Advanced Communications Function for VTAM, Version 2

Advanced Communications Function for Network Control Program, Version 3

Advanced Communications Function for System Support Programs, Version 2

Network Communications Control Facililty, Version 2

Network Logical Data Manager

IBM

Network Program Products General Information

GC27-0657-1

Advanced Communications Function for VTAM, Version 2 Release 2
Program Number 5665-280

Advanced Communications Function for Network Control Program, Version 3
Program Number 5667-124

Advanced Communications Function for System Support Programs, Version 2 Release 2
Program Number 5735-XXA

Network Communications Control Facility, Version 2
Program Number 5668-947

Network Logical Data Manager, Release 2
Program Number 5668-971

Network Program Products General Information

GC27-0657-1
(File No. S370/4300-50)

Second Edition (February 1984)

This edition applies to the following program products:

1. Advanced Communications Function for the Virtual Telecommunications Access Method (ACF/VTAM) Version 2 Release 2 for the OS/VS2 (MVS) and MVS/XA operating systems (Program Number 5665-280)

2. Advanced Communications Function for the Network Control Program (ACF/NCP) Version 3 for the OS/VS2 (MVS) and MVS/XA operating systems (Program Number 5667-124)

3. Advanced Communications Function for Systems Support Programs (ACF/SSP) Version 2 Release 2 for the OS/VS2 (MVS) and MVS/XA operating systems (Program Number 5735-XXA)

4. Network Communications Control Facility (NCCF) Version 2 for the OS/VS2 (MVS) and MVS/XA operating systems (Program Number 5668-947)

5. Network Logical Data Manager (NLDM) Release 2 for the OS/VS2 (MVS) and MVS/XA operating systems (Program Number 5668-971)

Information about the optional ACF/VTAM Encrypt/Decrypt Feature is also included. Changes are made periodically to the information herein; before using this publication in connection with the operation of IBM systems, consult the latest *IBM System/370 and 4300 Processors Bibliography*, GC20-0001, for the editions that are applicable and current.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this publication is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program may be used instead.

Publications are not stocked at the address given below. Requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for reader's comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Department E03, P.O. Box 12195, Research Triangle Park, North Carolina U.S.A. 27709. IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1983, 1984

Preface

This book describes the services you can obtain from a telecommunication network operating with the following IBM program products:

- ACF/VTAM Version 2 Release 2
- ACF/NCP Version 3
- ACF/SSP Version 2 Release 2
- NCCF Version 2
- NLDM Release 2

It is directed to system programmers and data processing managers who have some experience with IBM networks.

Frequently in this book the names of these five program products are used without version or release numbers. You should assume that the version and release numbers used in the list above apply, unless otherwise noted. Publications cited for these products refer only to the versions and releases listed above.

Information in This Book

The information in this book is arranged as follows:

- Chapter 1 contains a general description of three types of network environments: single-domain, multiple-domain, and interconnected. The emphasis in this part is on the work that each type of network can do for you, and the variety and flexibility of its functions. Readers without a technical background will find this chapter more accessible.
- Chapter 2 describes the functions of each program product. The information here is arranged so that you can see which functions are new to you.
- Chapter 3 describes the hardware that the five program products need and the types of programs they operate with. It describes any problems of compatibility the program products may have with other programs. It also lists changes you may need to make in application programs, if your installation is migrating from previous releases of any the five program products.
- Appendix A lists devices and related programs that the program products support.
- Appendix B describes the libraries of books that IBM provides for the five program products. It also lists books on other programs, such as operating systems, that may be applicable to your network installation.

Since most of these libraries have been evolving toward a task-oriented structure, this appendix also provides:

  - A brief description of each book
  - A description of the task-oriented library structure
  - A chart showing the task-oriented structure of each library
  - (Where the library has changed considerably) charts showing the evolution to each current library from the libraries of previous releases

- Appendixes C through G are summaries of the five program products
- The glossary defines terms and abbreviations used throughout the book.

Notes:

1. Since this book describes those releases of IBM program products that are associated with SNA network interconnection, ACF/TCAM is not described as an alternative access method. All the program products except ACF/VTAM, however, operate with ACF/TCAM. Functions specifically designed for ACF/TCAM only are therefore preceded by the phrase "ACF/TCAM only."

2. In addition to the network program products included in this manual, there are others, for example the Network Problem Determination Application (NPDA) and INFO/Systems. For more information about these and other IBM products, contact your local branch office.

Product Names

The two operating systems under which ACF/VTAM Version 2 Release 2 operates are as follows:

- Operating System/Virtual Storage Release 2 (Multiple Virtual Storage), called OS/VS2 (MVS), is referred to as MVS.
- Operating System/Virtual Storage Release 2 (Multiple Virtual Storage/Extended Architecture), called OS/VS2 (MVS/XA) is also referred to as MVS. Where necessary to make the distinction, it is referred to as MVS/XA.

For the network program products discussed in this book, the following are used:

- *ACF/VTAM* for Advanced Communications Function for the Virtual Telecommunications Access Method
- *ACF/NCP* for Advanced Communications Function for the Network Control Program
- *ACF/SSP* for Advanced Communications Function for Systems Support Programs
- *NCCF* for Network Communications Control Facility
- *NLDM* for Network Logical Data Manager

Contents

Chapter 1. Introducing SNA Telecommunication Networks 1-1
The Organization of This Chapter 1-3
Single-Domain Networks 1-4
Network Structure 1-4
Types of Devices 1-5
Choosing Types of Lines 1-5
The Concept of Subareas 1-6
The Concepts of Owning, Activating, and Deactivating Network Resources 1-6
Session Flow 1-7
Network Operation 1-8
Network Performance 1-10
Problem Determination and Network Maintenance 1-11
Network Recovery 1-12
Network Security 1-13
Application Programming 1-13
Configuration Design 1-13
Multiple-Domain Networks 1-21
Network Structure 1-21
Sharing ACF/NCP Resources 1-21
Types of Connections 1-23
Session Flow 1-23
Network Operation 1-24
Network Performance 1-25
Problem Determination and Network Maintenance 1-26
Network Recovery 1-26
Configuration Design 1-27
General Considerations for Designing Networks 1-27
Intermediate Routing Nodes (IRNs) 1-28
Communication Management Configuration Networks 1-28
Interconnected Networks 1-35
Network Structure 1-36
Ownership of Gateway ACF/NCP Resources 1-36
Session Flow 1-36
Network Operation 1-37
Network Performance 1-38
Problem Determination and Network Maintenance 1-38
Network Recovery 1-39
Recovery at Network Boundaries 1-39
Recovery within Individual Networks 1-39
Network Security 1-39
Configuration Design 1-39
Single-Gateway Configuration 1-40
Multiple-Gateway Configurations 1-40
Tandem Configurations 1-42

Chapter 2. Network Program Product Functions 2-1
ACF/VTAM and ACF/NCP Functions 2-1
Introduction to ACF/VTAM Functions 2-1
Network Structure 2-2
Session Flow 2-2
Network Operation 2-2
Network Performance 2-2
Problem Determination and Network Maintenance 2-2
Network Recovery 2-2
Network Security 2-3
Application Programs 2-3
Introduction to ACF/NCP Functions 2-3
Network Structure 2-4
Session Flow 2-4
Network Operation 2-4
Network Performance 2-4
Problem Determination and Network Maintenance 2-5
Network Recovery 2-5
Network Security 2-5
Functional Enhancements to ACF/VTAM and ACF/NCP 2-5
How to Use the Tables 2-5

Network Structure 2-6
Session Flow 2-11
Network Operation 2-13
Network Performance 2-16
Problem Determination and Network Maintenance 2-19
Network Recovery 2-24
Network Security 2-26
Application Programming 2-27
ACF/SSP Functions 2-28
ACF/NCP Generation Procedure 2-28
Generation Language 2-29
Generating Multiple ACF/NCPs 2-29
Communication Controller Assembler 2-29
Conditional Assembly Removal 2-29
Loader Utility 2-29
Dump Utility 2-31
Dynamic Dump Utility 2-31
Trace Analysis Program 2-31
Configuration Report Program 2-32
NCCF Functions 2-32
Introduction to NCCF Functions 2-32
NCCF and Communication Network Management (CNM) 2-32
Basic NCCF Functions 2-33
Functional Enhancements to NCCF 2-34
Logical Overview of NCCF Processing 2-39
NLDM Functions 2-41
Session Awareness Data 2-47
Session Trace Data 2-49
Response Time Data 2-49

Chapter 3. Requirements and Compatibilities 3-1
ACF/VTAM 3-1
Storage Requirements 3-1
Hardware Requirements 3-1
Programming Requirements 3-1
Compatibility 3-3
ACF/NCP 3-3
ACF/VTAM Application Programs 3-3
BTAM Application Programs 3-4
Related IBM Programs 3-4
Cross-Domain Communication 3-5
Cross-Network Communication 3-6
Conversion 3-6
ACF/VTAM Application Programs 3-6
BTAM Application Programs 3-6
Data Security, Auditability, and Control 3-7
ACF/NCP and ACF/SSP 3-7
Storage Requirements 3-7
Hardware Requirements 3-7
Programming Requirements 3-7
Compatibilities 3-8
compatibility 3-8
NCCF 3-8
Storage Requirements 3-8
Hardware Requirements 3-8
Programming Requirements 3-8
Compatibilities 3-10
NLDM 3-10
Storage Requirements 3-10
Hardware Requirements 3-10
Programming Requirements 3-10
Compatibilities 3-11

