using one of three transmission priority levels. A fourth priority level is the "network priority" level. This level carries virtual route pacing responses (VRPRSs) separately from other traffic because VRPRSs are critical for network performance and must be transmitted ahead of all other virtual route traffic. This order ensures that heavy traffic in one direction does not interfere with the flow of virtual route pacing responses in the other direction. Such interference would decrease network throughput under heavy loads and increase exposure to deadlock situations.

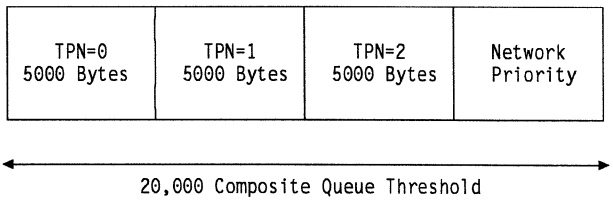


Figure 59. Transmission Group Queue Thresholds

Transmission priority also ensures consistent response time to favored applications during periods of heavy network load. The network displaces low-priority traffic with higher-priority traffic under heavy loads. This increases the "round-trip delay" for the low-priority PIUs. This delay slows the exchange of virtual route pacing messages by delaying the pacing request (but not the pacing response) and reducing the amount of low-priority traffic admitted to the network. The delay usually shows as a "held virtual route" for the lower-priority traffic virtual routes. Held virtual routes should be considered acceptable for low-priority traffic under heavy network loads. Low-priority virtual routes are delayed under heavy loads and use only excess network capacity.

Higher-priority traffic is always queued ahead of any lower-priority traffic at each transmission group outbound queue. The only exception is a PIU on the transmission group outbound queue with the sweep indicator bit on. Priority code will not schedule a higher-priority PIU ahead of one with the sweep indicator on. See "Multilink (Transmission Group) Protocol Details" on page 356 for additional details about the sweep function. Within each priority level, traffic is queued first-in, first-out (FIFO), for delivery to an adjacent node. Priority scheduling can be done in transmission group outbound queues. A PIU must be transmitted once it is on an SDLC link-outbound queue. This PIU cannot be preempted by a higher priority PIU because all PIU ordering and prioritizing is done in the transmission group outbound queue (see Figure 60 on page 357).

All PIUs in the transmission group outbound queue are given high priority after every 256 PIUs are transmitted. This ensures that lower-priority traffic is eventually serviced under heavy load. The PIUs remain unchanged, but are only logically set to high priority and transmitted. A modulo-256 counter is kept and decremented every time a PIU is enqueued on the transmission group outbound queue. When the count reaches 0, all PIUs on the transmission group outbound queue are logically set to high priority. The count is reset to 255 every time the transmission group outbound queue is emptied. Transmission priority is a property of virtual routing and is specified at the virtual route level of the network.

Once the transmission group is active, NCP monitors the amount of data waiting to be transmitted on a transmission group. The amount of data waiting to be sent is measured in bytes. Associated with this monitoring process are four transmission group thresholds: low-priority (TPN=0), medium-priority (TPN=1), high-priority (TPN=2), and a composite threshold. Network priority traffic is counted only towards the composite threshold. The default values of the thresholds are 5000, 5000, 5000, and 20 000 bytes respectively. You can change these default values in the generation definition using a keyword on the NCP PATH definition statement. When a PIU is scheduled to a transmission group, a check is made to determine the transmission priority and the PIU length. Its byte length is added to the transmission group counter for the PIU's priority and to the composite transmission group counter. If any particular transmission group priority counter exceeds 5000 bytes, CWI is set on in this PIU. If the composite transmission group counter exceeds 20 000 bytes, the reset window indicator (RWI) is set on in every PIU flowing in the opposite direction on this particular transmission group until the transmission group congestion ceases.

In summary, the transmission group queue mechanism lets NCP detect the congestion at the subarea-node-to-subarea-node level in the network. The congestion indicators in the PIUs flowing through the congested subarea node denote con-

gestion to the network sources. The indicators cause adjustments to the virtual route window size, which restricts data flow to the congested network.

Multilink (Transmission Group) Protocol Details

Session and other network protocols have always required that all requests and responses arrive at the destination in the same order that they were sent. However, PIUs flowing over a multilink transmission group can arrive at the receiving end of the transmission group in a sequence other than transmission order because:

- Transmission group links may operate at different speeds with different propagation times
- PIUs of various lengths may be transmitted across the transmission group
- Link errors result in re-transmission.

Any out-of-order PIUs are resequenced at the receiving end of each transmission group in the path. The multilink protocol operates only with FID4 PIUs. The FID4 transmission header contains a sequence-number field. The sending side of each transmission group sets the sequence-number field, and the receiving side of each transmission group checks the sequence-number field. Although a channel connection to an NCP is considered a transmission group, PIUs are not assigned a sequence number while they flow across the channel transmission group.

The transmission group scheduler does PIU sequencing. Whenever a PIU is scheduled to a link, the scheduler assigns a transmission group sequence number in the transmission group SNF field of the FID4 header. This field allows a maximum of 4096 sequence numbers. When this limit is reached, no additional PIUs are scheduled to the links until all previously scheduled PIUs are successfully transmitted. The sequencing is then restarted at 0. This method greatly simplifies the resequencing procedure, with only a small delay penalty at infrequent intervals.

At the receiving end of the transmission group, each transmission group sequence number is checked against the expected number (shown in Subarea B in Figure 60 on page 357) and one of the following happens:

- If the PIU sequence number is equal to the expected number, the transmission group sequence number field is zeroed out, and the PIU is passed to the explicit route control function of Path Control.
- If the PIU sequence number is lower, it is discarded as a duplicate. (Duplicate PIUs can occur due to the link error recovery process).
- If the PIU sequence number is higher, it is held in the transmission group resequence queue until it matches a later update of the received expected number.

Figure 60 shows the logic performed by the transmission group scheduler. This is the part of path control that manages the flow and sequencing of PIUs with multiple priorities flowing on multiple links.

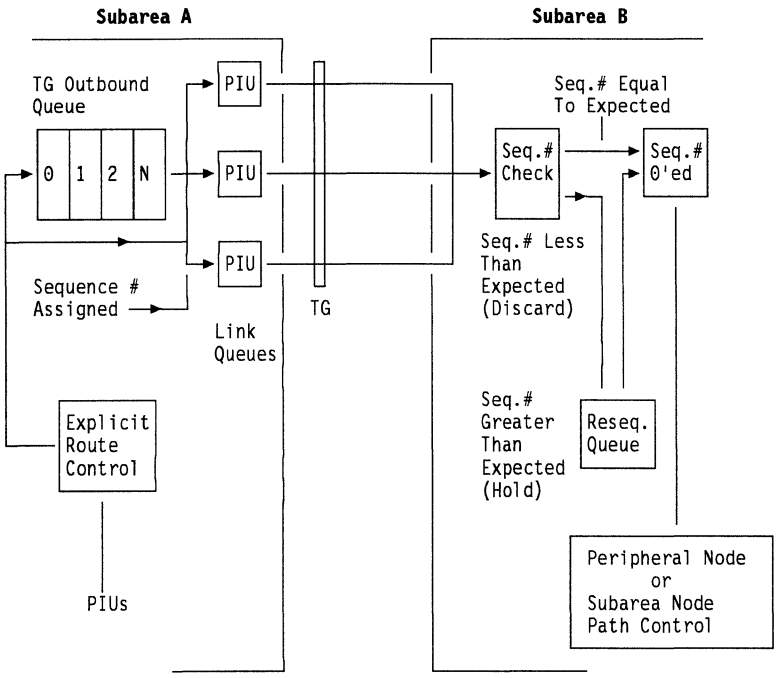


Figure 60. Transmission Group Multilink Protocol

Figure 60 shows that PIUs arrive at explicit route control, which queues them on the correct transmission group outbound queue in priority order, if a link queue is not immediately available for transmission. PIUs are placed on the transmission group outbound queue only when all the transmission group SDLC links are busy.

When a link queue becomes available, the PIUs on the transmission group outbound queue are then sent to the link outbound queue. This transfers the PIU to the link to be transmitted to the next subarea node (Subarea B). Subarea B checks the sequence number according to the resequence rules. If sequencing is correct, the sequence number field is zeroed out. The PIU is passed to subarea node path control or to the peripheral node function. The outbound queues of the transmission groups are serviced from the head of the line. PIUs are taken from the queue for transmission as if the queue were FIFO ordered. In other words, ordering and prioritizing is done when PIUs are placed in the transmission group outbound queue, not when PIUs are taken from the queue for transmission.

When a link in a transmission group enters error recovery, a PIU may need to be retransmitted. At that time, a copy is made and scheduled for transmission on that same link. The original PIU is requeued on another active link in the same transmission group without having to be rescheduled. See Figure 61 on page 358.

All the SDLC link-outbound queues in a transmission group are considered arranged in a logical ring. Proceeding sequentially around this ring, each queue acts as a backup for the next adjacent queue. If the original PIU encounters a link error on the backup link, the procedure is repeated. A copy is again made, and the original then goes to the next backup queue. Associated with the original PIU is a counter that is set at one as it moves to the first backup link and incremented by one as it progresses to each subsequent backup link in the transmission group. This rescheduling to backup links terminates when the count indicates that the PIU is about to move to the link from which it first started.

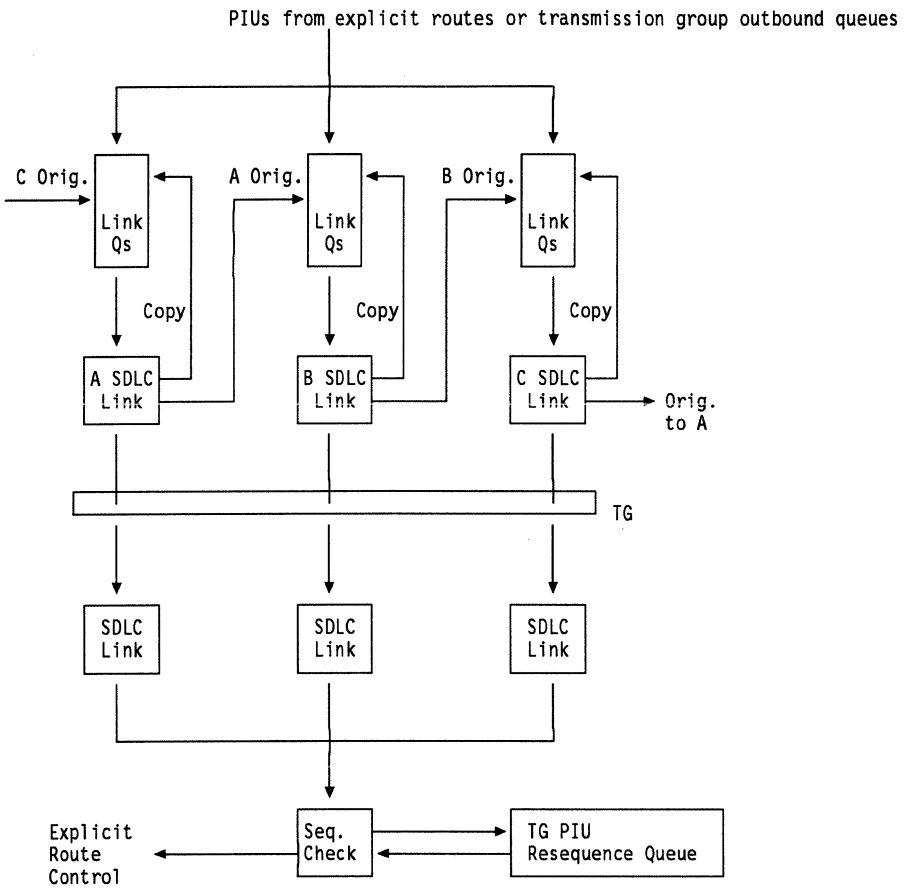


Figure 61. Transmission Group Link Backup and Error Recovery

Following normal error recovery procedures, the copies are retransmitted on their originally assigned links. This arrangement ensures that normal error recovery attempts occur on the individual links, and that the PIU is delayed as little as possible by diverting it to an alternate link. This minimizes a buildup of PIUs on the resequence queue. Because of buffer considerations, PIUs are not copied when NCP is in slowdown and the original is rescheduled on the same link. When a link fails, it is removed from the transmission group, and any original PIUs queued for it are rescheduled on its backup link. When the last link in a transmission group fails, all PIUs in the queue for both the transmission group and the link are discarded. The explicit route manager is advised that the transmission group has failed. Explicit route INOPs propagate from the failed transmission group, and VTAM error messages are issued.

At each link the following priorities are observed for the transmission of PIUs scheduled for that link:

1. Copies of PIUs being retransmitted on the same link
2. Original PIUs, rescheduled from another link to this link for backup
3. PIUs from the transmission group outbound queue, provided the link queue is empty, and the transmission group is not in purging traffic mode (sweep function).

The sweep function suspends passing PIUs from the transmission group outbound queue to the associated links in a multilink transmission group until all PIUs in

transit are acknowledged at the SDLC level. The sweep function is invoked in the following situations:

- The sweep indicator is on in the FID4 transmission header. The originating function sets this bit on when building any of the following control PIUs: ACTVR and its RSP, DACTVR and its RSP, ER-ACT, ER-ACT REPLY. This prevents these control PIUs from overtaking each other or any preceding session PIUs. This avoids situations that could lead to deadlocked sessions or middle segments missing from long messages.
- A link receives RNR. This avoids congestion problems such as congestion at the transmission group receiver's resequence queue. This may occur when a multilink transmission group operates under a heavy load. The transmitter enters an extended error recovery procedure (ERP) on one of its links but cannot copy the PIU for error processing because of a buffer shortage condition (slowdown). Meanwhile, the transmitter sends successive PIUs on the other transmission group links while a lower sequence number PIU is still in ERP processing. The receiver must hold all the PIUs in the resequence queue until ERP is over. If buffer depletion occurs at the receiver, a deadlock situation can occur.
- The transmission group sequence number field overflows. This simplifies the receiver's resequence logic and avoids a buffer depletion situation due to congestion on the parallel links resequence queue. The receiving NCP must send a FID F response. To successfully end the sweep function in this case, the transmitting NCP's links must be empty.

The transmission group sequence number field overflow (or rollover) occurs when a PIU with X'FFF' in the transmission group sequence number field is sent. The transmission group sequence number field allows a maximum of 4096 sequence numbers. When this limit is reached, no PIUs are scheduled to the links until all previously scheduled PIUs are successfully transmitted. The sequencing is then restarted at 0. When a transmission group sequence field overflow occurs, the following occurs:

1. The PIU with transmission group sequence number of X'FFF' is sent across a link in the transmission group. The sending NCP enters an expecting FID F condition.
2. The receiving NCP sends a FID F PIU to the sending NCP.
3. The sending NCP sets sweep on and queues all PIUs on the transmission group outbound queue (pointed to by FLBXQCB) until all preceding PIUs are acknowledged as being successfully sent by the NCP's Data Link Control (DLC) function.
4. When the DLC acknowledges that all PIUs were successfully sent, NCP sends a PIU with transmission group sequence number X'000'. The sending NCP waits for the DLC to acknowledge receipt of the sequence number PIU X'000'. This is necessary because temporary errors can cause duplicate PIUs with a transmission group sequence number field of X'FFF' or duplicate FID F PIUs. When the DLC acknowledges receipt of the PIU with sequence number X'000', normal transmission group PIU flow can resume.

A FID F PIU indicates that the receiving end of the transmission group sent all PIUs in the resequence queue to explicit route control. (This means that all PIUs were received and forwarded). This PIU is sent to the transmitting end of a transmission

group when a receiving transmission group gets a PIU with a sequence number of X'FFF', and the resequence queue is empty. If the transmitting NCP's links are also empty, the sweep function ends. This protocol prevents lost PIUs when the number expected rolls over to 0 at the receiving end of a transmission group. The protocol also prevents PIUs from being discarded when the number received is less than the number expected.

The transmission group may hang if link error recovery occurs while the transmission group is in sequence number field rollover. It hangs because sweep cannot end until all the individual link queues of the transmitting NCP transmission group are empty. A link in error recovery will not have an empty queue until error recovery finishes (successfully or unsuccessfully). Temporarily held virtual routes are usually symptoms of this activity and can occur if all the following are true:

- Retry or link activity time-out is specified with a high value.
- A link of a multilink transmission group breaks.
- A PIU is waiting to be sent over this link.
- Sweep begins.

The entire transmission group hangs (and, subsequently, virtual routes using the transmission group will enter the held state) until either retry ends (link inoperative), link activity times out (permanent error), or the link is successfully recovered.

VTAM Buffer Management Mechanisms

VTAM keeps the number of I/O requests as low as possible. This keeps the central processing unit (CPU) utilization to a minimum by using a *coattailing algorithm*. Coattailing occurs when the number of messages transferred in or out of the host is greater than the number of channel programs issued. VTAM carries out this algorithm for all SNA channel-attached devices, including channel-attached NCPs, CTCAs, 3790s, and SNA 3274s. The VTAM coattailing algorithm delays outbound traffic until one of the following occurs:

- Channel delay time-out occurs. VTAM waits for the channel delay time-out before scheduling input/output for the channel queue.
- Channel queue depth limit is reached. If the number of PIUs on the channel queue reaches the queue depth limit, VTAM schedules the channel.
- Channel buffer capacity is reached. When the number of PIUs on the channel queue reaches the known buffer capacity of the adjacent node, VTAM schedules the channel.
- Priority traffic is in the channel queue. VTAM immediately schedules the channel if any VRPRSs or transmission priority-2 traffic gets onto the channel queue.

For further discussion of this algorithm and its uses, see the section "VTAM Channel Coattailing Algorithm" in the technical bulletin *ACF Network Flow Control*.

VTAM has fewer local flow control mechanisms than NCP. VTAM's flow control mechanisms center around the use of the I/O buffer pool and CPU utilization.

The VTAM I/O buffer pool expands until MVS runs out of common storage area (CSA) or until the VTAM CSALIMIT start option value is reached. If VTAM reaches CSALIMIT, runs out of CSA, or has to wait for an I/O buffer pool expansion, VTAM will not accept any application data and will not issue read channel programs to any

channel-attached devices. Once I/O buffers become available again, VTAM sends RWIs on all virtual routes to indicate that VTAM congestion is occurring. VTAM never turns on CWI.

A VTAM process could be waiting for I/O buffers because of a thrashing of the I/O buffer pool's expansion and contraction. An expansion increment or threshold that is too small can cause the buffer pool thrashing. *VTAM Customization* describes how to tune these parameters.

VTAM never intentionally withholds VRPRSs. VTAM always requires one fixed I/O buffer to build the VRPRS. If VTAM cannot obtain this buffer immediately, it waits until a buffer becomes available.

When NCP owes VTAM a pacing response, and the virtual route becomes held in VTAM, VTAM queues the PIUs that are waiting for the held virtual route on the virtual route hold queue. When the virtual route hold queue contains more than one window full of PIUs, VTAM marks the virtual route blocked. VTAM no longer copies data from application buffers into VTAM buffers for the applications that use the held virtual route. This limits the number of VTAM I/O buffers that can be tied up by a blocked virtual route. However, SSCP-SSCP, SSCP-PU, and SSCP-LU traffic continues to be queued on the virtual route hold queue regardless of route status.

Channel-attached logical units that do not use inbound session pacing and feed a blocked virtual route cause VTAM to stop issuing read channel programs to the logical unit's physical unit. Even if one logical unit attached to a channel controller uses the blocked virtual route, all the logical units on that controller are affected. If inbound session pacing is specified, VTAM withholds the pacing response from the logical unit. Other logical units running off the physical unit are unaffected as long as they do not also feed the blocked virtual route. Thus, inbound pacing is recommended for channel-attached devices.