Appendix A. Supported Products A-1
Products Supported by ACF/VTAM Version 2 Release 2 A-1
Network Terminal Option (NTO) A-1
Communication Controllers Supported by ACF/VTAM Version 2 Release 2 A-5
Programs Supported by ACF/VTAM Version 2 Release 2 A-6
Products Supported by ACF/NCP A-7

SDLC Control Units and Display Stations A-7
BSC Control Units and Display Stations A-7
Start-Stop Stations A-8
Programs Supported by ACF/NCP A-8
Products Supported by NCCF Version 2 A-9
Controllers A-9
Controllers/Display Units A-9
Display Units A-9
Printers A-10
Access Methods A-10
CNM Products A-11
Network Problem Determination Application (NPDA) A-11
Network Logical Data Manager (NLDM) A-11
Multiple Virtual Storage/Operator Communication Control Facility (MVS/OCCF) A-11
Information/Management Feature of Information/System Release 2 A-11
Products Supported with NLDM A-11

Appendix B. Library Summaries B-1
Organization of the Libraries B-1
Abstracts of Publications B-2
ACF/VTAM Publications B-2
Evolution of the ACF/VTAM Library B-8
ACF/NCP Publications B-13
Evolution of the ACF/NCP Library B-18
SSP Publications B-21
NCCF Publications B-25
Evolution of the NCCF Library B-27
NLDM Publications B-29
Related Publications B-31
Systems Network Architecture (SNA) Publications B-31
Cryptography Publications B-31
Network Terminal Option (NTO) Publications B-32
Network Problem Determination Application (NPDA) Publications B-32
TSO and TSO/VTAM Publications B-32
Publications on Other Access Methods B-32
OS/VS Publications B-33
MVS Publications B-33
MVS/Extended Architecture Publications B-34

Appendix C. Advanced Communications Function for VTAM Version 2 Release 2: Summary C-1
Testing Period C-1
License C-1
Program Services C-1
Local Licensed Program Support C-1
Warranty C-2
Availability of Licensed Program C-2

Appendix D. Advanced Communications Function for NCP Version 3: Summary D-1
Testing Period D-1
License D-1
Program Services D-1
Local Licensed Program Support D-1
Warranty D-1
Availability of Licensed Program D-2

Appendix E. Advanced Communications Function for SSP Version 2 Release 2: Summary E-1
Testing Period E-1
License E-1
Program Services E-1
Local Licensed Program Support E-1
Warranty E-1
Availability of Licensed Program E-2

Appendix F. Network Communications Control Facility Version 2: Summary F-1
Testing Period F-1
License F-1
Program Services F-1
Local Licensed Program Support F-1

Warranty F-2
Availability of Licensed Program F-2

Appendix G. Network Logical Data Manager Release 2: Summary G-1
Testing Period G-1
License G-1
Program Services G-1
  Local Licensed Program Support G-1
Warranty G-2
Availability of Licensed Program G-2

Glossary X-1
  Reference Words Used in the Entries X-1

Index X-23

Figures

1-1. An Example of Connecting ACF/NCPs 1-6
1-2. An Example of Alternate Routes 1-14
1-3. An Example of Configuring Lines for Less Expense 1-16
1-4. An Example of a Single-Domain Network 1-17
1-5. An Example of Shared Ownership 1-20
1-6. Considerations for Using Various Configurations 1-26
1-7. Examples of Intermediate Routing Node (IRN) Configurations 1-27
1-8. An Example of a Multiple-Domain Network 1-29
1-9. Example of Multiple ACF/NCPs Acting as Gateways 1-37
1-10. An Example of Tandem Interconnected Networks (Adjacent) 1-38
1-11. An Example of Tandem Interconnected Networks (Nonadjacent) 1-39
1-12. An Example of Interconnected Networks. 1-41
2-1. ACF/VTAM and ACF/NCP Functions Used in Network Structure 2-7
2-2. Cross-Domain Links between ACF/NCPs in Link-Attached Communication Controllers 2-9
2-3. Shared Ownership of an ACF/NCP 2-9
2-4. ACF/VTAM and ACF/NCP Functions Used in Session Flow 2-12
2-5. ACF/VTAM and ACF/NCP Functions Used in Network Operation 2-14
2-6. ACF/VTAM and ACF/NCP Functions Used in Network Performance 2-17
2-7. ACF/VTAM and ACF/NCP Functions Used in Problem Determination and Network Maintenance 2-20
2-8. ACF/VTAM and ACF/NCP Functions Used in Network Recovery 2-24
2-9. ACF/VTAM and ACF/NCP Functions Used in Network Security 2-26
2-10. ACF/VTAM and ACF/NCP Functions Used in Application Programming 2-27
2-11. Functional Enhancements to NCCF Since Version 1 Release 1 2-35
2-12. Overview of NCCF Operation 2-40
2-13. Functions in NLDM Releases 1 and 2 2-43
2-14. Resources that Can Have Sessions Traced 2-45
3-1. Factors for Moving Programs from Prior Releases of ACF/VTAM or VTAM Level 2 3-4
3-2. NCCF Functions Available with ACF/VTAM and ACF/TCAM 3-9
3-3. Subsystem Sessions Supported by the Terminal Access Facility 3-9
A-1. Terminal Products Supported by ACF/VTAM Version 2 Release 2 A-2
A-2. Terminals Supported by TSO/VTAM A-4
A-3. IBM Program Products Supported by ACF/VTAM Version 2 Release 2 A-6
B-1. The ACF/VTAM Version 2 Release 2 Library B-3
B-2. Evolution of the ACF/VTAM Version 2 Release 2 Library B-9
B-3. The ACF/NCP Version 3 Library B-14
B-4. Evolution of the ACF/NCP Version 3 Library B-19
B-5. The ACF/SSP Library B-21
B-6. The NCCF Version 2 Library B-25
B-7. Evolution of the NCCF Version 2 Library B-28
B-8. The NLDM Release 2 Library B-29

Chapter 1. Introducing SNA Telecommunication Networks

This chapter is an an overview of five IBM program products that work together in various types of networks. The emphasis is on the work that such networks can do for you, rather than the concepts upon which their functions are based. A more detailed discussion of network concepts is in the publication *SNA Concepts and Products*. A brief description of the functions of each of the five program products is in Chapter 2 of this book. If you would like to know more about the functions of the IBM network program products themselves, see Appendix B, "Library Summaries", for descriptions of the appropriate books.

The networks described here use the following five IBM program products:

- ACF/VTAM for providing an interface between resources in a network or interconnected networks as the telecommunication access method
- ACF/NCPs for controlling sets of devices and for forwarding information along the network paths
- ACF/SSP for performing utility functions in connection with ACF/NCPs, such as generating an ACF/NCP or loading it into a communication controller
- NCCF for performing operator functions, such as entering commands to automate network operation and providing an interface with the network for network management application programs
- NLDM for collecting, correlating and storing session-related and problem-determination information for online user access.

SNA networks allow you to send information from one location in your company to another. The information can range in size from a one-line cash transaction to book-size documents.

At an office in Los Angeles, for instance, you might obtain the following from another office in Chicago:

- Information stored in Chicago, such as a document or a list of sales to a particular customer
- A service, such as a scientific calculation or the rendering of a bank balance or the editing of a document
- Periodic information, such as stock market prices or announcements broadcast from the home office.

The office in Chicago might obtain the following from the Los Angeles office:

- A report on sales for the previous day or week
- A running log of events during a manufacturing process, such as integrated circuit processing

- Random entries and withdrawals of money as they occur at a cashier's office, or sales as they occur at a retail outlet.

IBM networks are made up of *hardware* elements and *software* elements.

Hardware consists of the physical elements that you can see. This book concerns the following hardware:

- *Processors* contain large storage areas for computing and manipulating data.
- *Communication controllers* are used as nodes for forwarding data through the network and as controllers to which various kinds of devices can be attached.
- *Devices* can be connected to processors or communication controllers. They range widely in purpose and type, for example:
  - Display terminals
  - Printers
  - Banking terminals
- *Link connections* are the electronic connections among processors, communication controllers, and devices. There are two basic types: telecommunication lines and channels. Communication controllers are connected to other communication controllers or to devices by telecommunication lines, which can range in type from public telephone lines to satellite transmissions. Processors are attached to communication controllers, devices, and other processors by channels, which allow limited-distance connections.

Software consists of sets of instructions called programs. In telecommunication, programs are used to run processors, communication controllers, and certain devices. This book concerns the following software:

- *ACF/VTAM* operates in a processor as an access method. It sends and receives data through a network on behalf of application programs.
- *Application programs* also operate in the processor with ACF/VTAM, which provides them with access to devices and other application programs in the network or interconnected networks. Application programs perform work you want done, such as scientific computation, accounting services, or text editing. You can create these programs yourself, or buy them from IBM or other software sources.
- *ACF/NCP* operates in a communication controller. It controls and services the devices attached to it and transmits data from its devices to other network elements and receives data for the devices. It also forwards data it may receive as a node along a route between the processor and other communication controllers. ACF/NCP can operate in the same communication controller with other IBM program products that supplement its actions, such as the Network Terminal Option (NTO) and Network Routing Facility (NRF). You can also write your own substitutes for these programs or routines for special activities.