VTAM displays and traces can be used to identify VTAM performance problems. See *VTAM Diagnosis* for more information about diagnosing VTAM performance problems.

Virtual Route State Information

Flow control action is initiated on an individual virtual route basis at the end point of the virtual route. The following three conditions make up the virtual route flow control state. Flow control actions are taken depending on the virtual route state.

A Current virtual route window = maximum virtual route window
B Virtual route is held
C Congestion indicator is on in a previous window.

Analyzing virtual route states provides indications of network resource over-subscription and under-subscription. Get this state information from the virtual route control blocks located in VTAM and NCP. In this discussion, these states are considered from the virtual route sender's point of view. In the list that follows, the ¬ symbol indicates the word *not*. The following conditions are a result of the virtual route states indicated:

1. A and B and C. The window size is decreasing because of network congestion (C condition), and window size is not at the minimum (at maximum). This is a transient condition because the virtual route window size will decrease below the maximum once congestion indicators are seen. Congestion indicators always cause the window size to be lowered (down to, but not below the minimum) whether or not the virtual route is held.
2. A and B and ¬C. The virtual route window size may be too small for the underlying physical network capacity. The network can accept more data from this virtual route, and the virtual route end point is congested (B condition). If *network delays are considered normal*, the window size should be raised for efficient use of the logical virtual route pipe.

   Note: Raising the virtual route maximum window size may release latent demand that has been throttled by the current maximum window size. In addition, if *network delays are excessive*, this state may be a symptom of a congested box (cycle-constrained), link along the route, or congestion at the other end point of the virtual route. Also, cross-network traffic may be affected because a held virtual route in one network may cause the window to run out at the virtual route sender held virtual routes in attached networks. A node such as an IBM 3725 Communication Controller may abnormally delay processing pacing requests or responses (without congestion indicators being set). This causes the window to run out at the virtual route sender (the B condition is seen at the virtual route sender). In these cases, raising the window size may aggravate congestion. High-priority virtual route traffic can preempt low-priority virtual route traffic at the network transmission groups. This delays low-priority virtual route pacing information. Thus, this state may represent a normal state for low-priority virtual routes.
3. A and ¬B and C. The window size is decreasing due to network congestion (C condition). This is a transient condition because virtual route window size decreases below maximum once congestion indicators are seen. The virtual route window size decreases as long as the current window size does not equal the minimum window size. (A or ¬A condition could be true; see item 7 that follows).
4. A and ¬B and ¬C. No congestion or held virtual route exists, and no action is necessary. This may indicate that a load spike or a transient network delay problem drove the window size to maximum at some time. This does not necessarily indicate maximum window usage. It only means that congestion did not bring the window below maximum (no congestion indicators were detected). The maximum window size may be optimal for the current traffic load and route delay.
5. ¬A and B and C. Virtual route window size is decreasing if the window size is not at the minimum. If the window size is at the minimum, there is an oversubscribed physical element along this virtual route path. The B condition indicates that congestion exists at the virtual route end point, caused by network congestion. The B condition also shows that this virtual route has sufficient load to be the sole or major contributor to the congestion problem.

6. ¬A and B and ¬C. This indicates that the current window size is less than maximum. Window size is increasing due to held virtual route (B condition) and there is no congestion. Window size will increase by one each time a pacing response is received, if the virtual route is in a held state, up to the maximum window size.
7. ¬A and ¬B and C . The window size is decreasing due to congestion. If the window size is already at the minimum, an oversubscribed physical element exists along this virtual route path. Because the ¬B condition is true, no congestion exists at the virtual route end point, showing that network congestion is not causing a data backup at this virtual route end point. Many virtual routes may be merging at some network location causing congestion. The ¬B condition indicates that the virtual route does not have sufficient load to cause the congestion problem.
8. ¬A and ¬B and ¬C. No congestion exists on the network path or virtual route end point transmit queue. An optimum window size has been found for current traffic load and route delay.

If conditions 2, 5, or 7 appear at a virtual route end point, review either network resources or virtual route window size options affecting this route. Conditions 1, 3, or 6 represent transient conditions that appear only briefly as the virtual route window is raised or lowered. Conditions 4 and 8 represent optimal states for current virtual route load and delay characteristics.

If you frequently see congestion indicators, investigate the transmission group thresholds along the route. This is especially necessary if multiple virtual routes intersect at a transmission group, and a great majority of them show congestion indicators for a long period of time. If transmission group thresholds seem reasonable and you still see congestion indicators, investigate network resources and increase them if necessary. If multiple virtual routes, which all end or go through a common NCP, show held status (without any congestion indicators seen), investigate that NCP for congestion (check for high box utilization, buffer problems, and so on).

Network Flow Control Variables

This section shows the control blocks and pertinent fields that you may need to reference while you are in the other sections of the flow control discussion. Each item includes:

- The control field name, offset, and meaning
- The location of the pointer to the control block.

A pointer to a control block is a fullword location in NCP storage that contains the address of the control block. To find the address of the control block, display the address shown at the pointer's NCP storage location. To find the contents of a specific field in a control block, add the offset to the control block address and display the resulting address.

If the pointer is in another control block, refer to the section for that control block to find out how to obtain the pointer.

For example: Find contents of XDA + X'3C'
Pointer to XDA at X'6E8'
NCP V6R1 and later: Pointer to XDA at X'38'
Display: X'6E8'= X'0002B504'
NCP V6R1 and later: Display: X'38'= X'0002B504'
Add: X'0002B504'+ X'3C'= X'0002B540'
Display: X'0002B540'= X'0003D458'

Bits within a byte are numbered 0–7. The high-order bit in a byte is bit 0 and the low-order bit is bit 7.

For example: Contents of XDB + X'19'= X'AC'= B'10101100'
Bit 0 = 1
Bit 1 = 0
Bit 2 = 1
Bit 3 = 0
Bit 4 = 1
Bit 5 = 1
Bit 6 = 0
Bit 7 = 0

TH—Transmission Header

This part of the PIU contains the congestion indicators and the bits that mark the PIU as either a VRPRS or a VRPRQ. You may need to check the following fields in a trace:

TH4B0 - variable - byte

LOCATION: TH + X'00'
DESCRIPTION: Transmission Header - Byte 1
Bit 4 on: Transmission group sweeping
Bit 6 on: PCI—Pacing count is 0

The PIU originator sets the transmission group sweeping bit in the following control PIUs: ACTVR, RSP ACTVR, DACTVR, RSP DACTVR, ERACT, and ERACT REPLY. The virtual route end point on the last PIU in a window sets the PCI bit when a VRPRS has not been received.

TH4B3 - variable - byte

LOCATION: TH + X'03'
DESCRIPTION: VRID - Virtual route number and transmission priority
Bits 0 through 3: Virtual route number
Bits 6 through 7: Transmission priority

For example: X'42' means virtual route 4.2

TH4VRCF - variable - byte

LOCATION: TH + X'04'
DESCRIPTION: Virtual route routing control field
Bit 0 on: CWI—Change window indicator

The NCP transmission group on any PIU sets the CWI bit to indicate minor congestion. When the other virtual route end point receives a PIU with this bit set on, the window size is decremented.

TH4PACE - variable - byte

LOCATION: TH + X'06'
DESCRIPTION: Virtual route pacing control field
Bit 0 on: VRPRQ — Virtual route pacing request indicator
Bit 1 on: VRPRS — Virtual route pacing response indicator
Bit 2 on: CWRI — Change window reset indicator
Bit 3 on: RWI — Reset window indicator.

The first PIU transmitted in a window sets the VRPRQ bit. The PIU containing the VRPRS bit is an isolated pacing response, which contains only a TH and no data. If a VRPRS has the CWRI bit set on, this tells the virtual route end point that the other virtual route received a PIU with the CWI bit on. Decrement the virtual route window size. If congestion exists at an NCP virtual route end point, the end point can set this bit on. An NCP virtual route end point can also set the RWI bit to indicate that the BPOOL threshold is exceeded. An intermediate node sets the bit when the total transmission group byte threshold is exceeded. It indicates severe congestion. VTAM sets this bit when there is a shortage of fixed I/O buffers. This bit can be on in any PIU flowing in a direction opposite to the PIU that encountered congestion. When this bit is on, the virtual route receiver resets the virtual route window size to the minimum.

TH4DSAF - variable - fullword

LOCATION: TH + X'08'
DESCRIPTION: Destination subarea address

The PIU receiver resides at this subarea of the node. The subarea is right-justified.

TH4OSAF - variable - fullword

LOCATION: TH + X'0C'
DESCRIPTION: Origin subarea address

The PIU sender resides at this subarea of the node. The subarea is right-justified.

TH4DEF - variable - halfword

LOCATION: TH + X'12'
DESCRIPTION: Destination element address

This is the element address of the PIU receiver.

TH4OEF - variable - halfword

LOCATION: TH + X'14'
DESCRIPTION: Origin element address

This is the element address of the PIU sender.

XDA—NCP Word Direct Addressable

This control block contains the pointers to many other control blocks. The pointer to XDA is at X'6E8'.

NCP V6R1 and Later: The pointer to XDA is at X'38'.

SYSBPGCC - variable - fullword

LOCATION: XDA + X'08' (for NCP V6R2 and later)
DESCRIPTION: Global committed buffers count

SYSBPCBC - variable - fullword

LOCATION: XDA + X'14' (for NCP V6R2 and later)
DESCRIPTION: Current free buffer count

SYSBPTBC - variable - fullword

LOCATION: XDA + X'18' (for NCP V6R2 and later)
DESCRIPTION: Slowdown entry threshold

SYSBP1FB - variable - fullword

LOCATION: XDA + X'44'
DESCRIPTION: Pointer to the first buffer on free-buffer chain

SYSHWE - constant - fullword

LOCATION: XDA + X'58'
DESCRIPTION: Pointer to the HWE control block

SYSHWX - constant - fullword

LOCATION: XDA + X'5C'
DESCRIPTION: Pointer to the HWX control block

SYSBP2FB - variable - fullword

LOCATION: XDA + X'70'
DESCRIPTION: Pointer to the last buffer on free-buffer chain

HWE—NCP Extended Halfword Direct Addressable

This control block contains the pointers to many other control blocks and contains some slowdown variables. The pointer to the HWE is at XDA + X'58'.

SYSBUFCT - constant - halfword

LOCATION: HWE + X'00' (FAX + X'5C' for NCP V6R2 and later)
DESCRIPTION: Total number of buffers in the communication controller

SYSBPQBC - constant - halfword

LOCATION: HWE + X'02' (FAX + X'60' for NCP V6R2 and later)
DESCRIPTION: Exit slowdown threshold

This is the number of free buffers needed to exit slowdown.

SYSBPBP - constant - fullword

LOCATION: HWE + X'54'
DESCRIPTION: Pointer to BPB control block

SYSNVTP - constant - fullword

LOCATION: HWE + X'60'
DESCRIPTION: Pointer to NVT control block

HWX — NCP Extension of HWE: This control block contains the pointers to many other control blocks. The pointer to the HWX is at XDA + X'5C'.

SYSVVTP - constant - fullword

LOCATION: HWX + X'28'
DESCRIPTION: Pointer to VVT control block

SYSDPTP - constant - fullword

LOCATION: HWX + X'30'
DESCRIPTION: Pointer to DPT control block

SYSCRBP - constant - fullword

LOCATION: HWX + X'34'
DESCRIPTION: Pointer to CRB control block

XDH—NCP Halfword Direct Addressable

This control block contains some slowdown constants and variables. The pointer to XDH is at X'6E4'.

NCP V6R1 and Later: The pointer to XDH is at X'34'.

SYSBPCW - constant - halfword

LOCATION: XDH + X'50'
DESCRIPTION: CWALL entry threshold

This is the number of free buffers left when NCP enters CWALL.

SYSBPGCC - variable - halfword

LOCATION: XDH + X'52' (XDA + X'08' for NCP V6R2 and later)
DESCRIPTION: Global committed buffers count

This is the total number of buffers committed to NCP lines. If this number is subtracted from the current free buffer count and the result is less than the slowdown entry threshold, then NCP is in pseudo-slowdown. If this number is subtracted from the current free buffer count and the result is less than the CWALL entry threshold, then NCP is in pseudo-CWALL.

SYSBPCBC - variable - halfword

LOCATION: XDH + X'54' (XDA + X'14' for NCP V6R2 and later)
DESCRIPTION: Current free buffer count

This number plus the system PRELEASE count is the total number of free buffers on the free-buffer pool chain. The current free buffer count is the number of buffers available for NCP processing. This represents free and not preleased buffers. When this count falls below the slowdown entry threshold, NCP enters slowdown.

SYSBPTBC - constant - halfword

LOCATION: XDH + X'56' (XDA + X'18' for NCP V6R2 and later)
DESCRIPTION: Slowdown entry threshold

This is the number of free buffers left when NCP enters slowdown.

XDB—NCP Byte Direct Addressable

This control block contains some slowdown constants and variables. The pointer to XDB starts at X'6E0'.

NCP V6R1 and Later: The pointer to XDB is at X'30'.

SYSPRELC - variable - byte

LOCATION: XDB + X'03'
DESCRIPTION: System PRELEASE count

This is the total number of buffers preleased by the current level 5 task.

SYSDSPM - variable - byte

LOCATION: XDB + X'04'
DESCRIPTION: System dispatch mask
Bit 0 on: System in CWALL
Bit 1 on: System in pseudo-slowdown

See "NCP Buffer Slowdown Mechanism" on page 346 for information on what NCP does in the CWALL and pseudo-slowdown states.

SYSBPSTS - variable - byte

LOCATION: XDB + X'09'
DESCRIPTION: Buffer pool and network status
Bit 0 on: System in slowdown
Bit 3 on: SDLC RR/RNR polling control during slowdown
Bit 4 on: SLOWDOWN ENTRY message required

See "NCP Buffer Slowdown Mechanism" on page 346 for information on what NCP does in the slowdown state.

VVT—NCP Virtual Route Vector Table

This table has a 4-byte entry for each VRB as well as the status of each VRB. The 4-byte entries start at byte 4. The last entry is delimited by a X'FFFFFFFF' The contents of each ENTRY is shown below. The pointer to the VVT is at HWX + X'28'.

VVTVRBP - constant - fullword

LOCATION: VVTENTRY + X'00'
DESCRIPTION: Pointer to VRB

These VVT entries can also be indexed by using the VVTI found in either a PIU or an RCB.

VVTFLAG - variable - byte

LOCATION: VVTENTRY + X'00'
DESCRIPTION: VVT entry status flag
Bit 0 on: VRB is assigned
Bit 0 off: VRB is available
Bit 4 on: Explicit route activation pending
Bit 5 on: Virtual route activation pending
Bit 6 on: Virtual route deactivation pending
Bit 7 on: VRB is on DACTVR queue

This is the status flag of the VRB that is pointed to by this entry.

VRB—NCP Virtual Route Block

Whenever NCP is an end point for a virtual route, a VRB exists. You can find the appropriate VRB using one of the following methods:

Find each VRB in the VVT. If this is a gateway NCP, compare VRID, the subarea on the other side of the virtual route, and the LNID.

Get the VVT index (VVTI) either from the RCB for a resource using the virtual route or from a PIU that is traveling on this virtual route. You can also find the VVTI from a PIU by using one of the following two methods:

To identify the virtual route over which the PIU arrived, use the 1-byte VVTI, which is located in the PIU buffer prefix. Subtract X'04' (1 byte) from the PIU buffer address to get the location of the 1-byte VVTI.

To identify the virtual route to which the PIU is being routed, use the 1-byte VVTI, which is located in the PIU buffer. Add X'1E' (1 byte) to the PIU buffer address to get the location of the 1-byte VVTI.

After you find the VVTI, multiply it by 4 and add it to the address of the VVT. The result is the correct VVT entry for this VRB.

The layout of the VRB is as follows:

VRBCHPF - variable - fullword

LOCATION: VRB + X'00'
DESCRIPTION: Pointer to the first RCB on the VRB

VRBCHPL - variable - fullword

LOCATION: VRB + X'04'
DESCRIPTION: Pointer to the last RCB on the VRB

VRBLNID - constant - byte

LOCATION: VRB + X'00'
DESCRIPTION: Local network ID

This is 0 for the native network or in non-GW NCPs.

VRBRECSQ - variable - halfword

LOCATION: VRB + X'08'- last 12 bits
DESCRIPTION: Next expected sequence number from received PIUs.

If NCP receives a PIU that is not the correct sequence number, it will discard it.

VRBXMTSQ - variable - halfword

LOCATION: VRB + X'0A'- last 12 bits
DESCRIPTION: Sequence number for the next PIU to be sent

VRBOSAF4 - constant - fullword

LOCATION: VRB + X'0C'
DESCRIPTION: Subarea on the other end of the virtual route

VRBTGBP - constant - fullword

LOCATION: VRB + X'10'
DESCRIPTION: Pointer to the TGB for this virtual route

VRBFCFLG - variable - byte

LOCATION: VRB + X'14'
DESCRIPTION: Virtual route status flags
t
Bit 0 on: Send VRPRS
Bit 1 on: VRPRS received
Bit 2 on: VRPRQ received
Bit 3 on: Virtual route held
Bit 4 on: Notify blocked tasks
Bit 5 on: Set CWRI on next VRPRS
Bit 6 on: Withholding VRPRS
Bit 7 on: Set RWI on next PIU sent

Check these bits for virtual route status. For more information about these bits, see "Network Flow Control Mechanisms" on page 343 and "Local Flow Control Mechanisms" on page 346.

VRBFLAGS - variable - byte

LOCATION: VRB + X'15'

DESCRIPTION: Virtual route status flags
Bit 0 on: Virtual route inoperative
Bit 2 on: Session outage notification triggered
Bit 3 on: Internal virtual route
Bit 4 on: Virtual route deactivation responsibility
Bit 6 on: Virtual route out of sequence (discarding PIUs)

Check these bits for virtual route status. For more information about these bits, see "Network Flow Control Mechanisms" on page 343 and "Local Flow Control Mechanisms" on page 346.

VRBPIUCT - variable - halfword

LOCATION: VRB + X'16'
DESCRIPTION: Number of buffers allocated to this virtual route

VRBVRID - constant - byte

LOCATION: VRB + X'19'
DESCRIPTION: VRID - Virtual route number and transmission priority
Bits 0-3: Virtual route number
Bits 6-7: Transmission priority

VRBXMTQC - variable - halfword

LOCATION: VRB + X'1A'
DESCRIPTION: Number of PIUs on virtual route transmit queue

VRBMWIND - constant - byte

LOCATION: VRB + X'1C'
DESCRIPTION: Virtual route maximum window size

VRBWIND - variable - byte

LOCATION: VRB + X'1D'
DESCRIPTION: Virtual route current window size

VRBWCNT - variable - byte

LOCATION: VRB + X'1E'
DESCRIPTION: Virtual route window count

VRBINOPC - variable - byte

LOCATION: VRB + X'1F'
DESCRIPTION: Virtual route INOP code
X'07'- Explicit route INOP
X'0B'- DACTVR

VRX1ECB - variable - fullword

LOCATION: VRB + X'20'
DESCRIPTION: Pointer to the first PIU on virtual route transmit queue

VRXLECB - variable - fullword

LOCATION: VRB + X'24'
DESCRIPTION: Pointer to the last PIU on virtual route transmit queue

VRW1ECB - variable - fullword

LOCATION: VRB + X'38'
DESCRIPTION: Pointer to the first ECB on virtual route wake-up queue

VRWLECB - variable - fullword

LOCATION: VRB + X'3C'
DESCRIPTION: Pointer to the last ECB on virtual route wake-up queue

VRBVVTI - constant - halfword

LOCATION: VRB + X'50'
DESCRIPTION: VVT index

VRBLWIND - constant - byte

LOCATION: VRB + X'53'
DESCRIPTION: Virtual route minimum window size

VRBFTHRS - constant - halfword

LOCATION: VRB + X'54'
DESCRIPTION: Virtual route Inbound PIU threshold

VRBFCNT - variable - halfword

LOCATION: VRB + X'56'
DESCRIPTION: Virtual route Inbound PIU count

BPB—NCP Boundary Pool Block

This control block contains all the information about NCP's destination boundary pool. The pointer to the BPB is at HWE + X'54'.