- *ACF/SSP* is a library of utility programs that operate independently in the communication controller and processor or with ACF/VTAM to provide such functions as loading or dumping an ACF/NCP.

- *NCCF* operates in a processor as an ACF/VTAM application program. It provides a program base for network management by supplying network operations, access method services, operating system services, data storage facilities, and facilities that allow you to customize NCCF to your business. NCCF operators can issue operator-control commands from a central operator terminal (or from multiple, distributed terminals) to host processors in a multiple-domain network.

- *NLDM* operates with NCCF. It provides online access to session-related information for monitoring network operation and to aid in communication network problem determination.

Notes:

1. ACF/VTAM, NCCF, NLDM, and all other application programs run under the control of another program, called an *operating system*. The network program products described in this book can run under the MVS or MVS/XA operating system.

2. All the IBM program products described here conform to an IBM telecommunication standard called Systems Network Architecture (SNA). SNA gives you the following advantages:

   - It encompasses a wide range of hardware and software products that provide uniform functions and present uniform interfaces to each other.

   - You can send and receive data independently of the method of transmission.

   - You do not need to install separate connections for different kinds of terminals or applications.

   - When you expand your SNA network, the original investment in application programs and telecommunication facilities can for the most part be preserved.

The Organization of This Chapter

The following description of IBM telecommunication networks with ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, and NLDM is organized around three kinds of networks:

- Single-domain networks (a domain consists of an ACF/VTAM and all the resources it controls)

- Multiple-domain networks (two or more ACF/VTAMs and their resources)

- Two or more interconnected networks

Note: Associated with the descriptions of the three types of networks are three diagrams: Figure 4, Figure 8, and Figure 12. Each diagram unfolds, so that you can refer to it as you read the text describing the network it illustrates.

The diagrams have been packaged at the back of the book. Please insert them at the places in the book indicated by their page numbers.

In describing these network environments, we will discuss the following topics:

- Network Structure: how you arrange and distribute network elements
- Session flow: how information passes from one network location to another
- Network operation: how you can control a network
- Network performance: strategies for making your network run more efficiently
- Problem determination (ways you can determine the causes of failures) and network maintenance (how you can monitor network events and detect symptoms of possible failure)
- Network recovery: how failing network elements can recover and how the effects of failure can be minimized
- Security: how you can protect data passing through the network from unauthorized use
- Application programming: how application programs obtain telecommunication services from ACF/VTAM
- Configuration design: factors to consider in designing a configuration for your needs

Single-Domain Networks

Figure 4 shows a single-domain network. In this network, terminals in Los Angeles (attached to NCP1) can communicate with application programs in the processor in Chicago as easily as can the terminals in Chicago.

Network Structure

In this section the following will be discussed:

- Types of devices that are available
- Types of lines that are available
- The concept of subareas
- The concept of owning network resources

Types of Devices

Appendix A lists all the devices supported in an ACF/VTAM network. In this appendix, the devices cited as channel-attached are those that can be attached directly to a processor. Those cited as "link-attached" can be connected to a communication controller.

Some types of devices are:

- Printers for making hard copies of data
- Interactive devices for entering data and displaying it
- Industrial subsystems for:
  - Banking and finance
  - Retail stores
  - Supermarkets
  - Plant communications
  - Manufacturing process monitoring
- Processors, such as the IBM Personal Computer and the IBM 8100 Information System.

Choosing Types of Lines

There are various types of lines available. Choices can be based on the following:

- Line speed: the maximum amount of data that can be transmitted per second.
- Device requirements: the type of link protocol for data transmission that a device requires, for example, binary synchronous control (BSC), start-stop, and synchronous data link control (SDLC).
- Connections: the manner in which terminals are connected into a network. For example, some of your terminals could be on switched lines where the terminal operator dials and creates a temporary connection, as opposed to nonswitched lines, which have permanent connections.

Communication controllers and devices are attached to processors by channels. Communication controllers are attached to other communication controllers by SDLC lines and to devices that they control by various types of lines, depending on device requirements. Multiple communication controllers can be connected to each other. For example, the configuration in Figure 1-1 is possible.

Two communication controllers can be connected by more than one line. Also, sets of one or more lines called *transmission groups* (TGs) can be used logically as if they were all one line. If one line in a multiple-line TG fails, the remaining lines are used for the transmission, and no data is lost.

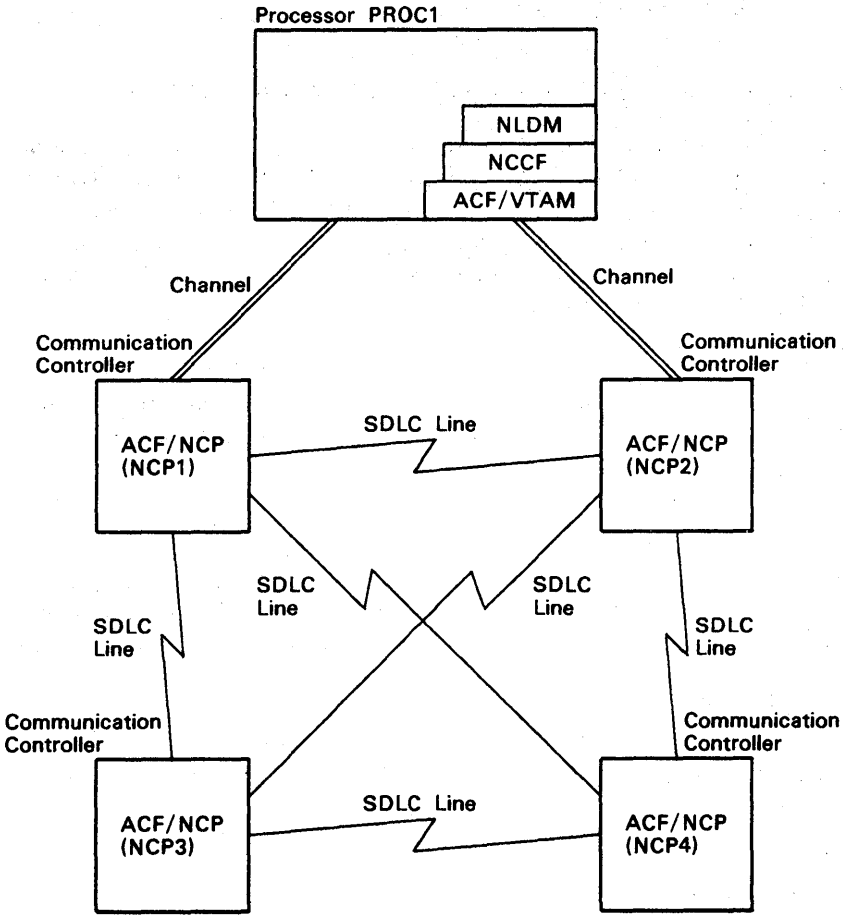


Figure 1-1. An Example of Connecting ACF/NCPs

The Concept of Subareas

Under SNA, a domain is a set of subareas. A subarea can be (1) an ACF/NCP and all the resources it controls or (2) an ACF/VTAM and all the resources it controls. In Figure 4 the following are subareas:

- NCP1 and its attached terminals
- NCP2 and its attached terminals
- ACF/VTAM, the network operator terminal, the application programs, NLDM, and NCCF.

Each subarea has a unique number, used as part of the network addresses of its resources.

The Concepts of Owning, Activating, and Deactivating Network Resources

In a single-domain network, ACF/VTAM "owns" a resource— an application program, an ACF/NCP, a line, a device— when it activates the resource. ACF/VTAM "activates" a resource by first determining that the resource is powered-on. It then informs the resource that the resource is active and indicates the active status in its own network configuration records. The resource is "active" in the sense that it is eligible to communicate with another active

resource in the domain. The resource continues to be active until deactivated by ACF/VTAM, that is, ACF/VTAM informs the resource it is inactive and so notes that status in its own records.

The concept of a resource being active or inactive allows you to control the use of resources in the network. You can define a resource to ACF/VTAM as active or inactive, and whenever the resource is powered-on ACF/VTAM will either activate it or leave it inactive as defined. The ACF/VTAM operator can also issue a command to ACF/VTAM to activate a resource previously defined as inactive.

As the owner of an application program, ACF/VTAM initiates, controls, and terminates sessions between it and the devices and other application programs it owns. It is also notified of errors associated with the resource or its sessions.

Session Flow

Communication between an application program and a terminal or another application program is called a *session*. ACF/VTAM is the control point that establishes the session between the two session partners. ACF/VTAM initiates sessions between itself and ACF/NCPs and devices whenever these resources are activated. Other sessions occur when:

- A person at a display terminal enters a request to initiate a session with an application program, for example, to get information from a file controlled by the program.

- An application program needs to communicate with another application program, for example, to prepare a financial report using information controlled by an accounting program.

- A terminal remains associated with a particular application program as long as they are both active, for example, a banking terminal and the associated central accounting program. For this type of session, ACF/VTAM can establish the session as the result of either:

  A request from the application program, or

  A combination of operator commands and the definition statement for the terminal, once the terminal and application program are both active.

When a session is established, it is assigned a route from a predefined list, and session data flows over that route until the session terminates. Ordinarily, the speed of the lines would determine the speed with which the data flows, but there are other factors to consider:

- *Amount of data*. If there is more data scheduled for transmission over the line than can currently be sent, then some of the data will be queued for later transmission. This delay of the transmission will decrease the speed of the data flow.

- *Route configuration*. Referring to Figure 1-1, if a session flows over a route from PROC1 through NCP1 to NCP2, NCP1 is a *routing node*. NCP1 examines the data coming over the channel, determines which route to send it over, and places it on the line to NCP2. This checking adds some time to the transmission, in addition to the time spent on the channel and the line.

- *Storage space in the routing node.* Each routing node must provide storage space for data it is sending and receiving. If more data is coming in than it has space for, it must send responses to neighboring nodes indicating that they cannot send data until it has enough free storage.

The first factor can be dealt with by understanding the pattern of traffic through your network. In Figure 1-1, for example, you could distribute sessions between PROC1 and NCP4 over four different physical paths. You could assign the sessions different transmission priorities with session data having high priority so it is scheduled ahead of session data with low or medium priority.

In designing the route configuration, cost must also be considered. For example, in Figure 1-3 NCP2 could be eliminated as a routing node by placing Seattle and Phoenix on separate lines to the home office, depending on the costs.

The problem of storage space in routing nodes can be alleviated by balancing data flow. It can also be helped by the pacing capability available in ACF/VTAM and ACF/NCP. They have two pacing mechanisms: *session pacing* to limit the amount of data that can be sent at one time between elements of the network and *route pacing* to control the flow of data along an entire route. You can modify both mechanisms in ACF/VTAM and ACF/NCP.

Network Operation

In a single-domain network, the ACF/VTAM operator at the system console can enter commands that will start ACF/VTAM, load ACF/NCPs into the communication controllers, and start up the application programs needed to do your company's work. While the network is operating, the operator can monitor network events through messages from ACF/VTAM on the terminal screen and take actions as needed. The operator can also deactivate the network at the end of the day when hardware or software maintenance must be done.

At start time, much time and human error can be saved through sets of commands called *start procedures* that the ACF/VTAM operator can use to perform activations of network elements automatically.

The operator can also ask ACF/VTAM to display the status of such things as storage, available resources, and sessions. The operator can activate network elements and deactivate them; request ACF/VTAM to collect information on how the network is operating; and invoke tests to determine, for example, whether a line is active.

When ACF/VTAM operates without NCCF, one operator must deal with messages from ACF/VTAM and the system, as well as from other subsystem application programs using ACF/VTAM services. You can alleviate this condition by using NCCF with ACF/VTAM.

Using NCCF functions, you can distribute network operations responsibility among a hierarchy of operators and, in addition, allow these operators control over a number of IBM subsystems:

- Multiple terminals can be designated as NCCF network operator terminals. NCCF operators can issue access method commands, commands invoking NCCF functions, and commands you can create to enhance or supplement NCCF commands.

  You can limit the commands, or operands within commands, an NCCF network operator can issue. You can also restrict the span of an operator's control to a subset of network resources (not supported under ACF/TCAM). These facilities allow you to establish a hierarchy of operator control.

  You can overlap spans of control so that more than one NCCF network operator can control the same set of resources. This allows you to provide for backup operators.

- Using the NCCF Terminal Access Facility, NCCF network operators can control a number of subsystems, such as IMS/VS and CICS/MVS. One operator can control any combination of these subsystems simultaneously from an NCCF terminal without logging off NCCF or using separate, dedicated terminals for each subsystem. This facility can help you to further define functional areas of control in a network control operation.

  For a description of these subsystems and a list of the ones supported under each access method, see the section on NCCF in "Appendix A. Supported Products."

NCCF can also help you automate network operations to relieve operators of repetitious actions, reduce the chance of human error, and provide rapid responses to network events. You can code sequences of commands, called command lists (CLISTs), each of which can be invoked by a single operator command. CLISTs can be made conditional through NCCF control statements for determining the sequence of execution. CLISTs can contain arithmetic functions, condition-testing, and user-defined, as well as NCCF, variables.

A CLIST can also be invoked as the result of NCCF receiving a specified access method message. This permits automatic responses to error messages, for example, reactivation of a link in response to a report of its failure.

CLISTs are one method of customizing NCCF to fit the needs of your business. Other ways are:

- Coding command processors to perform your own NCCF commands. You can also have command processors invoked when NCCF receives access method messages or by exit routines (see below).

- Initiating commands and CLISTs with a timer. Application programs could automatically be activated, for example, at a specific time of day or at timed intervals.

- Writing exit routines to be called during NCCF input and output processing. Exit routines can, for example, modify messages presented to the operator or prevent certain messages from reaching a particular network operator.

- Writing your own subtasks. An example would be a subtask for central control of a resource such as a data base.

Using NLDM with NCCF, operators can:

- Determine session history.
- Display the session configuration.
- View problem determination information, such as traces, interactively.
- Collect actual end user response time data as measured by the Response Time Monitor.
- Display response time data interactively (optionally in color), graphically comparing it to a predetermined objective by terminal and by session.

For additional uses of NCCF, see the section "Problem Determination and Network Maintenance."

Network Performance

SNA telecommunication networks provide a number of ways for monitoring network performance:

- ACF/VTAM provides the following:
  - Displays of ACF/VTAM storage use to help define storage allotments for greater efficiency. This data can also be traced on a continuing basis.
  - Tuning statistics on how efficient traffic is over a channel between ACF/VTAM and an ACF/NCP or a channel-attached device.
  - Operator messages on network events and operator-requested displays of the status of network elements.
- ACF/NCP provides:
  - Information about the percentage of available 3705 or 3725 machine cycles used for instruction processing, cycle sharing, and maintenance.
  - Measurements of data activity (such as the number of bytes sent and received) that involves ACF/NCP resources (such as links and boundary LUs) or that involves the ACF/NCP itself. This is done through the Network Performance Analyzer in ACF/NCP.
- With NCCF as its base, the Network Problem Determination Application (NPDA) program product with the Threshold Analysis and Remote Access Feature can give you an analysis of IBM 3600 and 4700 Finance Communication System performance.
- With NCCF as its base, the Network Logical Data Manager (NLDM) program product, in conjunction with terminal control units equipped with the Response Time Monitor feature, can accurately measure and display end-user response time data.

Using this information, you can:

- Reconfigure data paths, reroute sessions, and change the priorities of sessions.
- Change the parameters of ACF/VTAM storage.
- Redefine sets of lines between ACF/NCPs as transmission groups (see "Configuration Design" above).
- Adjust transmission group threshold counts.
- Adjust negative response times for BSC and start-stop devices.
- Redefine pacing parameters.
- Adjust the times ACF/VTAM and ACF/NCP wait for certain events, for instance, delaying transmission of data over a channel so that the data can be sent in larger amounts and thus reduce the number of I/O operations.

Problem Determination and Network Maintenance

You can collect information about the network that will help you keep it operating, and, if a failure occurs, determine the reason. You can:

- Run tests to determine if:
  - A link between an ACF/NCP and a device is active.
  - A terminal or application program is connected to ACF/VTAM.
  - A route is active.
- Obtain dumps of ACF/NCP storage—either all of the ACF/NCP storage or sections of it dynamically (while it is running). For a 3725 Communication Controller, you can obtain dumps of the microcode for the communication scanner processor (CSP) and the maintenance and operator subsystem (MOSS).
- Record events taking place in network hardware, such as line failure.
- Keep a running hard-copy log of terminal activity for each NCCF network operator. This printout includes time-stamped commands, responses, and messages, along with the operator ID associated with each entry. The information can be used to document and analyze network problems local to each operator. You can also keep an NCCF disk log on the activity of all the operators, for use as an audit trail.
- Using the NPDA program on NCCF as a base, keep a running account of hardware errors, including operator messages when error counts exceed defined limits.
- Using NLDM, trace session message traffic in a host processor, examine session trace information in an ACF/NCP, display and test the connectivity of a route used for a session, and determine the session protocols used for the session.

- With the trace analysis program (ACF/TAP) under ACF/SSP, analyze trace data supplied by ACF/VTAM and ACF/NCP and provide network data traffic and network error reports.

- Trace the following:

  - The contents of ACF/VTAM inbound and outbound storage areas, to make sure that ACF/VTAM has not altered the messages it is forwarding.

  - Message traffic between ACF/VTAM and other elements in the network, to determine that messages are not being lost in transit.

  - The status of a line each time the ACF/NCP sends or receives data over the line, to determine that the line is working.

  - The sequence of messages entering and exiting a transmission group, to determine that the transmission group is working.

  - Message traffic between an application program and ACF/VTAM.

  - The movement of PIUs through the network. For a 3725 Communication Controller, this includes a trace of messages passing to and from a line at the ACF/NCP communication scanner processor (CSP) line scanner.

  - Events that occur within ACF/VTAM, such as the scheduling of work, storage management, and the flow of messages. When trying to diagnose a failure in ACF/VTAM, this helps you reconstruct the sequence of events leading up to it.

Using NCCF with NPDA and NLDM combines problem determination and network recovery. Malfunctions in a line reported by NPDA could be used to invoke an NCCF command list (CLIST) that would reactivate the line. By using NLDM, a network operator could detect a session failure and then, using a CLIST, save the problem determination data for further analysis and restart the session.