BPBSIZE - constant - halfword

LOCATION: BPB + X'00'
DESCRIPTION: Number of buffers in the BPOOL

BPBCNT - variable - halfword

LOCATION: BPB + X'02'
DESCRIPTION: Number of buffers allocated to the BPOOL

BPBTHRS1 - constant - halfword

LOCATION: BPB + X'04'
DESCRIPTION: BPOOL 62.5% threshold

BPBTHRS2 - constant - halfword

LOCATION: BPB + X'06'
DESCRIPTION: BPOOL 75% threshold

BPBTHRS3 - constant - halfword

LOCATION: BPB + X'08'
DESCRIPTION: BPOOL 87.5% threshold

BPBFLAGS - variable - byte

LOCATION: BPB + X'0A'
DESCRIPTION: BPOOL status flags
Bit 0 on: Set RWI for low priority virtual routes
Bit 1 on: Set RWI for medium priority virtual routes
Bit 2 on: Set RWI for high priority virtual routes
Bit 3 on: BPOOL FULL - withhold VRPRS

TGB—NCP Transmission Group Control Block

This control block contains the information related to the transmission group associated with a particular channel or link. The pointer to the TGB is at VRB + X'10'.

TGBDLCP - constant - fullword

LOCATION: TGB + X'10'
DESCRIPTION: Pointer to the DLC block

This DLC block can be either a CAB, SCB, or FLB

TGBNUM - constant - byte

LOCATION: TGB + X'10'
DESCRIPTION: Transmission group number

TGBSUBA - constant - fullword

LOCATION: TGB + X'14'
DESCRIPTION: Subarea address of adjacent node connected to the transmission group

TGBTCNT - variable - fullword

LOCATION: TGB + X'18'
DESCRIPTION: Total inbound byte count

TGBHCNT - variable - fullword

LOCATION: TGB + X'1C'
DESCRIPTION: High-priority inbound-byte count

TGBSTATE - variable - byte

LOCATION: TGB + X'1C'
DESCRIPTION: TG state definitions

See *NCP and EP Reference Summary and Data Areas*, Volume 1, for state definitions.

TGBMCNT - variable - fullword

LOCATION: TGB + X'20'
DESCRIPTION: Medium-priority inbound-byte count

TGBLCNT - variable - fullword

LOCATION: TGB + X'24'
DESCRIPTION: Low-priority inbound-byte count

TGBTTHR - constant - fullword

LOCATION: TGB + X'28'
DESCRIPTION: Total byte-count threshold

TGBHTHR - constant - fullword

LOCATION: TGB + X'2C'
DESCRIPTION: High-priority byte-count threshold

TGBMTHR - constant - fullword

LOCATION: TGB + X'30'
DESCRIPTION: Medium-priority byte-count threshold

TGBLTHR - constant - fullword

LOCATION: TGB + X'34'
DESCRIPTION: Low-priority byte-count threshold

TGBLNID - constant - byte

LOCATION: TGB + X'3C'
DESCRIPTION: Local network ID

FLB—NCP Multilink Transmission Group Control Block

This control block contains the information for controlling traffic on a multilink transmission group (TG). The pointer to the FLB is at TGB + X'10'.

FLBRQCB - variable - fullword

LOCATION: FLB + X'00'
DESCRIPTION: Head pointer for resequence queue

FLBRQCB - variable - fullword

LOCATION: FLB + X'04'
DESCRIPTION: Tail pointer for resequence queue

FLBXQCB - variable - fullword

LOCATION: FLB + X'18'
DESCRIPTION: Head pointer for transmit queue

FLBXQCB - variable - fullword

LOCATION: FLB + X'1C'
DESCRIPTION: Tail pointer for transmit queue

FLBTGBP - constant - fullword

LOCATION: FLB + X'28'
DESCRIPTION: Pointer to the TGB

FLBSOC - variable - byte

LOCATION: FLB + X'28'
DESCRIPTION: Station operative count

FLBSCBP - constant - fullword

LOCATION: FLB + X'2C'
DESCRIPTION: Pointer to the first SCB

FLBSTF - variable - byte

LOCATION: FLB + X'32'
DESCRIPTION: State flags
Bit 2 on: TG in sweep mode
Bit 3 on: Special FIDF PIU expected

FLBNRO - variable - halfword

LOCATION: FLB + X'34'
DESCRIPTION: Next sequence number for outbound PIUs

Only last 12 bits.

FLBNRI - variable - halfword

LOCATION: FLB + X'36'
DESCRIPTION: Next expected sequence number from inbound PIUs

Only last 12 bits; if bit 3 is on, roll-over is occurring.

FLBSTFC - variable - byte

LOCATION: FLB + X'41'
DESCRIPTION: State flags
Bit 1 on: TG out of sequence

SCB—NCP Station Control Block

This control block contains the queues, status, and scheduling information for subarea node station control. The pointer to the SCB is at FLB + X'2C'. It is also pointed to by an entry in the RVT.

SCB1ECB - variable - fullword

LOCATION: SCB + X'00'
DESCRIPTION: Head pointer for link-inbound queue

SCBLECB - variable - fullword

LOCATION: SCB + X'04'
DESCRIPTION: Tail pointer for link-inbound queue

SCBLOBH - variable - fullword

LOCATION: SCB + X'18'
DESCRIPTION: Head pointer for link-outbound queue

SCBEERS - variable - byte

LOCATION: SCB + X'18'
DESCRIPTION: Extended retry status

SCBLOBT - variable - fullword

LOCATION: SCB + X'1C'
DESCRIPTION: Tail pointer for link-outbound queue

SCBLOSH - variable - fullword

LOCATION: SCB + X'20'
DESCRIPTION: Head pointer for link-outstanding queue

SCBNRA - variable - byte

LOCATION: SCB + X'20'
DESCRIPTION: Number of PIUs requiring acknowledgement

SCBLOST - variable - fullword

LOCATION: SCB + X'24'
DESCRIPTION: Tail pointer for link-outstanding queue

SCBLKB - constant - fullword

LOCATION: SCB + X'28'
DESCRIPTION: Pointer to link control block (LKB)

SCBADRC - constant - halfword

LOCATION: SCB + X'2C'
DESCRIPTION: Element address of physical unit

SCBSSCF - variable - halfword

LOCATION: SCB + X'2E'
DESCRIPTION: Station state definitions

See *NCP and EP Reference Summary and Data Areas*, Volume 1, for state definitions.

SCBSTATS - variable - byte

LOCATION: SCB + X'30'
DESCRIPTION: Station status
Bit 2 on: Station quiesce pending
Bit 5 on: COMMIT in progress for this station
Bit 6 on: One or more SDLC error record counters has reached its limit

See *NCP and EP Reference Summary and Data Areas*, Volume 1, for more bit definitions.

SCBOCF - variable - byte

LOCATION: SCB + X'31'
DESCRIPTION: Station service seeking output control flags
Bit 0 on: Output skip bit
Bit 2 on: RNR received
Bit 3 on: Second level ERP pause in progress
Bit 6 on: RNR re-poll

See *NCP and EP Reference Summary and Data Areas*, Volume 1, for more bit definitions.

SCBERS - variable - halfword

LOCATION: SCB + X'3A'
DESCRIPTION: First error encountered

SCBRTCNT - variable - halfword

LOCATION: SCB + X'3C'
DESCRIPTION: ERP retry counts

SCBOCL - variable - halfword

LOCATION: SCB + X'3E'
DESCRIPTION: Outstanding count limit and count

SCBSRTLR - constant - byte

LOCATION: SCB + X'40'
DESCRIPTION: Second-level retry limit

SCB2ERPT - constant - halfword

LOCATION: SCB + X'42'
DESCRIPTION: Second-level ERP timeout value

SCBTERR - variable - byte

LOCATION: SCB + X'44'
DESCRIPTION: Monitor station error count

SCBERPT - constant - byte

LOCATION: SCB + X'45'
DESCRIPTION: Second-level ERP pause

SCBTRTCT - variable - halfword

LOCATION: SCB + X'48'
DESCRIPTION: Total retry counter

SCBRECNT - variable - halfword

LOCATION: SCB + X'4A'
DESCRIPTION: Receive I-format error counter

SCBTINCT - variable - halfword

LOCATION: SCB + X'56'
DESCRIPTION: Total I-format retransmission counter

SCBSRTR - variable - halfword

LOCATION: SCB + X'5A'
DESCRIPTION: Total retries threshold value

SCBCBBP - constant - fullword

LOCATION: SCB + X'60'
DESCRIPTION: Pointer to committed buffers block (CBB)

SCBTGBP - constant - fullword

LOCATION (NCP V4R1 (VSE) and NCP V4R2):
SCB + X'68'
LOCATION (NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4, and NCP V6R1 and later):
SCB + X'6C'
DESCRIPTION: Pointer to TGB

SCBFLPF - variable - fullword

LOCATION (NCP V4R1 (VSE) and NCP V4R2):
SCB + X'6C'
LOCATION (NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4, and NCP V6R1 and later):
SCB + X'74'
DESCRIPTION: Chain pointer to next SCB on FLB

SCBCSCF - variable - byte

LOCATION: SCB + X'70'
DESCRIPTION: Configurable station control flags

SCBFLST - variable - byte

LOCATION: SCB + X'71'
DESCRIPTION: Status of multilink TG
Bit 0 on: Station ready to send

See *NCP and EP Reference Summary and Data Areas*, Volume 1, for state definitions.

CBB—NCP Committed Buffers Block

This control block maintains buffer commitment status on SDLC stations and pre-SNA lines. The pointer to the CBB is at LCB + X'58' for BSC and start-stop lines. The pointer to the LCB is in the RVT control block, indexed using the element address of the link. The pointer to the CBB is at SCB + X'60' or CUB + X'60' for SDLC stations. The pointer to the SCB or CUB is in the RVT control block, indexed using the element address of the physical unit.

CBBACBP - constant - fullword

LOCATION: CBB + X'00'
DESCRIPTION: Pointer to the associated ACB

CBBFLGS - variable - byte

LOCATION: CBB + X'00'
DESCRIPTION: Committed-buffers flag
Bit 0 on: No polling
Bit 0 off: Poll requested

CBBCURC - variable - halfword

LOCATION: CBB + X'04'
DESCRIPTION: Current commitment

CBBMAXC - variable - halfword

LOCATION: CBB + X'06'
DESCRIPTION: Maximum commitment

CBBMINC - variable - halfword

LOCATION: CBB + X'08'
DESCRIPTION: Minimum commitment

CBBRBC - variable - halfword

LOCATION: CBB + X'0A'
DESCRIPTION: Receive buffer count

CBBRESP - constant - fullword

LOCATION: CBB + X'0C'
DESCRIPTION: Pointer to the associated SCB, CUB, or LCB

CBBRNRC - variable - halfword

LOCATION: CBB + X'10'
DESCRIPTION: RNR poll count

NVT—NCP Network Vector Table

This control block contains the parameters unique to a particular network in NCP. Entries for each network in NCP start at offset 8 into this control block. Each entry is X'2C' long. The pertinent fields in each entry are given below. The pointer to the NVT is at HWE + X'60'.

NVTNWID - constant - 2 fullwords

LOCATION: NVT ENTRY + X'00'
DESCRIPTION: Network ID

NVTSUBA - constant - fullword

LOCATION: NVT ENTRY + X'0C'
DESCRIPTION: NCP subarea in this network

NVTLNID - constant - byte

LOCATION: NVT ENTRY + X'10'
DESCRIPTION: Local network ID

NVTRVTP - constant - fullword

LOCATION: NVT ENTRY + X'14'
DESCRIPTION: Pointer to RVT for this network

RVT—NCP Resource Vector Table

This control block is the master directory to all the resource control blocks (lines, physical units, logical units, and so on) for a particular network in NCP. There is an 8-byte entry for every resource in this network.

See *NCP and EP Reference Summary and Data Areas*, Volume 1, for details.

NCP V4R3.1 for IBM 3725; NCP V5R3 (VSE) and NCP V5R4 for IBM 3720 or 3745; NCP V6R1 and later for IBM 3745: the pointer to the RVT is in the NVT entry for the given network at NVT ENTRY + X'14'. To obtain the pointer to the entry for the resource:

1. Multiply the element address of the resource by 8
2. Add the result to the pointer in the NVT
3. Add 4.

The pointer in the NVT points to the 4-byte RVT prefix.

RVTTYPE - constant - 2 bytes

LOCATION: RVT ENTRY + X'00'
DESCRIPTION: Resource type

RVTRP - constant - fullword

LOCATION: RVT ENTRY + X'04'
DESCRIPTION: Pointer to the resource control block

This resource control block can be either a PSB, LCB, DVB, LKB, CUB, SCB, LUB, VLB, NPB, NLB, or LRB.

For NCP V7R1 and later: Check if the resource was created dynamically or non-dynamically. Check if the element address is in the range of the RVT by looking at the first 2 bytes of the RVT prefix. If it is less than or equal to the range, it was created non-dynamically. If it is greater than the range, it was created dynamically.

For non-dynamic, to obtain the pointer to the entry for the resource, you:

1. Multiply the element address of the resource by 8
2. Add the result to the pointer in the NVT. The pointer in the NVT ENTRY + X'14' points to the 4-byte RVT prefix.
3. Add 4.

RVTTYPE - constant - 2 bytes

LOCATION: RVT ENTRY + X'00'

DESCRIPTION: Resource type

RVTRP - constant - fullword

LOCATION: RVT ENTRY + X'04'
DESCRIPTION: Pointer to the resource control block

For dynamic, you need to find the RVB for the network. The RVB pointer is at NVT ENTRY + X'24'.

To find the particular RVT entry that goes with the element address, you have two options:

1. Using the RVB AABs chain. The RVB AAB is a linked list of RVT entries that are in element address order. The AAB is at offset X'08' of the RVB. The chain pointer between RVT entries is at offset X'08' of the RVT entry.
2. Using the SHB in the RVB. The RVB SHB is the head block of a binary search tree that uses the element address as the search key.

RVTTYPE - constant - 2 bytes

LOCATION: RVT ENTRY + X'00'
DESCRIPTION: Resource type

RVTRP - constant - fullword

LOCATION: RVT ENTRY + X'04'
DESCRIPTION: Pointer to the resource control block

Note: If you cannot locate the element address, it means the resource is not in use and you cannot see the control blocks.

This resource control block can be a PSB, LCB, DVB, LKB, CUB, SCB, LUB, VLB, NPB, NLB, or LRB.

RCB—NCP Resource

Connection Block

An RCB is associated with every network resource that can participate in a session. It contains routing and flow control information. When a network resource is associated with a virtual route, its RCB is chained to the VRB. Use the RCB to find the virtual route associated with a particular network. To find an RCB for a given resource, you must first know the element address of the resource. See "Obtaining Network Flow Control Information" on page 115 for information on obtaining the element address of a resource. For independent logical units and cross-network resources, you must also know the name of the resource with which the logical unit is in session. For a specific resource type, you can find the RCB as follows:

Note: The following examples use the RVT control block listed above.

BSC or SS terminal:

Using the element address, find the address of the DVB in the RVT entry for the terminal. The 1-byte offset to the RCB is at DVB + X'3E'. Add the offset to the address found in the RVT entry to obtain the starting address of the RCB.

SNA physical unit (NCP V4R1 (VSE) and NCP V4R2 for IBM 3725; NCP V4R1 (VSE) and NCP V4R2 for IBM 3720):

Using the element address, find the address of the CUB in the RVT entry for the physical unit. The 1-byte offset to the RCB is at CUB + X'74'. Add the offset to the address found in the RVT entry to obtain the starting address of the RCB.

SNA logical unit (NCP V4R1 (VSE) and V4R2 for IBM 3725; NCP V4R1 (VSE) and NCP V4R2 for IBM 3720):

Using the element address, find the address of the LUB in the RVT entry for the logical unit. The 1-byte offset to the RCB is at LUB + X'54'. Add the offset to the address found in the RVT entry to obtain the starting address of the RCB.

SNA physical unit (NCP V4R3.1 for IBM 3725; NCP V5R3 (VSE) and NCP V5R4 for IBM 3720 or 3745; NCP V6R1 and V6R2 for IBM 3745):

Using the element address, find the address of the CUB in the RVT entry for the physical unit. The starting address of the RCB is at CUB + X'BC'.

SNA physical unit with NCP V7R1:

Using the element address, find the address of the CUB in the RVT entry for the physical unit. The starting address of the RCB is at CXI + X'54'. To find the CXI you must start at the CUB.

Start at the CUB. The CXB pointer is at X'64' into the CUB. The CXI pointer is at offset X'78' in the CXB. The RCB is CXI + X'54'. (In other words, take the address of the CXI and add X'54'.)

SNA logical unit (dependent logical unit with NCP V4R3.1 for IBM 3725; NCP V5R3 (VSE) and NCP V5R4 for IBM 3720 or 3745; NCP V6R1 and later for IBM 3745):

Using the element address, find the address of the LRB in the RVT entry for the logical unit. The LRB is embedded in the LNB control block. For each dependent logical unit, there is only one LNB. Dependent logical units can only have one LU-LU session. Find the RCB for this session embedded in the BSB for this session. The pointer to this BSB is at a negative offset from the LRB address found in the RVT, LRB - X'08'. The starting address of the RCB is BSB + X'48'.

SNA logical unit (dependent logical unit with NCP V7R1 and later):

Using the element address, find the address of the LRB in the RVT entry for the logical unit. The LRB is embedded in the LNB control block. For each dependent logical unit, there is only one LNB. Dependent logical units can only have one LU-LU session. Find the RCB for this session embedded in the LU-LU BSB for this session. The pointer to this BSB is at a negative offset from the LRB address found in the RVT, LRB - X'0C'. The starting address of the RCB is BSB + X'48'.

SNA logical unit (independent logical unit with NCP V4R3.1 for IBM 3725; NCP V5R3 (VSE) and NCP V5R4 for IBM 3720 or 3745; NCP V6R1 and later for IBM 3745):

Using the element address, find the address of the LRB in the RVT entry for the logical unit. The LRB is embedded in the LNB control block. For each independent logical unit, there can be many LNBs. Each has its own network addresses. An LNB may also be involved in many sessions, each having a BSB. Find the RCBs for these sessions embedded in the BSBs. The pointer to the first BSB in the LNB is at a negative offset from the LRB address found in the RVT, LRB - X'08'. LRB - X'0C'.

To determine if this is the correct BSB, find the name of the logical unit's partner in this session. Find this in the BXI. The 1-byte offset to the BXI is at BSB + X'2B'. Add this offset to the address of the BSB to obtain the address of the BXI. Eight bytes containing the session partner name are at BXI + X'2C'. If this is not the correct session partner, try another BSB. The pointer to the next BSB is in the current BSB, at BSB + X'18'. When you locate the correct BSB, the starting address of the RCB is BSB + X'48'.