Network problems are often performance-related, and facilities discussed previously under "Network Performance" can often be used to isolate such problems.

Network Recovery

As described later under "Configuration Design," you can have backup replacements for processors, communication controllers, lines, and devices. The failing hardware can be switched off, and the replacement switched on. As shown in Figure 1-2, when a line or communication controller fails, sessions can be rerouted through other lines and communication controllers when the session is reestablished. Also, a line within a multiple-line transmission group is automatically backed up by the others in the group.

When an ACF/VTAM or ACF/NCP fails, the ACF/VTAM operator can restart and restore ACF/VTAM's records of the ACF/NCP configuration to where the failure occurred.

When an application program loses a session due to the failure of a node or line along the route, the program or terminal operator can reinitiate the session over another route.

Network Security

You can prevent unauthorized use of your network by limiting access to it and by protecting the data that flows through it. Access can be limited as follows:

- Terminal operators requesting sessions with application programs can be required to furnish IDs and passwords. You can also write routines that will authorize access to certain application programs. Application programs requesting sessions with other application programs are limited in the same way. Their access to terminals can also be limited.

- Application programs can get telecommunication services from ACF/VTAM only by supplying IDs and, if required, passwords.

Data can be protected as it is transmitted over public lines. Using IBM program products, you can have data encrypted at one location and decrypted at its destination.

Application Programming

Application programs request telecommunication services through macro instructions that expand into calls to ACF/VTAM. Generally, application programmers do not have to be aware of network considerations, for instance which lines or ACF/NCPs are being used to transmit their programs' information to their destinations. For certain network events, however, ACF/VTAM gives control to specific functions in the application program called *exit routines*. These routines allow the application program to handle events such as a request for a session with the application program or notification of an error in the network.

Configuration Design

You can use the flexibility of an SNA network to design the configuration to suit the special needs of your business. These needs can be summarized as:

- Performance

- Availability

- Ease of operation

Performance: Performance expectations may depend on the job being done. For example, people sitting at terminals expect quick responses from the programs they are in communication with. An application program communicating with another application program may not have the same need. If your telecommunication traffic consists mostly of interactive sessions over short distances with people at terminal displays, lower-speed lines may be adequate for the small and intermittent amounts of data that are exchanged, and still provide the required response time. Steady, long bursts of information might require higher-speed and more expensive lines.

Availability: Availability is the degree to which a resource is ready when needed. If you must minimize interruptions for some part of your network, you might want backup hardware for it. For example, if NCP2 in Figure 4 were the focal point for message traffic from branches all over the country, you might want a backup communication controller there. Using multiple lines in a transmission group is another form of backup. Backup processors, backup communication controllers, and backup lines are frequently used for application programs that require high availability, such as airline reservation systems.

The ability to define multiple routes can also be used for backup. For example, the lines between Los Angeles and Chicago can instead be configurated as shown in Figure 1-2 if you want an alternative path to the Los Angeles office in case the primary path became unavailable.

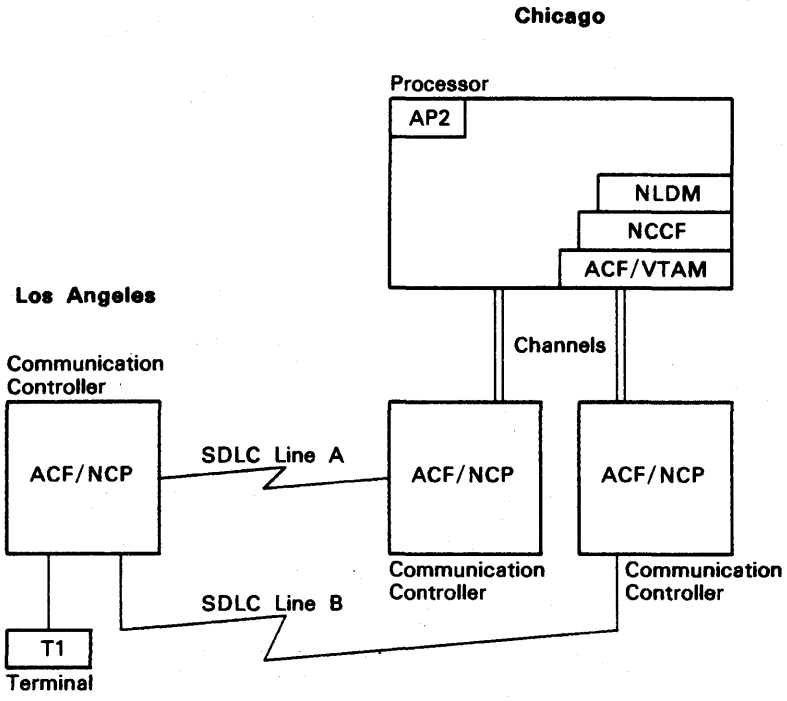


Figure 1-2. An Example of Alternate Routes

If there is a session between device T1 and application program AP2 in the processor and line A fails, the session also fails. However, the session partners (the terminal user and the application program) can ask ACF/VTAM to reestablish the session, and ACF/VTAM can do so using line B. NLDM provides the network operator with easy access to session information and route configuration data through panel displays. The network operator, using this information and (if necessary) session trace data, can analyze the failure.

Availability might not be as important for some parts of your network. For example, you may not need a separate line from the main office to each branch office. If, as shown in Figure 3, there were branch offices in Seattle, Los Angeles, and Phoenix, you could use NCP1 as a message concentrator, thus eliminating the cost of separate lines between Phoenix and the main office and Seattle and the main office.

Ease of Operation: Part of configuration design involves arranging resources in convenient groups. When resources are defined to ACF/VTAM and ACF/NCP, you can define them in sets called "major nodes" that the operator can activate as a set, rather than individually. For example, you might have a set of application programs that put together a monthly report. These programs can be defined together in a major node, perhaps called MONTHRPT. On the appropriate day each month the operator would start the application programs and then with one ACF/VTAM command activate them all. With NCCF command lists (see the description of NCCF functions under "Network Operation" earlier in this section), you can activate several major nodes with one command.

When the configuration of the resources controlled by an ACF/NCP fluctuates according to work needs, the operator can also use a dynamic reconfiguration facility to redefine the configuration temporarily without having to regenerate the ACF/NCP and interrupt service.

Note: The section "Configuration Design" under "Multiple-Domain Networks" presents some information that also applies to single-domain networks. It is presented there, because the multiple-domain configuration allows more scope for examples.

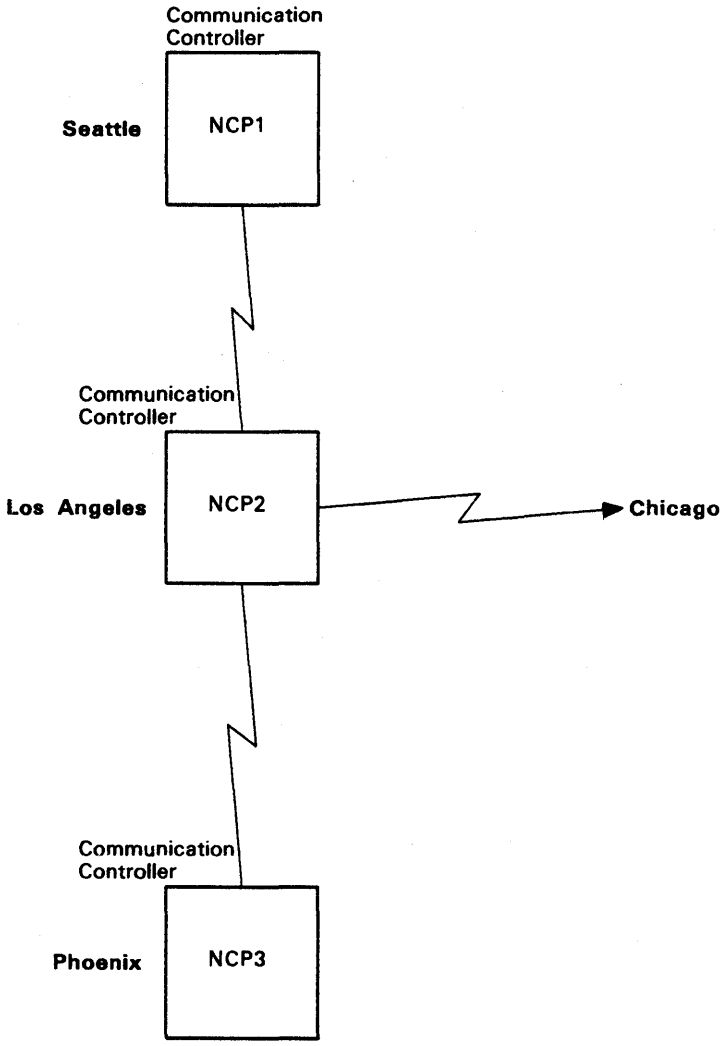


Figure 1-3. An Example of Configuring Lines for Less Expense

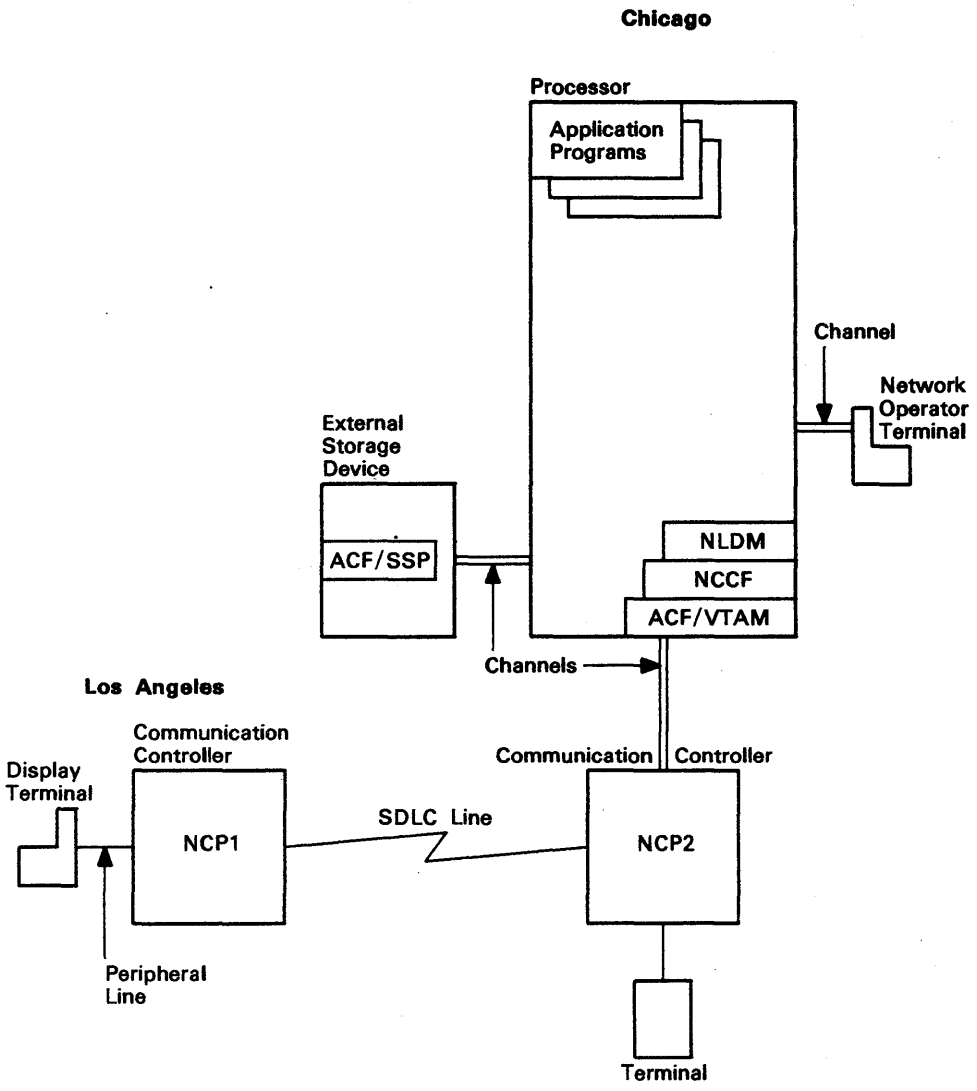


Figure 1-4. An Example of a Single-Domain Network

Multiple-Domain Networks

Figure 8 shows a network made up of four domains. In this figure, the domains are separated by dotted lines. Domain A is associated with the ACF/VTAM in New York City. Domains B and C are located in Chicago. Domain D is in San Francisco. The ACF/VTAM in New York owns the resources controlled by NCP1; the ACF/VTAM in the Chicago processor PROC2 owns the resources controlled by NCP2 and NCP21; and the ACF/VTAM in PROC3 owns the resources controlled by NCP3. The ACF/VTAM in the Chicago computer PROC2A does not own any ACF/NCP resources, and thus does not activate resources or provide session services for them. PROC2A performs work offloaded from PROC2.

All that has been said before under "Single-Domain Networks" applies to the individual domains shown in Figure 8. We will discuss here the added things you can do with multiple-domain networks, under the following categories:

- Network structure
- Session flow
- Network operation
- Network performance
- Network maintenance and problem determination
- Network recovery
- Configuration design

There are no functions in multiple-domain networks for the network security and application programming categories other than those described under "Single-Domain Networks."

Network Structure

In this section the following will be discussed:

- Sharing ACF/NCP resources
- Types of connections

Sharing ACF/NCP Resources

In a single-domain network, the single ACF/VTAM owns all the resources. It activates and deactivates them, receives error notifications about them, and initiates any recovery procedures.

In a multiple-domain network, there are multiple ACF/VTAMs. In an SNA multiple-domain network, ACF/VTAMs can share the ownership of an ACF/NCP and its resources. Up to eight ACF/VTAMs can share ownership of

an ACF/NCP and each line between ACF/NCPs. Ownership is established in the following ways:

- You define an ACF/VTAM as eligible to own the ACF/NCP. An ACF/VTAM that is not predefined to own the ACF/NCP cannot activate it.
- The first eight eligible ACF/VTAMs to activate the ACF/NCP own it.

Only one ACF/VTAM can own a device. Ownership is secured in the following ways:

- You can define an ACF/VTAM as the owner of the device, and when the ACF/VTAM activates it, ACF/VTAM becomes its owner. No other ACF/VTAM can activate it.
- If no ACF/VTAM is predefined as the owner, the first ACF/VTAM to activate the device owns it.

Figure 1-5 is an example of shared ownership. Both NCP2 and NCP21 are owned by domains D, C, and B. Device TERM1, controlled by NCP2, is owned by the ACF/VTAM in domain D. The ACF/VTAM in domain B owns TERM2, controlled by NCP2, and TERM4, controlled by NCP21. Domain C owns TERM3, controlled by NCP21.

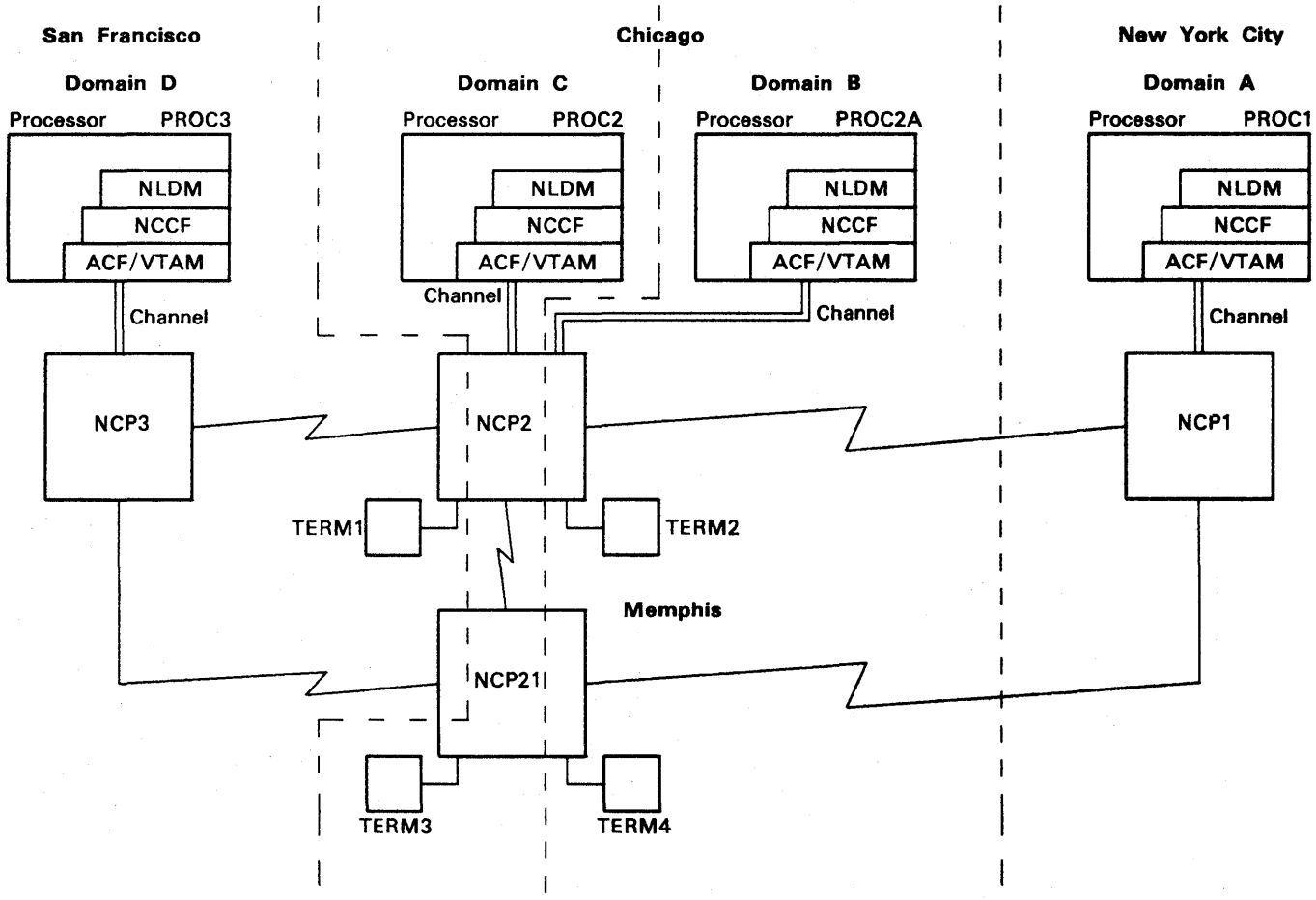


Figure 1-5. An Example of Shared Ownership

Note that although domain D is on the West Coast, it can include a resource thousands of miles away. Note also that ownership can extend through several levels of ACF/NCP attachments.