SNA logical unit (independent logical unit with NCP V7R1):

Using the element address, find the address of the LRB in the RVT entry for the logical unit. The LRB is embedded in the LNB control block. For each independent logical unit, there can be many LNBs. Each has its own network addresses. An LNB may also be involved in many sessions, each having a BSB. Find the RCBs for these sessions embedded in the BSBs. The pointer to the first BSB in the LNB is at a negative offset from the LRB address found in the RVT, LRB - X'0C'.

To determine if this is the correct BSB, find the name of the logical unit's partner in this session. You can find the session partner in the BXI. See "BXI—Boundary Session Block Extension" on page 383 to find the BXI. Eight bytes containing the session partner name are at BXI + X'2C'. If this is not the correct session partner, try another BSB. The pointer to the next BSB is in the current BSB, at BSB + X'18'. When you locate the correct BSB, the starting address of the RCB is BSB + X'48'.

SNA Cross Network Resources:

Using the element address, find the address of the NLB in the RVT entry for the cross network logical unit or SSCP. There are two RCBs for this cross network resource's session, one for each network. These RCBs are not associated with the current NLB, but with NLX control blocks. For every session in which this cross network resource participates, there is an NLX control block. To find the correct NLX, find the NIB and the correct NIX control blocks. The pointer to the NIB is at NLB + X'28'. The pointer to the first NIX for this NIB is at NIB + X'18'. In the NIX there is an 8-byte name of the session partner for this resource, at NIX + X'0C'. If this is not the correct name of the session partner, then try the next NIX. Each NIX in the chain points to the next NIX at NIX + X'00'. When you find the correct NIX, find the pointer to the correct NLX at NIX + X'14'. Find the RCB for this NLX at a 1-byte offset of + X'23'. Add this offset to the starting address of the NLX to obtain the starting address of the RCB.

RCBAEBCP - variable - fullword

LOCATION: RCB + X'00'
DESCRIPTION: Pointer to the next RCB on the VRB

RCBAEBFG - variable - byte

LOCATION: RCB + X'00'
DESCRIPTION: RCB AEB flag
Bit 0 on: RCB in chain

RCBIEBCP - variable - fullword

LOCATION: RCB + X'04'
DESCRIPTION: Pointer to the next ECB on the VRB

RCBVRAL - variable - fullword

LOCATION: RCB + X'08'
DESCRIPTION: Pointer to the virtual route activation work list

RCBCSTAT - variable - byte

LOCATION: RCB + X'08'
DESCRIPTION: RCB CSTAT flags
Bit 0 on: ECB on a chain

RCBZQCBP - variable - fullword

LOCATION: RCB + X'0C'
DESCRIPTION: Pointer to release held task QCB

RCBIMTSK - variable - fullword

LOCATION: RCB + X'10'
DESCRIPTION: Pointer to the held immediate task

RCBFLAGS - variable - byte

LOCATION: RCB + X'10'
DESCRIPTION: RCB flags
Bit 0 on: Branch to immediate routine
Bit 2 on: RCB counted in VRB threshold

RCBVVT - constant - halfword

LOCATION (NCP V4R1 (VSE) and NCP V4R2 for IBM 3725; NCP V4R1 (VSE) and NCP V4R2 for IBM 3720):
RCB + X'16'
LOCATION (NCP V4R3.1, NCP V5R3 (VSE), NCP V5R4, and NCP V6R1 and later):
RCB + X'18'
DESCRIPTION: VVTI - Index into the VVT to find the VRB

BXI—Boundary Session Block Extension

This section applies to NCP V7R1 and later.

The BXI contains additional data for an LU-LU session and is obtainable from the BSB. For NCP V7R1, it is more complex getting from the BXI to the BSB.

First, check if you have a dynamic BSB or a non-dynamic BSB by finding X'2D' bit 7 in the BSB. If bit 7 is on, you have a dynamic BSB. If bit 7 is off, you have a non-dynamic BSB.

For non-dynamic:

The 1 byte offset to the BXI is at BSB + X'2B'. Add this offset to the address of the BSB to obtain the address of the BXI.

For dynamic:

Determine if it is an independent or dependent LU-LU BSB. In the BSB check X'2B' bit 0. If bit 0 is off, you have an independent LU-LU BSB. If bit 0 is on, you have a dependent LU-LU BSB.

Independent LU; BSB + X'6C' is a pointer to the BXI.

Dependent LU; BSB + X'64' is a pointer to the BXI.

VRBLK—VTAM Virtual Route Control Block

This is the only VTAM control block that is listed in this section. Check this control block to determine VTAM's virtual route status. VTAM has a control block for every virtual route ending in its node. This control block contains the status for each of the transmission priorities for this virtual route number.

VRBVRN - constant - byte

LOCATION: VRBLK + X'02'
DESCRIPTION: Virtual route number

VRBRHOLD - variable - fullword

LOCATION: VRBLK + X'48'
DESCRIPTION: Virtual route hold queue pointer for TP=0

VRBPACNT - variable - halfword

LOCATION: VRBLK + X'56'
DESCRIPTION: Virtual route window count for TP=0

VRBMINWS - constant - byte

LOCATION: VRBLK + X'58'
DESCRIPTION: Virtual route minimum window size for TP=0

VRBMAXWS - constant - byte

LOCATION: VRBLK + X'59'
DESCRIPTION: Virtual route maximum window size for TP=0

VR status - variable - byte

LOCATION: VRBLK + X'5C'
DESCRIPTION: Virtual route status byte for TP=0
Bit 1 on: VRPRQ (Virtual route pacing request received)
Bit 2 on: VRPRS (Virtual route pacing response received)
Bit 3 on: CWI (Change window indicator received)
Bit 4 on: CWRI (Change window reset required)
Bit 5 on: RWI (Reset window required)
Bit 6 on: Virtual route held
Bit 7 on: Some half session queues must be checked for held sessions

VRBRHOLD - variable - fullword

LOCATION: VRBLK + X'68'
DESCRIPTION: Virtual route hold queue pointer for TP=1

VRBPACNT - variable - halfword

LOCATION: VRBLK + X'76'
DESCRIPTION: Virtual route window count for TP=1

VRBMINWS - constant - byte

LOCATION: VRBLK + X'78'
DESCRIPTION: Virtual route minimum window size for TP=1

VRBMAXWS - constant - byte

LOCATION: VRBLK + X'79'
DESCRIPTION: Virtual route maximum window size for TP=1

Virtual route status - variable - byte

LOCATION: VRBLK + X'7C'
DESCRIPTION: Virtual route status byte for TP=1
Bit 1 on: VRPRQ (Virtual route pacing request received)
Bit 2 on: VRPRS (Virtual route pacing response received)
Bit 3 on: CWI (Change window indicator received)
Bit 4 on: CWRI (Change window reset required)
Bit 5 on: RWI (Reset window required)
Bit 6 on: Virtual route held
Bit 7 on: Some half session queues must be checked for held sessions

VRBRHOLD - variable - fullword

LOCATION: VRBLK + X'88'
DESCRIPTION: Virtual route hold queue pointer for TP=2

VRBPACNT - variable - halfword

LOCATION: VRBLK + X'96'
DESCRIPTION: Virtual route window count for TP=2

VRBMINWS - constant - byte

LOCATION: VRBLK + X'98'
DESCRIPTION: Virtual route minimum window size for TP=2

VRBMAXWS - constant - byte

LOCATION: VRBLK + X'99'
DESCRIPTION: Virtual route maximum window size for TP=2

VR status - variable - byte

LOCATION: VRBLK + X'9C'
DESCRIPTION: Virtual route status byte for TP=2
- Bit 1 on: VRPRQ (Virtual route pacing request received)
- Bit 2 on: VRPRS (Virtual route pacing response received)
- Bit 3 on: CWI (Change window indicator received)
- Bit 4 on: CWRI (Change window reset required)
- Bit 5 on: RWI (Reset window required)
- Bit 6 on: Virtual route held
- Bit 7 on: Some half session queues must be checked for held sessions

VRBDSTSA - constant - fullword

LOCATION: VRBLK + X'A4'
DESCRIPTION: Subarea of the other end of the VR.

Appendix B. Maintaining SSP Utilities

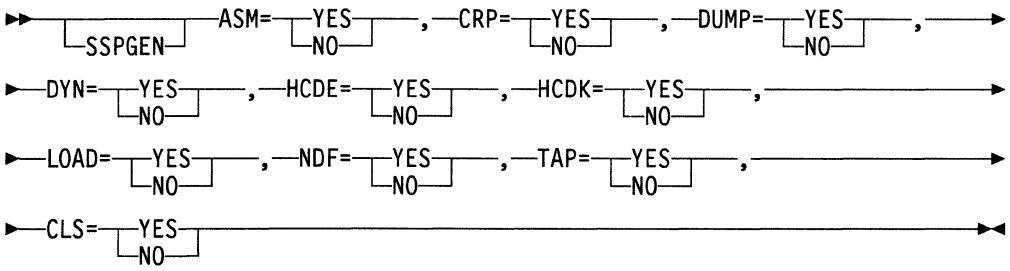
The SSPGEN macro enables you to install and maintain updates to SSP under MVS. It creates the job control and link-edit statements needed by the system to link-edit specified portions of the SSP utilities into the system. Use SSPGEN when maintenance procedures require a definition of the link-edit job.

Please note the following:

- VM and VSE do not use SSPGEN. The SSPGEN macro is valid only for MVS.
- The SSPGEN macro is not a resource definition statement like BUILD or GROUP.

SSPGEN Macro Format

The format of the SSPGEN macro is:



ASM
Specifies whether you include link-edit statements for the CWAX assembler utility. Use the assembler only if you intend to develop user-written code to run in the controller. If you omit this keyword, ASM=NO is assumed.

CRP
Specifies whether you include link-edit statements for the configuration report program. If you omit this keyword, CRP=NO is assumed.

DUMP
Specifies whether you include link-edit statements for the independent dump utility. If you omit this keyword, DUMP=NO is assumed.

DYN
Specifies whether you include link-edit statements for the dynamic dump utility. If you omit this keyword, DYN=NO is assumed.

HCDE
Specifies whether you include link-edit statements for the English version of the SSP HCD support. If you omit this keyword, HCDE=NO is assumed.

HCDK
Specifies whether you include link-edit statements for the Kanji version of the SSP HCD support. If you omit this keyword, HCDK=NO is assumed.

LOAD
Specifies whether you include link-edit statements for the SSP loader utility. If you omit this keyword, LOAD=NO is assumed.

NDF
Specifies whether you include link-edit statements for the NCP/EP definition facility. If you omit this keyword, NDF=NO is assumed.

TAP
Specifies whether you include link-edit statements for ACF/TAP. If you omit this keyword, TAP=NO is assumed.

CLS
Specifies whether you include link-edit statements for SSP CLISTs. If you omit this keyword, CLS=NO is assumed.

Input to the SSPGEN Macro

The SSPGEN macro can be called by any of the system assemblers. The following example shows job control statements needed to call the SSPGEN macro to generate link-edit control statements for the assembler utility, trace analysis program, independent dump utility, and dynamic dump utility:

```
//SSPGEN   JOB     MSGLEVEL=1
//STP1     EXEC    PGM=IFOX00,PARM='DECK'
            .
            .
            .
   (JCL statements for assembler)
            .
            .
            .
//SYSIN    DD      *
INPUT       SSPGEN  ASM=YES,TAP=YES,DUMP=YES,DYN=YES
            END
/*
```

Output from the SSPGEN Macro

The output from running the SSPGEN macro consists of the job control and link-edit statements needed for linking the particular utilities specified. You can produce this output as a job or as data for the maintenance process. Following is an example of the output from the SSPGEN macro:

```
//SSPLINK   JOB      SSPINST,MSGLEVEL=1
//LINK      EXEC     PGM=IEWL,
//                   PARM='XREF,LET,NCAL,LIST,DC,
//                   SIZE=(200K,24K)'
            .
            .
            .
   (JCL in this job stream may require modification
   to meet individual installation requirements)
            .
            .
            .
//SYSPRINT  DD       SYSOUT=A
//SYSUT1    DD       UNIT=SYSDA,SPACE=(1024,(200,20))
//SSPOBJ    DD       DSN=SYS1.SSPOBJ,DISP=SHR
//SYSLMOD   DD       DSN=SYS1.SSPLIB,DISP=SHR
//SYSLIN    DD       *
            INCLUDE  SSPOBJ(CWAX0A,CWAX0B)
            ENTRY    CWAX0A01
            NAME     CWAX00(R)
            .
            .
            .
   (Additional link-edit control statements for all
   modules as required.)
            .
            .
            .
/*
```

Glossary, Bibliography, and Index

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology*. Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The Network Working Group Request for Comments: 1208.

The following cross-references are used in this glossary:

Contrast with: This refers to a term that has an opposed or substantively different meaning.

Synonym for: This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with: This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also: This refers the reader to terms that have a related, but not synonymous, meaning.

Deprecated term for: This indicates that the term should not be used. It refers to a preferred term, which is defined in its proper place in the glossary.

A

abend. (1) Abnormal end of task. (2) Synonym for *abnormal termination.*

ACB. (1) In VTAM, access method control block. (2) In NCP, adapter control block. (3) Application control block.

access method. (1) A technique, implemented in software, that controls the flow of information through a network. (2) A technique for moving data between main storage and input/output devices.

access method control block (ACB). A control block that links an application program to VTAM.

ACF. Advanced Communications Function.

ACF/TAP. Advanced Communications Function/Trace Analysis Program. Synonymous with *TAP.*

ACF/TCAM. Advanced Communications Function for the Telecommunications Access Method. Synonym for *TCAM.*

ACF/VTAM. Advanced Communications Function for the Virtual Telecommunications Access Method. Synonym for *VTAM.*

activate. To make a resource ready to perform its function. Contrast with *deactivate.*

active gateway. A gateway that is treated like a network interface in that it is expected to exchange routing information. If it does not do so for a period of time, the route associated with the gateway is deleted.

ACTLU. Activate logical unit. In SNA, a command used to start a session on a logical unit.

ACTPU. Activate physical unit. In SNA, a command used to start a session on a physical unit.

adapter. A part that electrically or physically connects a device to a computer or to another device.

adapter control block (ACB). In NCP, a control block that contains line control information and the states of I/O operations for BSC lines, SS lines, or SDLC links.

Address Resolution Protocol (ARP). A protocol that dynamically maps between Internet addresses, baseband adapter addresses, X.25 addresses, and token-ring adapter addresses on a local area network.

address space manager (ASM). A component in an APPN or LEN node that assigns and frees session addresses.

addressing. (1) The assignment of addresses to the instructions of a program. (2) A means of identifying storage locations. (3) In data communication, the way in which a station selects the station to which it is to send data. (4) Specifying an address or location within a file.

adjacent link station (ALS). (1) In SNA, a link station directly connected to a given node by a link connection over which network traffic can be carried.

Note: Several secondary link stations that share a link connection do not exchange data with each other and therefore are not adjacent to each other. (2) With respect to a specific node, a link station partner in an adjacent node.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Advanced Communications Function (ACF). A group of IBM licensed programs, principally VTAM, TCAM, NCP, and SSP, that use the concepts of Systems Network Architecture (SNA), including distribution of function and resource sharing.

Advanced Communications Function/Trace Analysis Program (ACF/TAP). An SSP program service aid that assists in analyzing trace data produced by VTAM, TCAM, and NCP and provides network data traffic and network error reports. Synonymous with *Trace Analysis Program (TAP).*

Advanced Peer-to-Peer Networking (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

Advanced Peer-to-Peer Networking (APPN) network. A collection of interconnected network nodes and their client end nodes.

Advanced Peer-to-Peer Networking (APPN) network node. A node that offers a broad range of end-user services and that can provide the following:

- Distributed directory services, including registration of its domain resources to a central directory server
- Topology database exchanges with other APPN network nodes, enabling network nodes throughout the network to select optimal routes for LU-LU sessions based on requested classes of service
- Session services for its local LUs and client end nodes
- Intermediate routing services within an APPN network

Advanced Peer-to-Peer Networking (APPN) node. An APPN network node or an APPN end node.

AIX. Advanced Interactive Executive.

AIX operating system. IBM's implementation of the UNIX operating system. The RISC System/6000 system, among others, runs the AIX operating system.

alert. (1) A message sent to a management services focal point in a network to identify a problem or an impending problem. (2) In the NetView and NETCENTER programs, a high priority event that warrants immediate attention.

allocate. A logical unit (LU) 6.2 application program interface (API) verb used to assign a session to a conversation for the conversation's use. Contrast with *deallocate.*

ALS. Adjacent link station.

APAR. Authorized program analysis report.

application control block (ACB). The control blocks created from the output of DBDGEN and PSBGEN and placed in the ACB library for use during online and DBB region type execution of IMS/VS.

application program interface (API). (1) A functional interface supplied by the operating system or by a separately orderable licensed program that allows an application program written in a high-level language to use specific data or functions of the operating system or the licensed program. (2) The interface through which an application program interacts with an access method. In VTAM, it is the language structure used in control blocks so that application programs can reference them and be identified to VTAM.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

ARP. Address Resolution Protocol.

ASCII (American Standard Code for Information Interchange). The standard code, using a coded char-

acter set consisting of 7-bit coded characters (8-bit including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

Note: IBM has defined an extension to ASCII code (characters 128–255).

ASM. Address space manager.

asynchronous (ASYNC). (1) Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T) (2) Without regular time relationship; unexpected or unpredictable with respect to the execution of program instructions.

authorized program analysis report (APAR). A report of a problem caused by a suspected defect in a current unaltered release of a program.

AVT. Address vector table.

B

basic encoding rules (BER). The rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). The rules specify the encoding technique, not the abstract syntax.

basic information unit (BIU). In SNA, the unit of data and control information passed between half-sessions. It consists of a request/response header (RH) followed by a request/response unit (RU).

basic link unit (BLU). In SNA, the unit of data and control information transmitted over a link by data link control.

basic transmission unit (BTU). In SNA, the unit of data and control information passed between path control components. A BTU can consist of one or more path information units (PIUs). See also *blocking of PIUs*.

batch. (1) An accumulation of data to be processed. (2) A group of records or data processing jobs brought together for processing or transmission. (3) Pertaining to activity involving little or no user action. Contrast with *interactive*.

begin bracket. In SNA, the value (binary 1) of the begin-bracket indicator in the request header (RH) of the first request in the first chain of a bracket; the value denotes the start of a bracket. Contrast with *end bracket*. See also *bracket*.

BER. (1) Box event record. (2) Box error record. (3) Basic encoding rules.

BF. Boundary function.

binary synchronous communication (BSC). A form of telecommunication line control that uses a standard set of transmission control characters and control character sequences, for binary synchronous transmission of binary-coded data between stations. Contrast with *Synchronous Data Link Control (SDLC)*.

BIND. In SNA, a request to activate a session between two logical units (LUs). See also *session activation request*. Contrast with *UNBIND*.

BIU. Basic information unit.

blocking of PIUs. In SNA, an optional function of path control that combines multiple path information units (PIUs) in a single basic transmission unit (BTU).

Note: When blocking is not done, a BTU consists of one PIU.

BN. Boundary node.

BNN. Boundary network node.

boundary function. (1) In SNA, a capability of a subarea node to provide protocol support for attached peripheral nodes, such as: (a) interconnecting subarea path control and peripheral path control elements, (b) performing session sequence numbering for low-function peripheral nodes, and (c) providing session-level pacing support. (2) In SNA, the component that provides these capabilities.

boundary network node (BNN). (1) In SNA, deprecated term for *boundary node (BN)*. (2) In NCP, deprecated term for *peripheral node*.

boundary node (BN). In SNA, a subarea node with boundary function.