The pattern of ownership in your network can affect a number of things. For example:

- The device TERM1 in Chicago engages in cross-domain sessions (see "Session Flow" below) when it is in session with application programs in PROC2, also in Chicago. However, it engages in same-domain sessions with application programs in PROC3, which is in San Francisco.

  This might be because TERM1 is predominantly in session with application programs in domain D. In this way, error notifications and other messages concerning the device could go to domain D. If its predominant use is with application programs in domain C, it might be more efficient to have TERM1 owned by the ACF/VTAM in domain C.

- Multiple ownership of NCP2 and NCP21 means that the ACF/VTAMs in domains D, C, and B all receive error notifications from these ACF/NCPs. Thus, if the ACF/VTAM in PROC2 fails, the other ACF/VTAMs receive notice of the failure from NCP2 and can take the appropriate recovery actions (see "Network Recovery" later in this section).

  If there were heavy session traffic from domain D over the line between NCP2 and NCP1, you might want domain D to share ownership of the line, in order to receive notification of any failures.

Types of Connections

Traffic from one domain to another (cross-domain) can be over the following attachments:

- Between processors over channels
- Between communication controllers over SDLC lines
- Between processors and communication controllers over channels.

Channels can carry data faster. SDLC lines can carry it over longer distances.

Session Flow

The same session flow described under "Single-Domain Networks" occurs in cross-domain sessions, except that there are extra dimensions. In a single-domain network, the single ACF/VTAM initiates, controls, and terminates all sessions. In a multiple-domain network, ACF/VTAMs in several domains must work together to provide the same services on a cross-domain basis. Thus:

- A session between an application program in one domain and an application program or terminal in another requires that a session between the owning ACF/VTAMs be started first.

- When a session-initiation request is issued by an application program or from a terminal, the resource that it requests can be in any one of the network domains. The ACF/VTAMs in the various domains must therefore recognize each other and each other's resources.

  You define ACF/VTAMs to each other as cross-domain resource managers (CDRMs). You can also define application programs that can be in session with application programs and devices in other domains as cross-domain resources (CDRSCs). One of the things you can define about a CDRSC is the CDRM that owns it.

  In some cases, you can choose not to define all the CDRSCs in the network to each ACF/VTAM. *Dynamic CDRSC definition* can be used for both senders and receivers of session-initiation requests. You can define the CDRMs for the sending and receiving domains in such a manner that definitions of the resources owned by the CDRMs are not needed. The sending or receiving ACF/VTAMs create temporary definitions.

The following methods can be used with dynamic CDRSC definition for outbound session-initiation requests where the domain of the resource is not known:

- *The alias name translation capability in NCCF.* A Version 2 NCCF that has an alias translation table defined for all these CDRSCs provides the identity of the domain that owns the destination resource. The alias name translation facility acts as a directory.

- *Default ACF/VTAM selection.* You can provide the ACF/VTAM that is sending a session-initiation request a list of ACF/VTAMs in the network that might own the resource that is the object of the request. The sending ACF/VTAM sends the request to each domain listed until the appropriate one is found.

  This trial-and-error method could lengthen session setup time. However, the problem would be minimized in networks with a communication management configuration (CMC) host (see "Configuration Design" below) or configurations in which one or two hosts contain the application programs used by all the terminals in the network.

Network Operation

In a multiple-domain network, there can be multiple ACF/VTAM operators. These operators must coordinate their actions, such as when each domain will start up, or how to handle takeover and recovery situations.

NCCF network operation functions described under "Single-Domain Networks" operate the same in each domain of a multiple-domain network. However, NCCF provides additional functions for cross-domain operation:

- NCCF operators can start sessions with NCCFs in other domains and send messages to NCCF operators in other domains. (Note that NCCF operations between two domains require an NCCF in one domain to be in session with an NCCF in the other domain.)

- Terminal operators can issue commands to be executed in their own domains or in other domains. Command responses are returned to the issuing operator. Unsolicited messages generated by the access method are sent to a predefined NCCF network operator.

- Span of control can extend across domain boundaries, letting an authorized operator control resources that are in domains other than the one in which the issuing operator is located (or connected).

- Using span of control, system programmers can assign groups of network resources to specific operators when the network is being defined.

- Using NLDM with NCCF, operators can:

  - Collect session awareness data for session partners in different domains.

  - Determine cross-domain session history.

  - View problem determination information such as traces collected in another domain.

  - Display response time data interactively (optionally in color), graphically comparing it to a predetermined objective by terminal and by session.

Tailoring of network control makes your network easier to manage and frees the system console for other uses. One operator can control an entire domain if required, or a network operator can control each of the smaller elements of a divided network. If the operators have proper authority and are defined in each domain, they may control resources outside of the domain in which their terminal is physically located.

Network Performance

Performance considerations within domains in a multiple-domain network are the same as described under "Single-Domain Networks." However, there is an added performance consideration for cross-domain sessions. In sessions between adjacent hosts when using ACF/NCPs as intermediate routing nodes, the time a message takes to reach its destination is increased by the extra linkage. This time increases as the number of domains traversed increases.

The following tools can be used to measure performance across domains:

- Tuning statistics can be gathered for traffic between two ACF/VTAMs connected through a channel-to-channel adapter.

- The Network Performance Analyzer in ACF/NCP can be used to measure the efficiency of cross-domain SDLC lines between communication controllers.

Problem Determination and Network Maintenance

Problem determination and network maintenance functions described under "Single-Domain Networks" operate within each domain in the same manner. In a multiple-domain network, responsibilities and coordination among network operators are additional concerns. For example:

- Which ACF/VTAM operator is responsible for an SDLC line between two domains?
- When a route that crosses several domains has a performance problem, who is responsible for determining where the problem is?

When NCCF is active in each domain of a network, an NCCF in one domain can be in session with the NCCFs in the other domains. With NPDA and NLDM operating under NCCF in each domain, you can set up a central control point where information on maintenance and problem determination can be monitored and acted upon throughout the network. The NPDAs in the other domains can send in hardware information, and the NLDMs can provide session-level information.

NCCF network operators at the central site can display error counts collected in other domains, receive alerts of trouble spots, and coordinate actions among the other operators. You can also automate this process. For example, NCCF command lists (CLISTs), command processors, and exit routines at the central site can obtain information from the other domains. When remedial actions are needed, either the operator or an automated process can invoke the appropriate CLISTs, command processors, and exit routines in the other domains.

Network Recovery

Recovery for NCPs and lines is the same in multiple-domain networks as it is in single-domain networks. Replacement of a failing ACF/VTAM, however, need not involve an ACF/VTAM in another processor standing by as a backup. Takeover of an ACF/NCP and its resources by an ACF/VTAM in one domain for a failing ACF/VTAM in another is also possible. In addition, recovery in a multiple-domain network becomes a cooperative effort. Potentially, any ACF/VTAM in the network can perform a takeover. The recovery actions must be cooridated among the operators of the various domains. System programmers might have to make decisions like these:

- Should there be a takeover at all? In some cases, it might be simpler to restart the failing ACF/VTAM and start over.
- Which ACF/VTAM should take over the resources of each failing ACF/VTAM?
- Which tables and records concerning the prefailure configuration have to be changed for those ACF/VTAMs not involved in the takeover?
- If there has been an ACF/NCP takeover and the failing ACF/VTAM has come back up, should it take back its previous resources? All sessions with BSC 3270 display terminals in that configuration would then be terminated.

When an ACF/VTAM fails, cross-domain sessions involving terminals attached to an ACF/NCP owned by that ACF/VTAM are not disrupted. In a takeover, some sessions with devices controlled by the ACF/NCP continue without interruption. When the failing ACF/VTAM is restarted and takes its resources back, all sessions are disrupted. If an ACF/VTAM is restarted without a previous takeover, some sessions are disrupted. Sessions that continue during these stages of recovery do so without session services from any ACF/VTAM, because the records set up when the sessions were initiated have been lost.

Configuration Design

This section discusses the following subjects:

- General considerations for designing networks
- Special Configurations
  - Intermediate routing nodes (IRNs)
  - Communication management configuration (CMC) networks

General Considerations for Designing Networks

Three general factors can be considered in designing a network:

- Performance
- Availability
- Ease of operation

Figure 1-6 lists network elements you can change to alleviate various conditions. The table shows in general terms how the three factors are affected.

Looking at Figure 8, for instance, if you want faster and more reliable transmission between NCP3 and NCP2, you can add a line and designate the two lines as a transmission group. This will give you greater line capacity and will help ensure continued transmission, should one line fail. Note that if speed and availability are important between PROC3 and PROC1, you would have to do the same for the line between NCP2 and NCP1.

If a terminal attached to NCP3 is in session with an application program in PROC1 over the path using NCP2, a failure of NCP2 or either of the lines leading to it would interrupt the session. The application program can then reinitiate the session over the path using NCP21. If the new route is already heavily used, however, there might now be a degradation of performance over that route.