Note: A subarea node may be a boundary node, an intermediate routing node, both, or neither, depending on how it is used in the network.

bps. Bits per second.

bracket. In SNA, one or more chains of request units and their responses that are exchanged between two session partners and that represent a transaction between them. A bracket must be completed before another bracket can be started. Examples of brackets are database inquiries/replies, update transactions, and remote job entry output sequences to workstations.

bridge. (1) A functional unit that interconnects two local area networks that use the same logical link

control protocol but may use different medium access control protocols. (T) (2) A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. (3) In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission. (4) See also *gateway.*

BSC. Binary synchronous communication.

BTU. Basic transmission unit.

C

CA. (1) Channel adapter. (2) Channel attachment.

casual connection. (1) In a subarea network, a connection in which type 5 nodes are attached through the boundary function using low-entry networking (LEN). Therefore, the nodes appear as LEN nodes rather than subarea nodes. (2) In an APPN network, a connection between an end node and a network node with different network identifiers.

CCITT. International Telegraph and Telephone Consultative Committee. An organization (one of four permanent organs of the International Telecommunication Union [ITU], headquartered in Geneva, Switzerland) that is concerned with the problems relating to international telephony and telegraphy. The CCITT Plenary Assembly meets at regular intervals to prepare a list of technical questions related to telephone and telegraph services. The Assembly assigns these questions to study groups, which then prepare recommendations to be presented at the next plenary meeting. Approved recommendations are published for the use of engineers, scientists, and manufacturers around the world.

CCU. Central control unit.

CCW. Channel command word.

CDRM. Cross-domain resource manager.

CDRSC. Cross-domain resource.

CDS. (1) Control data set. (2) Configuration data set. (3) Central directory server.

CEB. Conditional end bracket.

central processing unit (CPU). The part of a computer that includes the circuits that control the interpretation and execution of instructions.

Note: A CPU is the circuitry and storage that executes instructions. Traditionally, the complete processing unit was often regarded as the CPU, whereas today the CPU is often a microchip. In either case, the centrality of a processor or processing unit depends on the configuration of the system or network in which it is used.

channel adapter. A communication controller hardware unit that is used to attach the communication controller to a host channel.

channel-attached. (1) Pertaining to the attachment of devices directly by input/output channels to a host processor. (2) Pertaining to devices attached to a controlling unit by cables, rather than by telecommunication lines. Contrast with *link-attached.* Synonymous with *local.*

channel-attachment major node. (1) A major node that includes an NCP that is channel-attached to a data host. (2) A major node that may include minor nodes that are the line groups and lines that represent a channel attachment to an adjacent (channel-attached) host. (3) In VM or VSE operating systems, a major node that may include minor nodes that are resources (host processors, NCPs, line groups, lines, SNA physical units and logical units, cluster controllers, and terminals) attached through a communication adapter.

channel link. A System/370 I/O channel to control unit interface that has an SNA network address. A channel link can be either a subarea link or a peripheral link and is defined in an NCP generation definition using the GROUP, LINE, and PU definition statements. See also *link* and *subarea link.*

character-coded. Synonym for *unformatted.*

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

cleanup. In SNA products, a network services request, sent by a system services control point (SSCP) to a logical unit (LU), that causes a particular LU-LU session with that LU to be ended immediately without requiring the participation of either the other LU or its SSCP.

CLP. Communication line processor.

CLSDST. Close destination.

cluster controller. A device that can control the input/output operations of more than one device connected to it. A cluster controller may be controlled by a program stored and executed in the unit; for example, the IBM 3601 Finance Communication Controller. Or, it

may be entirely controlled by hardware; for example, the IBM 3272 Control Unit.

CMS. Conversational monitor system.

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

common operations services (COS). The portion of SNA management services that pertains to the major vectors for limited remote operations control.

communication adapter. (1) A circuit card with associated software that enables a processor, controller, or other device to be connected to a network. (2) A mechanism that enables communication facilities to be attached to host processors.

communication controller. A type of communication control unit whose operations are controlled by one or more programs stored and executed in the unit. It manages the details of line control and the routing of data through a network.

communication line. Deprecated term for *telecommunication line*.

communication line processor (CLP). In a communications controller, the processor that manages telecommunications lines.

communication scanner processor (CSP). A processor in the 3725 Communication Controller that contains a microprocessor with control code. The code controls transmission of data over links attached to the CSP.

concentrator. (1) In data transmission, a functional unit that permits a common transmission medium to serve more data sources than there are channels currently available within the transmission medium. (T) (2) Any device that combines incoming messages into a single message (concentration) or extracts individual messages from the data sent in a single transmission sequence (deconcentration).

conditional end bracket (CEB). In SNA, the value (binary 1) of the conditional end bracket indicator in the request header (RH) of the last request of the last chain of a bracket; the value denotes the end of the bracket. Contrast with *end bracket*. See also *begin bracket* and *bracket*.

configuration report program (CRP). An SSP utility program that creates a configuration report listing network resources and resource attributes for networks with NCP, EP, PEP, or VTAM.

connectivity. (1) The capability of a system or device to be attached to other systems or devices without modification. (T) (2) The capability to attach a variety of functional units without modifying them.

connectivity subsystem (CSS). An expansion frame, such as the 3746 Model 900, that extends connectivity and enhances the performance of the IBM 3745 Communication Controller.

contention. In a session, a situation in which both NAUs attempt to initiate the same action at the same time, such as when both attempt to send data in a half-duplex protocol (half-duplex contention), or both attempt to start a bracket (bracket contention). At session initiation, one NAU is defined to be the contention winner; its action will take precedence when contention occurs. The contention loser must get explicit or implicit permission from the contention winner to begin its action.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control vector. One of a general class of RU substructures that has variable length, is carried within some enclosing structure, and has a one-byte key used as an identifier.

controller. A device that coordinates and controls the operation of one or more input/output devices, such as workstations, and synchronizes the operation of such devices with the operation of the system as a whole.

conversational monitor system (CMS). A virtual machine operating system that provides general interactive time sharing, problem solving, and program development capabilities, and operates only under control of the VM/370 control program.

COS. (1) Class of service. (2) Common operations services.

coupler. A device that connects a modem to a telephone network.

CP. (1) VM/370 control program. (2) Control point.

CPU. Central processing unit.

cross-domain. In SNA, pertaining to control or resources involving more than one domain.

cross-domain resource (CDRSC). In VTAM, synonym for *other-domain resource*.

cross-network session. An LU-LU or SSCP-SSCP session whose path traverses more than one SNA network.

CRP. Configuration report program.

CSA. (1) Common service area. (2) Common storage area.

CSALIMIT. Common service area (CSA) buffer use limit.

CSMA/CD. Carrier sense multiple access with collision detection.

CSP. Communication scanner processor.

CSS. Connectivity subsystem.

CSW. Channel status word.

CWALL. An NCP threshold of buffer availability, below which the NCP will accept only high-priority path information units (PIUs).

D

DAF'. Destination address field prime.

DASD. Direct access storage device.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data flow control (DFC). In SNA, a request/response unit (RU) category used for requests and responses exchanged between the data flow control layer in one half-session and the data flow control layer in the session partner.

data flow control (DFC) layer. In SNA, the layer within a half-session that controls whether the half-session can send, receive, or concurrently send and receive, request units (RUs); groups related RUs into RU chains; delimits transactions via the bracket protocol; controls the interlocking of requests and responses in accordance with control modes specified at session activation; generates sequence numbers; and correlates requests and responses.

data flow control (DFC) protocol. In SNA, the sequencing rules for requests and responses by which network addressable units (NAUs) in a session coordinate and control data transfer and other operations; for example, bracket protocol.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link escape character (DLE). (1) A transmission control character that changes the meaning of a limited number of contiguously following characters or coded representations. (I) (A) (2) In binary synchronous communication (BSC), a transmission control character used usually in transparent mode to indicate that the next character is a transmission control character.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data services manager (DSM). A function in the NetView program that provides VSAM services for data storage and retrieval.

data stream. (1) All information (data and control commands) sent over a data link usually in a single read or write operation. (2) A continuous stream of data elements being transmitted, or intended for transmission, in character or binary-digit form, using a defined format.

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data types. In the NetView program, a description of the organization of panels. Data types are alerts, events, and statistics. Data types are combined with resource types and display types to describe the NetView program's display organization. See also *display types* and *resource types.*

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. See also *packet* and *segment.*

DCE. Data circuit-terminating equipment.

ddname. Data definition name.

definite response (DR). In SNA, a protocol requested in the form-of-response-requested field of the request header that directs the receiver of the request to return a response unconditionally, whether positive or negative, to that request chain. Contrast with *exception response* and *no response.*

definition statement. (1) In VTAM, the statement that describes an element of the network. (2) In NCP, a type of instruction that defines a resource to the NCP. See Figure 62, Figure 63, and Figure 64. See also *macroinstruction.*

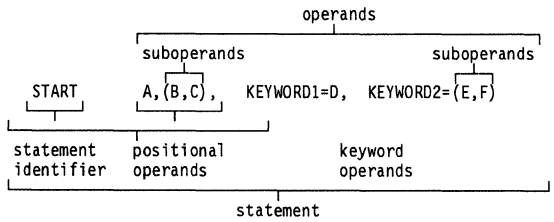


Figure 62. Example of a Language Statement

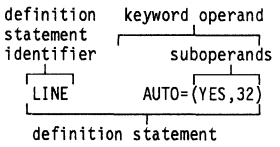


Figure 63. Example of an NCP Definition Statement

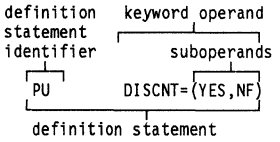


Figure 64. Example of a VTAM Definition Statement

dependent LU. See *SSCP-dependent LU.*

destination address field (DAF). In SNA, a field in a FID0 or FID1 transmission header that contains the network address of the destination.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP).*

destination subarea field (DSAF). In SNA, a field in a FID4 transmission header that contains a subarea address, which combined with the element address in the destination element field, gives the complete network address of the destination network addressable unit (NAU). Contrast with *origin subarea field.*

DEV. Device address field.

DFC. Data flow control.

DISC. Disconnect.

DLC. Data link control.

DLCI. Data link connection identifier.

DM. Disconnect mode.

DMA. Direct memory access.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In SNA, see *end node domain*, *network node domain*, and *system services control point domain*. (3) In the Internet, a part of a naming hierarchy in which the domain name consists of a sequence of names (labels) separated by periods (dots). (4) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies.

download. (1) To transfer programs or data from a computer to a connected device, typically a personal computer. (T) (2) To transfer data from a computer to a connected device, such as a workstation or microcomputer. Contrast with *upload*.

DR. (1) In VTAM, NCP, and CCP, dynamic reconfiguration. (2) In SNA, definite response.

DSAF. Destination subarea field.

DSAP. Destination service access point.

DSR. Data set ready.

DTE. Data terminal equipment. (A)

DTR. Data terminal ready.

dump. (1) To record, at a particular instant, the contents of all or part of one storage device in another storage device. Dumping is usually for the purpose of debugging. (T) (2) Data that has been dumped. (T) (3) To copy data in a readable format from main or auxiliary storage onto an external medium such as tape, diskette, or printer. (4) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

dynamic. (1) In programming languages, pertaining to properties that can only be established during the execution of a program; for example, the length of a variable-length data object is dynamic. (I) (2) Pertaining to an operation that occurs at the time it is needed rather than at a predetermined or fixed time. (3) Contrast with *static*.

dynamic LPDA. A function that enables a NetView application to set or query the Link Problem Determination Aid (LPDA) status for a link or station.

dynamic path update. The process of changing the network path for sending information without regenerating complete configuration tables.

dynamic reconfiguration (DR). The process of changing the network configuration (peripheral PUs and LUs) without regenerating complete configuration tables or deactivating the affected major node.

dynamic resource allocation. An allocation technique in which the resources assigned for execution of computer programs are determined by criteria applied at the moment of need. (I) (A)

dynamic threshold alteration. The process that allows a network operator to dynamically change the traffic count and temporary error threshold values associated with SDLC and BSC devices in communication controllers and network controllers.

E

EC. Engineering change.

ECB. Event control block.

EIA. Electronic Industries Association.

EIA 232. In data communications, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

EID. Event identifier.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

element address. In SNA, a value in the element address field of the network address identifying a specific resource within a subarea. See *subarea address*.

emulation mode. The function of a network control program that enables it to perform activities equivalent to those performed by a transmission control unit. Contrast with *network control mode*.

Emulation Program (EP). An IBM control program that allows a channel-attached 3705 or 3725 communication controller to emulate the functions of an IBM 2701 Data Adapter Unit, an IBM 2702 Transmission Control, or an IBM 2703 Transmission Control. See also *network control program*.

end bracket. In SNA, the value (binary 1) of the end bracket indicator in the request header (RH) of the first request of the last chain of a bracket; the value denotes the end of the bracket. Contrast with *begin bracket*. See also *bracket*.

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is

frequently attached to a single data link and cannot perform intermediate routing functions.

end-of-transmission (EOT) character. (1) A transmission control character used to indicate conclusion of a transmission that may have included one or more texts and associated message headings. (I) (A) (2) In binary synchronous communication, the transmission control character usually used to end communication.

Enterprise Systems Connection (ESCON). A set of IBM products and services that provide a dynamically connected environment within an enterprise.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

EOT. The end-of-transmission character. (A)

EP. (1) Emulation Program. (2) Entry point.

ER. (1) Explicit route. (2) Exception response.

ERACT. Error action.

EREP. Environmental Record Editing and Printing Program. A program that makes the data contained in the system recorder file available for further analysis.

ERP. Error recovery procedures.

error recovery procedures (ERP). (1) Procedures designed to help isolate and, where possible, to recover from errors in equipment. The procedures are often used in conjunction with programs that record information on machine malfunctions. (2) A set of routines that attempt to recover from transmission errors.

ESC. Execution sequence control.

ESCON. Enterprise Systems Connection.

ESCP. ESCON processor.

ESS. Ethernet subsystem. See ETHERNET and ETHERNET-type LAN

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

Ethernet-type LAN. A local area network that uses either the Ethernet Version 2 or IEEE 802.3 protocol.

event control block (ECB). A control block used to represent the status of an event.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response.*

exchange identification (XID). A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

expedited flow. In SNA, a data flow designated in the transmission header (TH) that is used to carry network control, session control, and various data flow control request/response units (RUs); the expedited flow is separate from the normal flow (which carries primarily end-user data) and can be used for commands that affect the normal flow. Contrast with *normal flow.*

Note: The normal and expedited flows move in both the primary-to-secondary and secondary-to-primary directions. Requests and responses on a given flow, whether normal or expedited, usually are processed sequentially within the path, but the expedited flow traffic may be moved ahead of the normal-flow traffic within the path at queuing points in the half-sessions and for half-session support in boundary functions.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR).*

EXT. External trace file.

extended architecture (XA). An extension to System/370 architecture that takes advantage of continuing high performance enhancements to computer system hardware.

extended binary-coded decimal interchange code (EBCDIC). A coded character set of 256 8-bit characters.

extended recovery facility (XRF). A facility that minimizes the effect of failures in MVS, VTAM, the host processor, or high availability applications during ses-

sions between high availability applications and designated terminals. This facility provides an alternate subsystem to take over sessions from the failing subsystem.

F

FDX. Full duplex.

FH. Frame handler.

FHSP. Frame handler subport.

FID. Format identification.

FIFO. First-in-first-out. (A)

flow control. In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units.

FMD. Function management data.

FMH. Function management header.

format identification (FID) field. In SNA, a field in each transmission header (TH) that indicates the format of the TH; that is, the presence or absence of certain fields. TH formats differ in accordance with the types of nodes between which they pass. Following are the six FID types:

FID0, used for traffic involving non-SNA devices between adjacent subarea nodes when either or both nodes do not support explicit route and virtual route protocols

FID1, used for traffic involving SNA devices between adjacent subarea nodes when either or both nodes do not support explicit route and virtual route protocols

FID2, used for traffic between a subarea node and an adjacent type 2 peripheral node

FID3, used for traffic between a subarea node and an adjacent type 1 peripheral node

FID4, used for traffic between adjacent subarea nodes when both nodes support explicit route and virtual route protocols

FIDF, used for certain commands (for example, for transmission group control) sent between adjacent subarea nodes when both nodes support explicit route and virtual route protocols.

fragmentation. The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame handler (FH). Synonym for *frame-relay frame handler (FRFH)*.

frame handler subport (FHSP). The access point of a frame-relay frame handler to a PVC segment. Frame handler subports function in pairs; frames enter the frame handler through one frame handler subport and exit through the other. Contrast with *terminating equipment subport*.

frame relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

frame-relay frame handler (FRFH). (1) The function in a frame-relay node that routes (or switches) frames along a permanent virtual circuit (PVC). A frame handler receives frames from an adjacent frame-relay node and uses the DLCI to forward them to the next node on the PVC. Synonymous with *frame handler*. (2) In NCP, the function that switches frames between frame handler subports on an internal PVC segment. The NCP frame handler function can also switch frames to the frame-relay terminating equipment function.

frame-relay network. A network that consists of frame-relay frame handlers (FRFH) and in which frames are passed from one frame-relay terminal equipment (FRTE) station to another through a series of one or more FRFHs.

frame-relay physical line. The physical connection between two frame-relay nodes. A frame-relay physical line can simultaneously support PVC segments for both the frame-handler and terminating-equipment functions.

In NCP, a frame-relay physical line is defined as a non-switched duplex line.

frame-relay switch. A frame-relay node that provides both the frame-relay frame handler function and the local management interface (LMI) function.

frame-relay switching equipment (FRSE). See *frame-relay switching equipment (FRSE) support.*

frame-relay switching equipment (FRSE) subport set. The set of primary and, optionally, substitute frame handler subports (FHSP) within an NCP that comprise those used for a given frame-relay segment set.

frame-relay switching equipment (FRSE) support. In NCP, a set of frame-relay functions that include the frame-relay frame handler function and the local management interface (LMI) function. These functions are defined by American National Standards Institute (ANSI) Standards T1.617 and T1.618 and International Telegraph and Telephone Consultative Committee (CCITT) Standards Q.922 and Q.933. NCP provides additional functions, including performance measurement and enhanced reliability, that are not defined by ANSI or CCITT standards.

frame-relay terminal equipment. A device that can connect to a frame-relay network and provide the frame-relay terminating equipment function. See also *frame-relay frame handler* and *frame-relay terminating equipment.*

frame-relay terminating equipment (FRTE). The function at the end of a frame-relay permanent virtual circuit (PVC). Frame-relay terminating equipment provides higher-layer protocols with access to a frame-relay network through terminating equipment subports (TESPs). It does this by (a) adding frame-relay frame headers to data for another protocol and sending the frames to adjacent frame-relay nodes, and (b) receiving frames from adjacent frame-relay nodes and removing the frame headers. See also *frame-relay frame handler, frame-relay switching equipment support,* and *frame-relay terminal equipment.*

FRFH. Frame-relay frame handler.

FRSE. Frame-relay switching equipment.

FRTE. Frame-relay terminal equipment.

full duplex (FDX). Synonym for *duplex.*

fullword. Synonym for *computer word.*

function management data (FMD). An RU category used for end-user data exchanged between logical units (LUs) and for requests and responses exchanged between network services components of LUs, PUs, and control points.

function management header (FMH). One or more headers, optionally present in the leading request units (RUs) of an RU chain, that allow one LU to (a) select a transaction program or device at the session partner and control the way in which the end-user data it sends is handled at the destination, (b) change the destination or the characteristics of the data during the session, and (c) transmit between session partners status or user information about the destination (for example, a program or device). Function management headers can be used with LU type 1, 4, and 6.2 protocols.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the AIX operating system, an entity that operates above the link layer and translates, when required, the interface and protocol used by one network into those used by another distinct network. (3) In TCP/IP, a device used to connect two systems that use either the same or different communications protocols. (4) The combination of machines and programs that provide address translation, name translation, and system services control point (SSCP) rerouting between independent SNA networks to allow those networks to communicate. A gateway consists of one gateway NCP and at least one gateway VTAM. (5) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols.

gateway NCP. An NCP that performs address translation to allow cross-network session traffic. The gateway NCP connects two or more independent SNA networks. Synonymous with *gateway node.*

gateway node. Synonym for *gateway NCP.*

GCS. Group control system.

generalized path information unit trace (GPT). A record of the flow of path information units (PIUs) exchanged between the network control program and its attached resources. PIU trace records consist of up to 44 bytes of transmission header (TH), request/response header (RH), and request/response unit (RU) data.

generalized trace facility (GTF). An optional OS/VS service program that records significant system events,

such as supervisor calls and start I/O operations, for the purpose of problem determination.

generation definition. The definition statement of a resource used in generating a program.

generic alert. A product-independent method of encoding alert data by means of both (a) code points indexing short units of stored text and (b) textual data.

GPT. Generalized path information unit trace.

group control system (GCS). A component of VM that provides multiprogramming and shared memory support to virtual machines. It is a saved system intended for use with SNA products.

GTF. Generalized trace facility.

H

half-duplex (HD, HDX). In data communication, pertaining to transmission in only one direction at a time. Contrast with *duplex*. See also *half-duplex operation* and *half-duplex transmission*.

half-session. A session-layer component consisting of the combination of data flow control and transmission control components comprising one end of a session.

halfword. A contiguous sequence of bits or characters that constitutes half a computer word and can be addressed as a unit. (A)

HDLC. High-level data link control.

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

high-performance transmission subsystem (HPTSS). A high-speed line adapter that attaches to the IBM 3745 Communication Controller.

host ID. In TCP/IP, that part of the Internet address that defines the host on the network. The length of the host ID depends on the type of network or network class (A, B, or C).

host node. (1) A node at which a host computer is located. (T) (2) A node that provides an application program interface (API) and a common application interface.

host processor. (1) A processor that controls all or part of a user application network. (T) (2) In a network, the processing unit in which the data communication access method resides.

HPTSS. High-performance transmission subsystem.

I

I format. Information format.

I frame. Information frame.

I/O. Input/output.

ICW. Interface control word.

IEEE. Institute of Electrical and Electronics Engineers.

independent LU. See *SSCP-independent LU*.

information (I) format. A format used for information transfer.

information (I) frame. A frame in I format used for numbered information transfer.

initial program load (IPL). (1) The initialization procedure that causes an operating system to commence operation. (2) The process by which a configuration image is loaded into storage at the beginning of a work day or after a system malfunction. (3) The process of loading system programs and preparing a system to run jobs. (4) Synonymous with *system restart* and *system startup*.

INITIATE. A network services request sent from a logical unit (LU) to a system services control point (SSCP) requesting that an LU-LU session be established.

INN. Intermediate network node.

INT. Internal trace table.

intensive mode recording (IMR). An NCP function that forces recording of temporary errors for a specified resource.

interactive problem control system (IPCS). A component of VM that permits online problem management, interactive problem diagnosis, online debugging for disk-resident CP abend dumps, problem tracking, and problem reporting.

Interactive System Productivity Facility (ISPF). An IBM licensed program that serves as a full-screen editor and dialogue manager. Used for writing application programs, it provides a means of generating standard screen panels and interactive dialogues between the application programmer and terminal user.

intermediate network node (INN). (1) In APPN, a node that is part of a route between an origin logical unit (OLU) and a destination logical unit (DLU), but does not contain the OLU or DLU and does not serve as the network server for the OLU or DLU. (2) In VTAM, deprecated term for *intermediate routing node (IRN).* (3) In NCP, deprecated term for *subarea node (SN).*

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet.*

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address.*

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

IP. Internet Protocol.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comment (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IPCS. Interactive problem control system.

IPM. Isolated pacing message.

IPR. Isolated pacing response.

IPX. Internetwork Packet Exchange.

IRN. Intermediate routing node.

ISO. International Organization for Standardization.

ISPF. Interactive System Productivity Facility.

ISTATUS. In VTAM and NCP, a definition specification method for indicating the initial status of resources. See also *indirect activation.*

J

JCL. Job control language.

job control language (JCL). A control language used to identify a job to an operating system and to describe the job's requirements.

L

LAN. Local area network.

LCB. Local block common.

LFSID. Local-form session identifier.

LIC. (1) Last-in-chain. (2) In NCP, line interface coupler.

line control discipline. Synonym for *link protocol.*

line discipline. Synonym for *link protocol.*

line group. One or more telecommunication lines of the same type that can be activated and deactivated as a unit.

line speed. The number of binary digits that can be sent over a telecommunication line in one second, expressed in bits per second (bps).

link. (1) The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration. (2) To interconnect items of data or portions of one or more computer programs: for example, the linking of object programs by a linkage editor, linking of data items by pointers. (T)

link access procedures (LAP). The link level elements used for data interchange between data circuit-terminating equipment (DCE) and data terminal

equipment (DTE) operating in user classes of service 8 to 11, as specified in CCITT Recommendation X.1.

link-attached. Pertaining to devices that are connected to a controlling unit by a data link. Contrast with *channel-attached*. Synonymous with *remote*.

link connection. The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). Synonymous with *data circuit*.

link level. A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT.

link level 2 test. See *link test*.

Link Problem Determination Aid (LPDA). A series of procedures that are used to test the status of and to control DCEs, the communication line, and the remote device interface. These procedures, or a subset of them, are implemented by host programs (such as the NetView program and VTAM), communication controller programs (such as NCP), and IBM LPDA DCEs. See also *LPDA-1* and *LPDA-2*.

link protocol. (1) The rules for sending and receiving data at the link level. (2) See *protocol*. (3) See also *link level*.

link station. (1) The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. See also *adjacent link station*. (2) In VTAM, a named resource within an APPN or a subarea node that represents the connection to another APPN or subarea node that is attached by an APPN or a subarea link. In the resource hierarchy in a subarea network, the link station is subordinate to the subarea link.

link test. In SNA, a test in which one link station returns data received from another link station without changing the data in order to test the operation of the link. Three tests can be made; they differ in the resources that are dedicated during the test.

LLB. Local Location Broker.

LLC. Logical link control.

LL2. Link level 2.

load module. All or part of a computer program in a form suitable for loading into main storage for execution. A load module is usually the output of a linkage editor. (T)

local. Pertaining to a device accessed directly without use of a telecommunication line. Synonym for *channel-attached*.

local address. In SNA, an address used in a peripheral node in place of a network address and transformed to or from a network address by the boundary function in a subarea node.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. See also *Ethernet* and *token ring*. (3) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local directory database. That set of resources (LUs) in the network known at a particular node. The resources included are all those in the node's domain as well as any cache entries.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. (1) In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*. (2) Originally, a set of frame-relay network management procedures and messages used by frame-relay nodes to exchange line status information over DLCI X'03FF' (1023). This protocol is defined in *Frame-Relay Specification with Extensions*, a document based on proposed T1S1 standards, which are copyrighted by Digital Equipment Corporation, Northern Telecom, Inc., and StrataCom, Inc. This protocol is not compatible with the ANSI or CCITT version. In this context, the term *local management interface* is a deprecated term for *link integrity verification tests (LIVT)*.

local session identification (LSID). In SNA, a field in an FID3 (format identification type 3) transmission header that contains an indication of the type of session

(SSCP-PU, SSCP-LU, or LU-LU) and the local address of the peripheral logical unit (LU) or physical unit (PU).

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical line. In NCP, the representation of the connection between NCP and a node communicating with NCP over a physical line such as token-ring or frame-relay. A single physical line can support multiple logical lines. Contrast with *physical line*.

logical link. (1) A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network. (2) In APPNTAM, the unidirectional representation in a node of a link.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T)

Note: The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical unit (LU). A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

logical unit (LU) 6.2. A type of logical unit that supports general communication between programs in a distributed processing environment. LU 6.2 is characterized by (a) a peer relationship between session partners, (b) efficient utilization of a session for multiple transactions, (c) comprehensive end-to-end error processing, and (d) a generic application program interface (API) consisting of structured verbs that are mapped into a product implementation.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

LPDA. Link Problem Determination Aid.

LPDA-1. The first version of the LPDA command set. LPDA-1 is not compatible with LPDA-2. See also *Link Problem Determination Aid (LPDA)* and *LPDA-2*.

LPDA-2. The second version of the LPDA command set. LPDA-2 provides all of the functions of LPDA-1; it also supports commands such as the following:

- DCE configuration
- Dial
- Set transmit speed
- Commands to operate a contact that can control external devices.

See also *Link Problem Determination Aid (LPDA)* and *LPDA-1*.

LSID. Local session identification.

LU. Logical unit.

LU-LU session. A logical connection between two logical units (LUs) in an SNA network that typically provides communication between two end users.

LU-LU session type. Deprecated term for *LU type*.

LU type. The classification of an LU in terms of the specific subset of SNA protocols and options it supports for a given session, namely:

- The mandatory and optional values allowed in the session activation request
- The usage of data stream controls, function management headers (FMHs), request unit parameters, and sense data values
- Presentation services protocols such as those associated with FMH usage

LU types 0, 1, 2, 3, 4, 6.1, 6.2, and 7 are defined.

LU type 6.2 (LU 6.2). A type of logical unit that supports general communication between programs in a distributed processing environment. LU 6.2 is characterized by (a) a peer relationship between session partners, (b) efficient utilization of a session for multiple transactions, (c) comprehensive end-to-end error processing, and (d) a generic application program interface consisting of structured verbs that are mapped into a product implementation.

LU 6.2. Logical unit 6.2.

LUS. Logical unit services.

M

MAC. Medium access control.

maintenance and operator subsystem (MOSS). A subsystem of an IBM communication controller, such as the 3725 or the 3720, that contains a processor and operates independently of the rest of the controller. It loads and supervises the controller, runs problem determination procedures, and assists in maintaining both hardware and software.

maintenance and operator subsystem extended (MOSS-E). A subsystem of the IBM 3745 Communication Controller that operates independently of the rest of the controller. It loads and supervises the controller, runs problem determination procedures, and assists in maintaining both hardware and software.

major node. In VTAM, a set of resources that can be activated and deactivated as a group.

Mb. Megabit; 1 048 576 bits.

MB. Megabyte; 1 048 576 bytes.

Mbps. One million bits per second.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T) See also *logical link control protocol.*

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

MLTG. Multilink transmission group.

MMMLTG. Mixed-media multilink transmission group.

mode. See *mode name.*

mode name. The name used by the initiator of a session to designate the characteristics desired for the session, such as traffic pacing values, message-length limits, sync point and cryptography options, and the class of service within the transport network.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus.*

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

MOSS. Maintenance and operator subsystem.

MOSS-E. Maintenance and operator subsystem extended.

MPF. Message processing facility.

multidrop line. Synonym for *multipoint line.*

multilink transmission group (MLTG). See *transmission group (TG).*

Multiple Virtual Storage (MVS). See *MVS.*

Multiple Virtual Storage/Extended Architecture (MVS/XA). See *MVS/XA product.*

multipoint connection. A connection established for data transmission among more than two data stations. (I) (A)

Note: The connection may include switching facilities.

MVS. Multiple Virtual Storage. Implies MVS/370, the MVS/XA product, and the MVS/ESA product.

MVS/ESA product. Multiple Virtual Storage/Enterprise Systems Architecture.

MVS/XA product. Multiple Virtual Storage/Extended Architecture product, consisting of MVS/System Product Version 2 and the MVS/XA Data Facility Product, operating on a System/370 processor in the System/370 extended architecture mode. MVS/XA allows virtual storage addressing to 2 gigabytes. See also *MVS.*

N

NAB. Network address block.

native network. The subnetwork whose network identifier a node uses for its own network-qualified resource names.

NAU. (1) Network accessible unit. (2) Network addressable unit.

NCP. Network Control Program.

NCP connectionless SNA transport (NCST). An NCP function that allows a communication controller to transfer data across the SNA subarea routing network using TCP/IP protocols. The NCST function causes LU 0 sessions to be established between NCST logical units in the NCP and between an NCST logical unit in the NCP and SNA network link (SNALINK) logical units in the host processors.

NCP/EP definition facility (NDF). A program that is part of System Support Programs (SSP) and that is used to generate a load module for a partitioned emulation program (PEP), a Network Control Program (NCP), or an Emulation Program (EP).

NCP/Token-Ring interconnection (NTRI). An NCP function that allows a communication controller to attach to the IBM Token-Ring Network and that provides both subarea and peripheral node data link control (DLC) services in the SNA network.

NCST. NCP connectionless SNA transport.

NDF. NCP/EP definition facility.

negative response (NR). In SNA, a response indicating that a request did not arrive successfully or was not processed successfully by the receiver. Contrast with *positive response*.

NETID. Network identifier.

NetView Performance Monitor (NPM). An IBM licensed program that collects, monitors, analyzes, and displays data relevant to the performance of a VTAM telecommunication network. It runs as an online VTAM application program.

NetView program. An IBM licensed program used to monitor and manage a network and to diagnose network problems.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. (1) In a subarea network, an address, consisting of subarea and element fields, that identifies a link, link station, physical unit, logical unit, or system services control point. Subarea nodes use network addresses; peripheral nodes use local addresses or local-form session identifiers (LFSIDs). The boundary function in the subarea node to which a peripheral node is attached transforms local addresses or LFSIDs to network addresses and vice versa. Contrast with *network name*. (2) According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network control mode. The mode in which a network control program can direct a communication controller to perform such activities as polling, device addressing, dialing, and answering. See also *emulation mode*.

Network Control Program (NCP). An IBM licensed program that provides communication controller support for single-domain, multiple-domain, and interconnected network capability.

network gateway accounting (NGA). The NetView Performance Monitor (NPM) subsystem that receives traffic information from the gateway NCP for sessions that flow throughout a network.

network identifier. (1) In TCP/IP, that part of the Internet address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network name. (1) The symbolic identifier by which end users refer to a network accessible unit, a link, or a link station within a given subnetwork. In APPN networks, network names are also used for routing purposes. Contrast with *network address*. (2) In a multiple-domain network, the name of the APPL statement defining a VTAM application program. The network name must be unique across domains. Contrast with *ACB name*. See *uninterpreted name*.

network node (NN). Synonym for *Advanced Peer-to-Peer Networking (APPN) network node*.

network-node domain. An APPN network-node control point, its attached links, the network resources for which it answers directory search requests (namely, its local LUs and adjacent LEN end nodes), the adjacent APPN end nodes with which it exchanges directory search requests and replies, and other resources (such as a local storage device) associated with its own node or an adjacent end node for which it provides management services.

network performance analyzer (NPA). A function of NCP that collects performance data about devices. The data is recorded by NPM.

Network Routing Facility (NRF). An IBM licensed program that resides in NCP. NRF provides a path for routing messages between terminals and routes messages over this path without going through the host processor.

network services. (1) The services within network accessible units that control network operation through SSCP-SSCP, SSCP-PU, SSCP-LU, and CP-CP sessions. (2) The session services (directory and route-selection functions) and management services provided by an APPN network-node control point to its domain.

network services (NS) header. In SNA, a 3-byte field in a function management data (FMD) request/response unit (RU) flowing in an SSCP-LU, SSCP-PU, or SSCP-SSCP session. The network services header is used primarily to identify the network services category of the request unit (RU) (for example, configuration services and session services) and the particular request code within a category.

network session accounting (NSA). The NetView Performance Monitor (NPM) subsystem that receives session accounting information from the NCP for sessions that flow throughout a network.

Network Terminal Option (NTO). An IBM licensed program, used in conjunction with NCP, that allows certain non-SNA devices to participate in sessions with SNA application programs in the host processor. When data is sent from a non-SNA device to the host processor, NTO converts non-SNA protocol to SNA protocol; and when data is sent from the host processor to the non-SNA device, NTO converts SNA protocol to non-SNA protocol.

NGA. Network gateway accounting.

NIB. Node initialization block.

NLDM. (1) Network Logical Data Manager. (2) A command that starts the NetView session monitor. NLDM also identifies various panels and functions as part of the session monitor.

NMVT. Network management vector transport.

NNCP. Network node control point.

NNT. NetView-NetView task.

no response. In SNA, a protocol requested in the form-of-response-requested field of the request header that directs the receiver of the request not to return any response, regardless of whether or not the request is received and processed successfully. Contrast with *definite response* and *exception response.*

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data. (3) An endpoint of a link or a junction common to two or more links in a network. Nodes can be processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities. (4) In VTAM, a point in a network defined by a symbolic name. See *major node* and *minor node.* (5) In NETDA/2, a combination of hardware, software, and microcode that can generate message traffic, receive and process message traffic, or receive and relay message traffic.

Non-SNA Interconnection (NSI). An IBM licensed program that provides format identification (FID) support for selected non-SNA facilities. Thus, it allows SNA and non-SNA facilities to share SDLC links. It also allows the remote concentration of selected non-SNA devices along with SNA devices.

nonswitched connection. A connection that does not have to be established by dialing. Contrast with *switched connection.*

nonswitched line. A telecommunication line on which connections do not have to be established by dialing. Contrast with *switched line.*

nontransparent mode. A mode of binary synchronous transmission in which all transmission control characters are treated as transmission control characters rather than as text. Contrast with *transparent mode.*

NPA. Network performance analyzer.

NPALU. In the NetView Performance Monitor (NPM), the virtual logical unit generated in an NCP with which the network subsystem communicates.

NPDA. (1) Network Problem Determination Application. (2) A command that starts the NetView hardware monitor. NPDA also identifies various panels and functions as part of the hardware monitor.

NPM. NetView Performance Monitor.

NPSI. X.25 NCP Packet Switching Interface.

NR. Negative response.

NRF. Network Routing Facility.

NRZ. Non-return-to-reference recording. (I) (A)

NRZI. Non-return-to-zero (inverted) recording. Deprecated term for *non-return-to-zero change-on-ones recording (NRZ-1)*.

NSA. (1) Network session accounting. (2) Nonsequenced acknowledgment.

NSI. Non-SNA Interconnection.

NTO. Network Terminal Option.

NTRI. NCP/Token-Ring interconnection.

NTune. A set of programs (NTuneMON and NTuneNCP) that allow monitoring and tuning of active NCPs. See *NTuneMON* and *NTuneNCP*.

NTuneMON. A program that runs on NetView, and monitors NCPs that were activated, by VTAM, on the host where NTuneMON is running. See *NTune* and *NTuneNCP*.

NTuneNCP. A program that runs in the communications controller and, together with NTuneMON and VTAM provides interactive tuning capability of internal NCP resources. See *NTune* and *NTuneMON*.

O

OAF. Origin address field.

OAF'. Origin address field prime.

ODLC. Outboard data link control.

operator station task (OST). The NetView task that establishes and maintains the online session with the network operator. There is one operator station task for each network operator who logs on to the NetView program. See *NetView-NetView task*.

origin address field (OAF). In SNA, a field in a FID0 or FID1 transmission header that contains the address of the originating network accessible unit (NAU). Contrast with *destination address field*. See also *format identification (FID) field* and *local session identification (LSID)*.

origin subarea field (OSAF). In SNA, a subarea field in a FID4 transmission header that contains a subarea address, which combined with the element address in the origin element field, gives the complete network address of the originating network accessible unit (NAU). Contrast with *destination subarea field*.

OS. Operating system.

OSAF. Origin subarea field.

other-domain resource. A representation for a logical unit that is owned by another domain and is referenced by a symbolic name, which can be qualified by a network identifier.

outboard data link control (ODLC). (1) Data link control (DLC) processing performed by a coprocessor. (2) In NCP, data link control (DLC) processing performed by the 3746 Model 900 connectivity subsystem (CSS). (3) For the IBM 6611 Network Processor, data link control (DLC) processing performed by a deep adapter.

outbound. In communications, data that is transmitted to the network.

P

PAB. Process anchor block.

pacing. A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. See also *flow control*.

pacing response. In SNA, an indicator that signifies the readiness of a receiving component to accept another pacing group. The indicator is carried in a response header (RH) for session-level pacing and in a transmission header (TH) for virtual route pacing.

pacing window. (1) The path information units (PIUs) that can be transmitted on a virtual route before a virtual-route pacing response is received, indicating that the virtual route receiver is ready to receive more PIUs on the route. (2) The requests that can be transmitted on the normal flow in one direction on a session before a session-level pacing response is received, indicating that the receiver is ready to accept the next group of requests. (3) Synonymous with *pacing group*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet assembler/disassembler (PAD). A functional unit that enables data terminal equipment (DTEs) not equipped for packet switching to access a packet switched network. (T) (A)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet level. (1) The packet format and control procedures for exchange of packets containing control information and user data between data terminal equipment (DTE) and data circuit-terminating equipment (DCE). (2) A part of Recommendation X.25 that defines the protocol for establishing logical connections between two DTEs and for transferring data on these connections.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation.* See also *circuit switching.*

parallel links. In SNA, two or more links between adjacent subarea nodes.

parallel sessions. Two or more concurrently active sessions between the same two network accessible units (NAUs) using different pairs of network addresses or local-form session identifiers. Each session can have independent session parameters.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

partitioned emulation programming (PEP) extension. A function of a network control program that enables a communication controller to operate some telecommunication lines in network control mode while simultaneously operating others in emulation mode.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment. See also *transmission header.*

PCF. Primary control field.

PCID. Procedure-correlation identifier.

PDF. Parallel data field.

PDS. Partitioned data set.

PEP. Partitioned emulation programming.

peripheral logical unit (LU). In SNA, a logical unit in a peripheral node.

peripheral node. A node that uses local addresses for routing and therefore is not affected by changes in network addresses. A peripheral node requires boundary-function assistance from an adjacent subarea node. A peripheral node can be a type 1, 2.0, or 2.1 node connected to a subarea boundary node.

peripheral PU. In SNA, a physical unit (PU) in a peripheral node.

permanent error. An error that cannot be resolved by error recovery programs. Contrast with *temporary error.*

physical level. In X.25, the mechanical, electrical, functional, and procedural media used to activate, maintain, and deactivate the physical link between the data terminal equipment (DTE) and the data circuit-terminating equipment (DCE). See *data link level* and *packet level.*

physical unit (PU). The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. See also *peripheral PU* and *subarea PU.*

physical unit (PU) services. In SNA, the components within a physical unit (PU) that provide configuration services and maintenance services for SSCP-PU sessions.

physical unit type. In SNA, the classification of a physical unit (PU) according to the type of node in which it resides. The physical unit type is the same as its node type; that is, a type 1 physical unit resides in a type 1 node, and so forth.

PING. Packet internet groper.

PIU. Path information unit.

PLB. Presentation services local block.

PLU. Primary logical unit.

point-to-point connection. A connection established between two data stations for data transmission. (I) (A)

Note: The connection may include switching facilities.

point-to-point line. A switched or nonswitched telecommunication line that connects a single remote station to a computer. Contrast with *multipoint line*.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

primary logical unit (PLU). In SNA, the logical unit (LU) that sends the BIND to activate a session with its partner LU. Contrast with *secondary logical unit*.

primary station. (1) In high-level data link control (HDLC), the part of a data station that supports the primary control functions of the data link, generates commands for transmission, and interprets received responses. (I) (2) In SNA, the station on an SDLC data link that is responsible for the control of the data link. There must be only one primary station on a data link. All traffic over the data link is between the primary station and a secondary station. (3) Contrast with *secondary station*.

Note: Specific responsibilities assigned to the primary station include initialization of control signal interchange, organization of data flow, and actions to perform error control and error recovery functions.

PRM. Protected-resource manager.

procedure-correlation identifier (PCID). In SNA, a value used to correlate all requests and replies associated with a given procedure.

process anchor block (PAB). In VTAM, a process scheduling services dispatch point.

product-set identification (PSID). (1) In SNA, a technique for identifying the hardware and software products that implement a network component. (2) A management services common subvector that transports the information described in definition (1).

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*.

PSID. Product-set identification.

PSW. Program status word.

PTF. Program temporary fix.

PU. Physical unit.

PU type. (1) Deprecated term for *node type*. (2) The type of physical unit in a node.

PVI. Primitive VTAM interface.

Q

QAB. Queue anchor block.

queue. (1) A list constructed and maintained so that the next data element to be retrieved is the one stored first. (T) (2) A line or list of items waiting to be processed; for example, work to be performed or messages to be displayed. (3) To arrange in or form a queue.

R

RACF. Resource Access Control Facility.

RDT. Resource definition table.

RDTE. Resource definition table entry.

redefinable line. A line that is in use and can be activated (defined using the USE keyword on the LINE definition statement). It can be changed to a spare line using NTuneMON with NTuneNCP.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

RECFMS. Record formatted maintenance statistics.

RECMS. Record maintenance statistics.

record formatted maintenance statistics (RECFMS). A statistical record built by an SNA controller and usually solicited by the host.

record maintenance statistics (RECMS). An SNA error event record built from an NCP or line error and sent unsolicited to the host.

remote. Pertaining to a system, program, or device that is accessed through a telecommunication line. Contrast with *local*. Synonym for *link-attached*.

remote modem self-test (RST). A check on hardware to identify a field-replaceable unit that is failing.

REQMS. Request for maintenance statistics.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

request for maintenance statistics (REQMS). A host solicitation to an SNA controller for a statistical data record.

request header (RH). The control information that precedes a request unit (RU). See also *request/response header (RH)*.

request unit (RU). A message unit that contains control information, end-user data, or both.

request/response header (RH). Control information associated with a particular RU. The RH precedes the request/response unit (RU) and specifies the type of RU (request unit or response unit).

request/response unit (RU). A generic term for a request unit or a response unit. See *request unit (RU)* and *response unit (RU)*.

Resource Access Control Facility (RACF). An IBM licensed program that provides for access control by identifying and verifying the users of the system, by authorizing access to protected resources, by logging the detected unauthorized attempts to enter the system, and by logging the detected accesses to protected resources.

resource definition table (RDT). In VTAM, a table that describes the characteristics of each node available to VTAM and associates each node with a network address. This is the main VTAM network configuration table.

resource level. In the NetView program, the hierarchical position of a device (and the software contained within it) in a data processing system. For example, a first-level resource could be the communication controller, and the second-level resource could be the line connected to it.

response header (RH). A header, optionally followed by a response unit (RU), that indicates whether the response is positive or negative and that may contain a pacing response.

response unit (RU). A message unit that acknowledges a request unit. It may contain prefix information received in a request unit. If positive, the response unit may contain additional information (such as session parameters in response to BIND SESSION). If negative, the response unit contains sense data defining the exception condition.

REX. Route extension.

RH. Request/response header.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

RIP. Routing Information Protocol.

RNAA. Request network address assignment.

RNR. Receive not ready.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

routing. (1) The process of determining the path to be used for transmission of a message over a network. (T) (2) The assignment of the path by which a message is to reach its destination. (3) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

RR. Receive ready.

RST. Remote modem self-test.

RU. Request/response unit.

S

SAP. (1) Service access point. (2) Service Advertising Protocol.

scanner interface trace (SIT). A record of the activity within the communication scanner processor (CSP) for a specified data link between an IBM 3725 Communication Controller and a resource.

SCB. (1) Session control block. (2) String control byte.

SCF. Secondary control field.

SDF. Serial data field.

SDLC. Synchronous Data Link Control.

SDT. Start data traffic.

secondary logical unit (SLU). In SNA, the logical unit (LU) that contains the secondary half-session for a particular LU-LU session. An LU may contain secondary and primary half-sessions for different active LU-LU sessions. Contrast with *primary logical unit (PLU)*.

secondary station. A data station that executes data link control functions as instructed by the primary station. A secondary station interprets received commands and generates responses for transmission. Contrast with *primary station*.

segment. (1) In the IBM Token-Ring Network, a section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte stream position and actual data bytes are identified along with a checksum to validate received data. (3) Synonym for *BIU segment*.

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

service point (SP). An entry point that supports applications that provide network management for resources not under the direct control of itself as an entry point. Each resource is either under the direct control of another entry point or not under the direct control of any entry point. A service point accessing these resources is not required to use SNA sessions (unlike a focal point). A service point is needed when entry point support is not yet available for some network management function.

session activation request. In SNA, a request that activates a session between two network accessible units (NAUs) and specifies session parameters that control various protocols during session activity; for example, BIND and ACTPU. Contrast with *session deactivation request*.

session control (SC). In SNA, either of the following:

- One of the components of transmission control. Session control is used to purge data flowing in a session after an unrecoverable error occurs, to resynchronize the data flow after such an error, and to perform cryptographic verification.
- A request unit (RU) category used for requests and responses exchanged between the session control components of a session and for session activation and deactivation requests and responses.

session control block (SCB). In NPM, control blocks in common storage area for session collection.

session data. Data about a session, collected by the NetView program, that consists of session awareness data, session trace data, and session response time data.

session deactivation request. In SNA, a request that deactivates a session between two network accessible units (NAUs); for example, UNBIND and DACTPU. Synonymous with *generic unbind*. Contrast with *session activation request*.

session information block (SIB). A control block that contains information about a particular SNA session.

session information retrieval (SIR). The function that allows an operator to enable or disable session information retrieval for a particular gateway or for all gateway sessions. When a gateway session ends, trace information about the most recent sequence or FID0 numbers to cross the gateway is passed back to all system services control points (SSCPs) that have enabled SIR for that session or for all sessions. This information can also be passed back to the requesting host.

session limit. (1) The maximum number of concurrently active LU-LU sessions that a particular logical unit (LU) can support. (2) In NCP, the maximum number of concurrent line-scheduling sessions on a non-SDLC, multipoint line.

session manager (SM). A product, such as NetView Access Services, that allows a user at a terminal to log on to multiple applications concurrently.

session partner. In SNA, one of the two network accessible units (NAUs) having an active session.

session path. The half-sessions delimiting a given session and their interconnection (including any intermediate session connectors).

session sequence number. In SNA, a sequentially incremented identifier that is assigned by data flow control to each request unit on a particular normal flow of a session, typically an LU-LU session, and is checked by transmission control. The identifier is carried in the transmission header (TH) of the path information unit (PIU) and is returned in the TH of any associated response. Contrast with *virtual route sequence number.*

SIB. Session information block.

SIO. Start I/O.

SIR. Session information retrieval.

SIT. Scanner interface trace.

SLU. Secondary logical unit.

SMMF. SSCP monitor mode function.

SN. Subarea node.

SNA. Systems Network Architecture.

SNA network. The part of a user-application network that conforms to the formats and protocols of Systems Network Architecture. It enables reliable transfer of data among end users and provides protocols for controlling the resources of various network configurations. The SNA network consists of network accessible units (NAUs), boundary function, gateway function, and intermediate session routing function components; and the transport network.

SNA network interconnection (SNI). The connection, by gateways, of two or more independent SNA networks to allow communication between logical units in those networks. The individual SNA networks retain their independence.

SNA Network Link (SNALINK). A function of the TCP/IP products for VM and MVS that allows the use of an SNA subarea routing network to transfer data using TCP/IP protocols. SNALINK provides the interface between TCP/IP and the SNA network. SNALINK must be defined as an application program to VTAM, which causes LU 0 sessions to be established between the SNALINK logical unit and other logical units in the SNA network.

SNA terminal. A terminal that supports SNA protocols.

SNALINK. SNA Network Link.

SNAP. Subnetwork Access Protocol.

SNI. SNA network interconnection.

SNRM. Set normal response mode.

SP. Service point.

spare line. A line that is not in use and cannot be activated (defined using the USE keyword on the LINE definition statement). It can be changed to a redefinable line using NTuneMON with NTuneNCP, and then activated.

SPL. Station polling list.

SRT. Symbol resolution table.

SS. (1) Start-stop. (2) Session services.

SSAP. Source service access point.

SSCP. System services control point.

SSCP-dependent LU. An LU that requires assistance from a system services control point (SSCP) in order to initiate an LU-LU session. It requires an SSCP-LU session.

SSCP-independent LU. An LU that is able to activate an LU-LU session (that is, send a BIND request) without assistance from an SSCP. It does not have an SSCP-LU session. Currently, only an LU 6.2 can be an independent LU.

SSCP-LU session. In SNA, a session between a system services control point (SSCP) and a logical unit (LU). The session enables the LU to request the SSCP to help initiate LU-LU sessions.

SSCP monitor mode function (SMMF). A function within NCP that keeps NCP resources active when an external SSCP has not established ownership of NCP.

SSCP-PU session. In SNA, a session between a system services control point (SSCP) and a physical unit (PU); SSCP-PU sessions allow SSCPs to send requests to and receive status information from individual nodes in order to control the network configuration.

SSP. System Support Programs.

ST. Session configuration screen abbreviation.

start-stop (SS) transmission. (1) Asynchronous transmission such that each group of signals representing a character is preceded by a start signal and is followed by a stop signal. (T) (A) (2) Asynchronous transmission in which a group of bits is (a) preceded by a start bit that prepares the receiving mechanism for the reception and registration of a character, and (b) followed by at least one stop bit that enables the receiving mechanism to come to an idle condition pending reception of the next character. See also *binary synchronous transmission* and *synchronous data link control*.

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subarea address. A value in the subarea field of the network address that identifies a particular subarea. See also *element address*.

subarea link. In SNA, a link that connects two subarea nodes. See *channel link* and *link*.

subarea network. Interconnected subareas, their directly attached peripheral nodes, and the transmission groups that connect them.

subarea node (SN). A node that uses network addresses for routing and maintains routing tables that reflect the configuration of the network. Subarea nodes can provide gateway function to connect multiple subarea networks, intermediate routing function, and boundary function support for peripheral nodes. Type 4 and type 5 nodes can be subarea nodes.

subarea PU. In SNA, a physical unit (PU) in a subarea node.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use $AA as their Service Advertising Protocol (SAP) value.

subport. (1) An access point for data entry or exit over a logical connection. The relationship between the physical line and the port is analogous to the relationship between the logical connection and the subport. (2) In a frame-relay network, the representation of a logical connection on a frame-relay physical line and the point where the logical connection attaches to the frame-relay frame handler (FRFH). Each subport on a physical line has a unique data link connection identifier (DLCI) and can represent an FRTE, FRFH, or LMI connection. See *frame handler subport (FHSP)* and *terminal equipment subport*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

subvector. A subcomponent of the NMVT major vector.

supervisor call (SVC). A request that serves as the interface into operating system functions, such as allocating storage. The SVC protects the operating system from inappropriate user entry. All operating system requests must be handled by SVCs.

SVC. (1) Supervisor call. (2) Switched virtual circuit.

switched connection. (1) A mode of operating a data link in which a circuit or channel is established to switching facilities as, for example, in a public switched network. (T) (2) A connection established by dialing. Contrast with *nonswitched connection*.

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line.

Synchronous Data Link Control (SDLC). A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) Contrast with *binary synchronous communication (BSC)*.

SYSREC. System error file.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for end users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

system slowdown. A network control program mode of reduced operation invoked when buffer availability drops below a threshold level. The network control program limits the amount of new data that the system accepts while continuing normal output activity.

System Support Programs (SSP). An IBM licensed program, made up of a collection of utilities and small programs, that supports the operation of the NCP.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

tailing. A feature on a multichannel modem that allows another modem link to be attached to one of the channels. See also *fanout*, *multitailed*, and *twin-tailed*.

takeover. The process by which the failing active subsystem is released from its extended recovery facility (XRF) sessions with terminal users and replaced by an alternate subsystem. See *resource takeover*.

TAP. Synonym for *ACF/TAP*.

TCAM. Telecommunications Access Method. Synonymous with *ACF/TCAM*.

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

Telecommunications Access Method (TCAM). An access method used to transfer data between main storage and remote or local terminals.

teleprocessing network simulator (TPNS). A testing package that enables a user to test and evaluate teleprocessing systems before actual terminal installation.

teletypewriter exchange service (TWX). Teletypewriter service in which suitably arranged teletypewriter stations are provided with lines to a central office for access to other such stations throughout the U.S. and Canada. Both baudot- and ASCII-coded machines are used. Business machines may also be used, with certain restrictions.

temporary error. A resource failure that can be resolved by error recovery programs. Synonymous with *performance error*. Contrast with *permanent error*.

TG. Transmission group.

TH. Transmission header.

TIC. Token-ring interface coupler.

Time Sharing Option (TSO). An operating system option; for the System/370 system, the option provides interactive time sharing from remote terminals.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring adapter type 2. A token-ring interface coupler (TIC) supported only on an IBM 3745 Communication Controller. The adapter can be configured to support 4-Mbps (megabits per second) or 16-Mbps token-ring speed and to support subarea and peripheral nodes on the same adapter. When configured for 16-Mbps, the token-ring adapter type 2 provides the capability for early token release.

token-ring interface coupler (TIC). An adapter that can connect a 3720, 3725, or 3745 Communication Controller to an IBM Token-Ring Network.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

TPF. Transaction processing facility.

TPNS. Teleprocessing network simulator.

TR. Trace.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

Trace Analysis Program (TAP). Synonym for *Advanced Communications Function for the Trace Analysis Program (ACF/TAP)*.

transaction processing facility (TPF). A high-availability, high-performance system, designed to

support real-time, transaction driven applications. The specialized architecture of TPF is intended to optimize system efficiency, reliability, and responsiveness for data communication and database processing. TPF provides real-time inquiry and update to a large, centralized database, where message length is relatively short in both directions, and response time is generally less than three seconds. Formerly known as the Airline Control Program/Transaction Processing Facility (ACP/TPF).

Transmission Control Protocol (TCP). A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transmission group (TG). (1) A connection between adjacent nodes that is identified by a transmission group number. See also *parallel transmission groups.* (2) In a subarea network, a single link or a group of links between adjacent nodes. When a transmission group consists of a group of links, the links are viewed as a single logical link, and the transmission group is called a *multilink transmission group (MLTG).* A *mixed-media multilink transmission group (MMMLTG)* is one that contains links of different medium types (for example, token-ring, switched SDLC, nonswitched SDLC, and frame-relay links). (3) In an APPN network, a single link between adjacent nodes.

transmission group (TG) vector. A representation of an endpoint TG in a T2.1 network, consisting of two control vectors: the TG Descriptor (X'46') control vector and the TG Characteristics (X'47') control vector.

transmission header (TH). Control information, optionally followed by a basic information unit (BIU) or a BIU segment, that is created and used by path control to route message units and to control their flow within the network. See also *path information unit.*

transmission priority. A rank assigned to a message unit that determines its precedence for being selected by the path control component in each node along a route for forwarding to the next node in the route.

transmission subsystem (TSS). A line adapter that attaches to the IBM 3745 Communication Controller.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

TRFILE. Trace file.

TRS. Topology and routing services.

TSO. Time Sharing Option.

TSS. Transmission subsystem.

TWX. Teletypewriter exchange service.

type 2.1 node. A node that can be an APPN network node, an APPN end node, or a LEN node. It can also attach as a peripheral node to a subarea boundary node in the same way as a type 2.0 node.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The European version (E1) transmits 2.048 Mbps. The Japanese version (J1) transmits 1.544 Mbps.

U

UA. Unnumbered acknowledgment.

UDP. User Datagram Protocol.

UNBIND. In SNA, a request to deactivate a session between two logical units (LUs). Contrast with *BIND.*

upload. (1) To transfer programs or data from a connected device, typically a personal computer, to a computer with greater resources. (T) (2) To transfer data from a device, such as a workstation or a microcomputer, to a computer. Contrast with *download.*

V

V.24. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.25. In data communications, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

V.25 bis. A procedure defined by CCITT that allows call establishment and data transfer to take place over the same link. The support eliminates the need for two

physical lines or ports when automatic call units (ACUs) are employed in a switched connection.

V.35. In data communications, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

vector. The MAC frame information field.

virtual machine (VM). In VM, a functional equivalent of a computing system. On the 370 Feature of VM, a virtual machine operates in System/370 mode. On the ESA Feature of VM, a virtual machine operates in System/370, 370-XA, ESA/370, or ESA/390 mode. Each virtual machine is controlled by an operating system. VM controls the concurrent execution of multiple virtual machines on an actual processor complex.

Virtual Machine/Enterprise Systems Architecture (VM/ESA). An IBM licensed program that manages the resources of a single computer so that multiple computing systems appear to exist. Each virtual machine is the functional equivalent of a *real* machine.

Virtual Machine/Extended Architecture (VM/XA). An operating system that facilitates conversion to MVS/XA by allowing several operating systems (a production system and one or more test systems) to run simultaneously on a single 370-XA processor. The VM/XA Migration Aid has three components: the control program (CP), the conversational monitor system (CMS), and the dump viewing facility.

virtual route (VR). In SNA, either a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). See also *explicit route (ER)*, *path*, and *route extension (REX)*.

virtual route (VR) pacing. In SNA, a flow control technique used by the virtual route control component of path control at each end of a virtual route to control the rate at which path information units (PIUs) flow over the virtual route. VR pacing can be adjusted according to traffic congestion in any of the nodes along the route. See also *pacing*.

virtual route identifier (VRID). In SNA, a virtual route number and a transmission priority number that, when combined with the subarea addresses for the subareas at each end of a route, identify the virtual route.

virtual route pacing response (VRPRS). A nonsequenced, supervisory path information unit (PIU) that flows at network priority. It may overtake VR-sequenced PIUs and consists of a transmission header with no basic information unit (BIU) data.

virtual route sequence number. In SNA, a sequential identifier assigned by the virtual route control component of path control to each path information unit (PIU) that flows over a virtual route. It is stored in the transmission header of the PIU. Contrast with *session sequence number*.

Virtual Storage Access Method (VSAM). An access method for direct or sequential processing of fixed and variable-length records on direct access devices. The records in a VSAM data set or file can be organized in logical sequence by a key field (key sequence), in the physical sequence in which they are written on the data set or file (entry-sequence), or by relative-record number.

Virtual Storage Extended (VSE). An IBM licensed program whose full name is the Virtual Storage Extended/Advanced Function. It is a software operating system controlling the execution of programs.

Virtual Telecommunications Access Method (VTAM). An IBM licensed program that controls communication and the flow of data in an SNA network. It provides single-domain, multiple-domain, and interconnected network capability.

VIT. VTAM internal trace.

VLB. VTAM services local block.

VM. Virtual machine.

VM/ESA. Virtual Machine/Enterprise Systems Architecture.

VM/SNA console support (VSCS). A VTAM component for the VM environment that provides Systems Network Architecture (SNA) support. It allows SNA terminals to be virtual machine consoles.

VM/SP. Virtual Machine/System Product.

VM/XA. Virtual Machine/Extended Architecture.

VM/370. IBM Virtual Machine Facility/370.

VM/370 control program (CP). The component of VM/370 that manages the resources of a single computer with the result that multiple computing systems appear to exist. Each virtual machine is the functional equivalent of an IBM System/370 computing system.

VR. Virtual route.

VRID. Virtual route identifier.

VRPRS. Virtual route pacing response.

VSAM. Virtual Storage Access Method.

VSCS. VM/SNA console support.

VSE. Virtual Storage Extended. Synonymous with *VSE/Advanced Functions.*

VSE/Advanced Functions. The basic operating system support needed for a VSE-controlled installation. Synonym for *VSE.*

VSE/ESA. Virtual Storage Extended/Enterprise Systems Architecture.

VSE/SP. Virtual Storage Extended/System Package.

VTAM. Virtual Telecommunications Access Method. Synonymous with *ACF/VTAM.*

VTAM internal trace (VIT). A trace used in VTAM to collect data on channel I/O, use of locks, and storage management services.

W

WAN. Wide area network.

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with *local area network (LAN)* and *metropolitan area network (MAN).*

window. (1) A portion of a display surface in which display images pertaining to a particular application can be presented. Different applications can be displayed simultaneously in different windows. (A) (2) In data communication, the number of data packets a data terminal equipment (DTE) or data circuit-terminating equipment (DCE) can send across a logical channel before waiting for authorization to send another data packet. The window is the main mechanism of pacing, or flow control, of packets. (3) See *pacing window.*

window size. The specified number of frames of information that can be sent before receiving an acknowledgment response.

X

X.25. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. See also *packet switching.*

X.25 NCP Packet Switching Interface (NPSI). An IBM licensed program that allows SNA users to communicate over packet switching data networks that have interfaces complying with CCITT Recommendation X.25. It allows SNA programs to communicate with SNA or non-SNA equipment over such networks.

XA. Extended architecture.

XI. X.25 SNA Interconnection.

XID. Exchange identification.

XMIT. Transmit.

XRF. Extended recovery facility.

3

37CS. Deprecated term for *3746 Model 900 connectivity subsystem (CSS).*

Bibliography

NCP, SSP, and EP Library

The following paragraphs briefly describe the library for NCP, SSP, and EP. The other books dealing with the networking systems products—VTAM, NPSI, the NetView program, and NPM—are listed without the accompanying descriptions.

NCP V7R2, SSP V4R2, and EP R12 Library Directory (SC31-6259)

This book helps users locate information on a variety of NCP, SSP, and EP tasks. It also provides a high-level understanding of NCP, SSP, and EP and summarizes the changes to these products and to the library for NCP V7R1, SSP V4R1, and EP R12.

NCP V7R2 Migration Guide (SC31-6258)

This book helps users migrate an NCP generation definition from an earlier release to NCP V7R1. It also describes how to add new functions for NCP V7R1.

NCP, SSP, and EP Resource Definition Guide (SC31-6223)

This book helps users understand how to define NCP and EP (in the PEP environment) using SSP. It describes functions and resources and lists the definition statements and keywords that define those functions and resources.

NCP, SSP, and EP Resource Definition Reference (SC31-6224)

This book helps users code definition statements and keywords to define NCP and EP (in the PEP environment) using SSP. It also provides a quick reference of definition statement coding order and keyword syntax.

NCP, SSP, and EP Generation and Loading Guide (SC31-6221)

This book provides detailed explanations of how to generate and load NCP and EP (in the PEP environment) using SSP. It contains information for generating and loading under MVS, VM, and VSE.

NCP and SSP Customization Guide (LY43-0031)

This book helps users who are familiar with the internal logic of NCP and SSP to modify these products. It describes how to change NCP and SSP to support stations that IBM-supplied programs do not support.

NCP and SSP Customization Reference (LY43-0032)

This book supplements the *NCP and SSP Customization Guide*. It describes the resources and macroinstructions provided by IBM for customizing NCP and SSP.

NCP, SSP, and EP Messages and Codes (SC31-6222)

This book is a reference book of abend codes issued by NCP and EP in the PEP environment, and messages issued by the system support programs associated with NCP.

NCP, SSP, and EP Diagnosis Guide (LY43-0033)

This book helps users isolate and define problems in NCP and EP (in the PEP environment) using SSP. The primary purpose of the book is to help the user interact with the IBM Support Center to resolve a problem. In addition, it explains some of the diagnostic aids and service aids available with SSP.

&icndgat. (LK2T-1999, diskettes)

The Diagnosis Aid is an IBM OS/2 application used to diagnose NCP, SSP, and EP problems. This tool has all the information contained in the *NCP, SSP, and EP Diagnosis Guide*.

NCP and EP Reference (LY43-0029)

This book describes various aspects of the internal processing of NCP and EP in the PEP environment. It provides information for customization and diagnosis.

NCP and EP Reference Summary and Data Areas (LY43-0030)

This two-volume book provides quick access to often-used diagnostic and debugging information about NCP and EP in the PEP environment.

Other Networking Systems Products Libraries

The following books provide cross-product information for VTAM, NPSI, NetView, and NPM. For detailed information about these products refer to the library for each.

Networking Systems Library

The following list shows the books in the Networking Systems library.

Planning for NetView, NCP, and VTAM (SC31-7122)

Planning for Integrated Networks (SC31-7123)

Planning Aids: Pre-Installation Planning Checklist for NetView, NCP, and VTAM (SX75-0092)

IBM Networking Systems Softcopy Collection Kit (CD-ROM, SK2T-6012)

IBM Online Libraries: Softcopy Collection Kit User's Guide (GC28-1700)

VTAM Library

The following list shows the books in the VTAM V4R2 library.

VTAM Migration Guide (GC31-6491)

VTAM Release Guide (GC31-6492)

Estimating Storage for VTAM (SK2T-2007)

VTAM Network Implementation Guide (SC31-6494)

VTAM Resource Definition Reference (SC31-6498)

VTAM Resource Definition Samples (SC31-6499, book and diskettes)

VTAM Customization (LY43-0063)

VTAM Operation (SC31-6495)

VTAM Operation Quick Reference (SX75-0205)

Using IBM CommandTree/2 (SC31-7013)

VTAM Messages and Codes (SC31-6493)

VTAM Licensed Program Specifications (GC31-6490)

VTAM Programming (SC31-6496)

VTAM Programming Quick Reference (SX75-0206)

VTAM Programming for LU 6.2 (SC31-6497)

VTAM Diagnosis (LY43-0065)

VTAM Diagnosis Quick Reference (LX75-0204)

VTAM Data Areas for MVS (LY43-0064)

NPSI Library

The following list shows the books in the NPSI Version 3 library.

X.25 NCP Packet Switching Interface General Information (GC30-3469)

X.25 NCP Packet Switching Interface Planning and Installation (SC30-3470)

X.25 NCP Packet Switching Interface Host Programming (SC30-3502)

X.25 NCP Packet Switching Interface Diagnosis, Customization, and Tuning (LY30-5610)

X.25 NCP Packet Switching Interface Data Areas (LY43-0034)

X.25 NCP Packet Switching Interface Master Index (GC31-6206)

NTune Library

The following list shows the publications in the NTune library.

NTune User's Guide (SC31-6247)

NTuneNCP Reference (LY43-0035)

NetView Library

The following list shows the books in the NetView V2R4 library.

NetView General Information (GC31-7098)

Learning about NetView (SK2T-6017, diskettes)

Learning about NetView Graphic Monitor Facility (SK2T-6018, diskettes)

NetView Graphic Monitor Facility Reference Poster (SX75-0100)

NetView Automation Planning (SC31-7083)

NetView Storage Estimates (SK2T-6016, diskette for a PS/2 or a PS/55)

NetView Installation and Administration Guide (SC31-7084 for MVS)

NetView Installation and Administration Facility/2 Guide (or *NIAF/2 Guide*, SC31-7099)

NetView Administration Reference (SC31-7080)

NetView Bridge Implementation (SC31-6131)

NetView Tuning Guide (SC31-7079)

NetView Automation Implementation (LY43-0016)

NetView Customization Guide (SC31-7091)

NetView Customization: Writing Command Lists (SC31-7092)

NetView Customization: Using PL/I and C (SC31-7093)

NetView Customization: Using Assembler (SC31-7094)

NetView Operation (SC31-7086)

NetView Graphic Monitor Facility User's Guide (SC31-7089)

NetView Command Quick Reference (SX75-0090)

NetView Messages (SC31-7096)

NetView Resource Alerts Reference (SC31-7097)

NetView Application Programming Guide (SC31-7081)

NetView Resource Object Data Manager Programming Guide (SC31-7095)

NetView Problem Determination and Diagnosis (LY43-0101)

NPM Library

The following list shows the books in the NPM V2 library.

NetView Performance Monitor at a Glance (GH19-6960)

NetView Performance Monitor Concepts and Planning (GH19-6961)

NetView Performance Monitor User's Guide (SH19-6962)

NetView Performance Monitor Messages and Codes (SH19-6966)

NetView Performance Monitor Graphic Subsystem (SH19-6967)

NetView Performance Monitor Installation and Customization (SH19-6964)

NetView Performance Monitor Reports and Record Formats (SH19-6965)

NetView Performance Monitor Diagnosis (LY19-6381)

NetView Performance Monitor Desk/2 User's Guide (SH19-6963)

Related Publications

The following publications, though not directly related to NCP, may be helpful in understanding your network.

MVS/Extended Architecture Programming Library: Service Aids (GC28-1159)

NLDM Installation and Operations (SC30-3165)

Tuning and Problem Analysis for NCP/SDLC (GC24-1629)

Communication Controller Publications

372x Publications: The following list shows selected publications for the IBM 372x Communication Controller.

IBM 3720 Component Description (GA27-2749)

3720/3721 Communication Controllers Extended Services Guide (GA33-0066)

3720/3721 Communication Controllers Introduction (GA33-0060)

3720/3721 Communication Controllers Configuration Guide (GA33-0063)

IBM 3720/3721 Communications Controllers Maintenance Information Reference (SY33-2040)

3720/3725 Communication Controllers Principles of Operation (GA33-0013)

IBM 3725/3726 Communications Controller Expansion VHSA Maintenance Information (SY33-2034)

3745 Publications: The following list shows selected publications for the IBM 3745 Communication Controller.

IBM 3745 Communication Controller Introduction (GA33-0092 for the 3745-210, 3745-310, 3745-410, and 3745-610)

IBM 3745 Communication Controller Introduction (GA33-0138 for the 3745-130, 3745-150, and 3745-170)

IBM 3745 Communication Controller Configuration Program (GA33-0093)

IBM 3745 Communication Controller Problem Determination Guide (SA33-0096)

IBM 3745 Communication Controller Advanced Operations Guide (SA33-0097)

IBM 3745 Principles of Operation (SA33-0102)

3745 Communication Controller Hardware Maintenance Reference (SY33-2066 for the 3745-130, 3745-150, and 3745-170)

IBM 3745 Maintenance Information Reference (SY33-2056 for the 3745-210, 3745-310, 3745-410, and 3745-610)

NPDA Publications

The following publications contain information on Network Problem Determination Application.

Network Problem Determination Application User's Guide (SC34-2112)

Network Problem Determination Application Recommended Action Guide (SC34-2113)

Network Problem Determination Application User's Reference (SC34-2114)

SNA Publications

The following publications contain information on SNA.

Systems Network Architecture Technical Overview (GC30-3073)

Systems Network Architecture Format and Protocol Reference Manual: Management Services (SC30-3346)

Systems Network Architecture Formats (GA27-3136)

TCAM Publications

The following publications contain information on TCAM.

TCAM Diagnosis Guide (LY30-3137)

TCAM Diagnosis Reference (LY30-3052)

TCAM Operation (LY30-3136)

TCP/IP Publications

The following books contain information on Transmission Control Protocol/Internet Protocol (TCP/IP).

General: The following list shows selected books with general information on TCP/IP.

TCP/IP Introduction (GC31-6080)

IBM TCP/IP Tutorial and Technical Overview (GG24-3376)

MVS Publications: The following list shows selected books on TCP/IP for MVS.

IBM TCP/IP Version 2 Release 2.1 for MVS: Planning and Customization (SC31-6085)

IBM TCP/IP Version 2 Release 2.1 for MVS: User's Guide (SC31-6088)

VM Publications: The following list shows selected books on TCP/IP for VM.

IBM TCP/IP Version 2 Release 2 for VM: Planning and Customization (SC31-6082)

IBM TCP/IP Version 2 Release 2 for VM: User's Guide (SC31-6081)

IBM OS/2 Publications: The following list shows selected books on TCP/IP for IBM OS/2.

IBM TCP/IP Version 1.2 for OS/2: Installation and Maintenance (SC31-6075)

IBM TCP/IP Version 1.2 for OS/2: User's Guide (SC31-6076)

VM Publications

The following publications contain information on VM.

VM Diagnosis Guide (LY24-5241)

VM/ESA CP Command and Utility Reference (SC24-5519)

VM/ESA Group Control System Reference (SC24-5531)

VM/SP Operator's Guide (SC19-6202)

VM/XA CP Command Reference (SC23-0358)

VM/XA Dump Viewing Facility Operation Guide (SC23-0359)

VM/XA Group Control System Command and Macro Reference (SC23-0433)

Technical Bulletins

The following list shows selected technical bulletins.

"Held VR" Symptom, Problem or Normal Operation (GR28-0632)

ACF Network Flow Control (G325-0101)

VR Performances and Window Size Tuning (GR28-0724)

Index

Special Characters

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Communicating Your Comments to IBM

Network Control Program
System Support Programs
Emulation Program
Diagnosis Guide

NCP Version 7 Release 2
SSP Version 4 Release 2
EP Release 12

Publication No. LY43-0033-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  United States and Canada: **1-800-227-5088**
- If you prefer to send comments electronically, use this network ID:
  - IBM Mail Exchange: **USIB2HPD at IBMMAIL**
  - IBMLink*: **CIBMORCF at RALVM13**
  - Internet: **USIB2HPD@VNET.IBM.COM**

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Help us help you!

Network Control Program
System Support Programs
Emulation Program
Diagnosis Guide

NCP Version 7 Release 2
SSP Version 4 Release 2
EP Release 12

Publication No. LY43-0033-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

Phone No.

Help us help you!
LY43-0033-01

Cut o
Along

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department E15
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NORTH CAROLINA 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

LY43-0033-01

Cut or
Along

Help us help you!

Network Control Program
System Support Programs
Emulation Program
Diagnosis Guide

NCP Version 7 Release 2
SSP Version 4 Release 2
EP Release 12

Publication No. LY43-0033-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	☐	☐

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	☐	☐
Complete	☐	☐
Easy to find	☐	☐
Easy to understand	☐	☐
Well organized	☐	☐
Applicable to your task	☐	☐

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

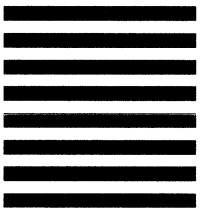
Phone No.

Help us help you!
LY43-0033-01

Cut o
Alon

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department E15
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NORTH CAROLINA 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

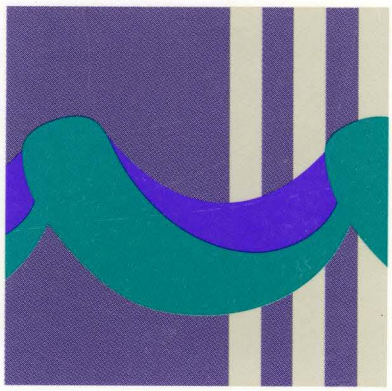
LY43-0033-01

Cut o
Alon

IBM®

Program Number: 5648-063

Printed in U.S.A.



LY43-0033-01