Configuration / Condition	Effect on Performance	Effect on Availability	Ease of Operation
Multiple-Line TG / Line Outage	Greater route capacity.	If a line fails, transmission is not interrupted, as long as one line in the TG is still active.	Reactivation of a line does not affect sessions.
Multiple Routes / ACF/NCP or Line Failure	No effect, but performance could be degraded on the new route.	If a line or ACF/NCP fails, recovery can be effected quickly by the application program or the operator.	No operator action is required.
Standby Replacement ACF/NCPs / ACF/NCP Failure	No effect.	If an ACF/NCP fails, recovery can be effected quickly. All sessions are interrupted.	Manual switching by the operator is required.
Shared ACF/NCP Ownership / ACF/VTAM Failure	No effect.	If an ACF/VTAM fails, recovery can be effected quickly. Some sessions could be interrupted.	With established recovery procedures, the operator action is simple to perform.
Increased Line Capacity / Slow Transmission	Faster transmission between NCPs.	No effect.	No effect.

Figure 1-6. Considerations for Using Various Configurations

Intermediate Routing Nodes (IRNs)

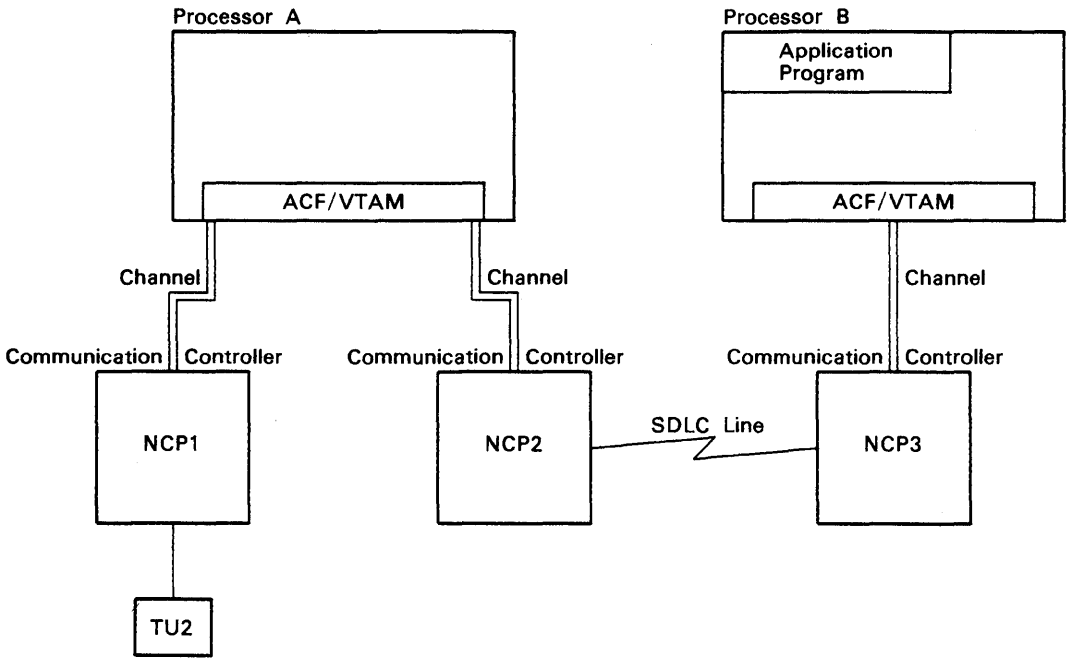
An ACF/VTAM can act as an intermediate routing node (IRN) on routes to other parts of the network. Figure 1-7 illustrates possible IRN configurations. In example 1, processor A is the IRN between communication controllers NCP1 and NCP2. This configuration would be useful when a line between NCP1 and NCP2 would be an unnecessary expense. In example 2, processor Y is the IRN between two processors, X and Z. This would be useful when there are only a few devices and the need for ACF/NCPs to control them is limited.

Communication Management Configuration Networks

You can arrange your network so that an ACF/VTAM in one processor owns and controls all ACF/NCPs, lines, and devices in the network, while the ACF/VTAMs in the other processors own all the application programs and perform data processing only. For example, in Figure 8 the ACF/VTAM in PROC2 in Chicago can own and control the devices in all four domains. This creates a central point of control for network resources and eliminates the need for other processors to activate and deactivate them. In the communication management configuration (CMC) all sessions between application programs and terminals are cross-domain.

If PROC2 fails, any of the other computers can take over as the CMC computer. However, no new sessions can be initiated until this happens. The ACF/VTAM that takes over would need configuration records that duplicated those of the original CMC ACF/VTAM. Sessions would be affected by the takeover in the same way as described above under "Network Recovery." A standby replacement host could be used, although the effect on sessions would be the same.

Example 1



Example 2

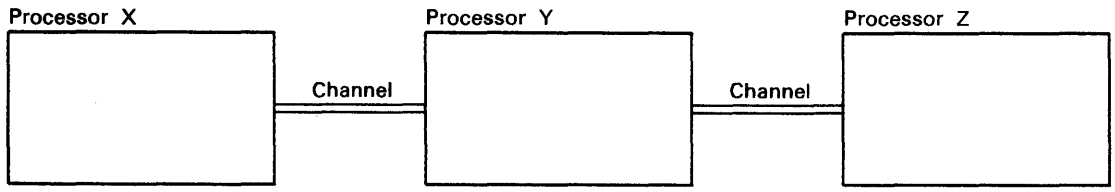


Figure 1-7. Examples of Intermediate Routing Node (IRN) Configurations

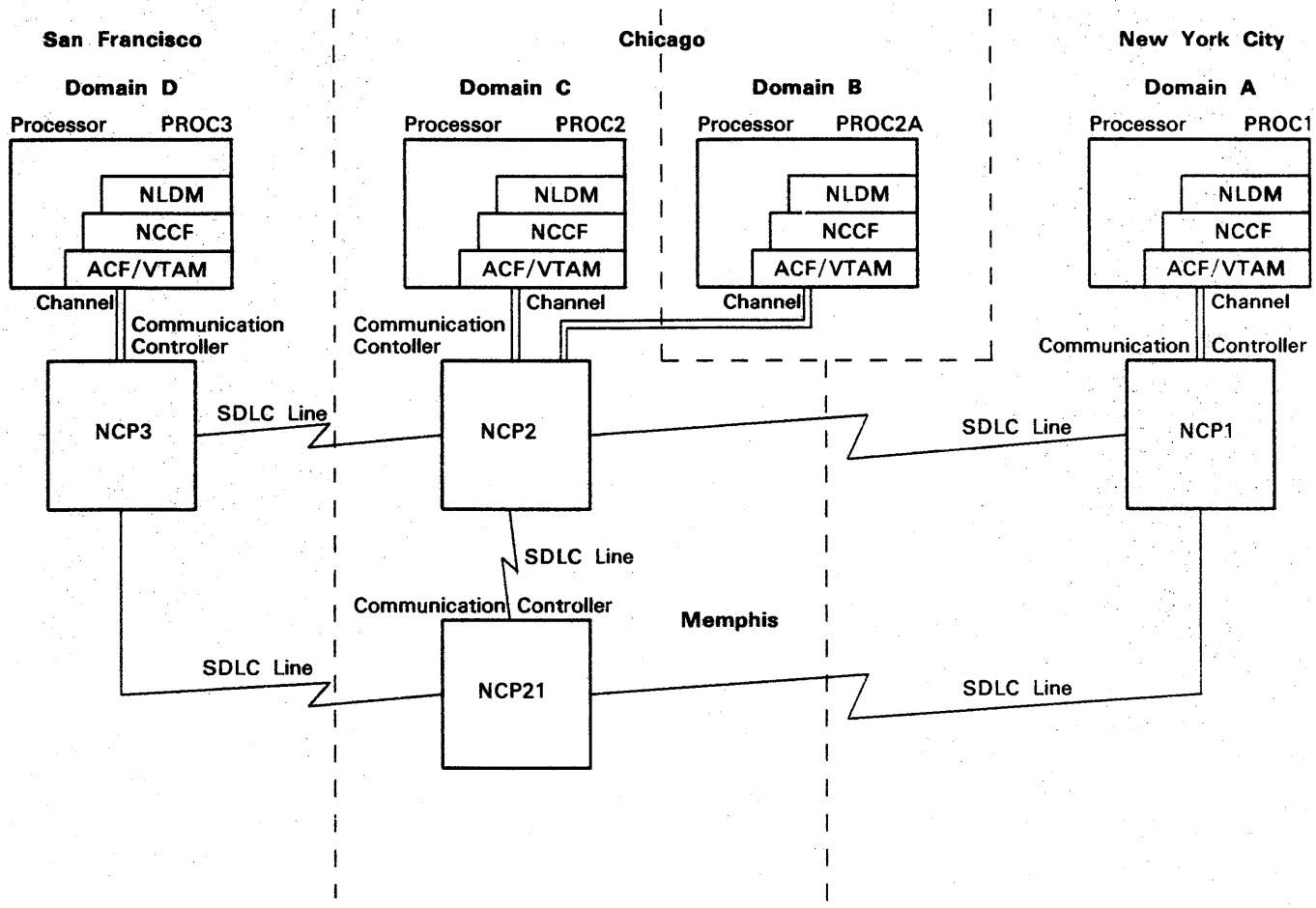


Figure 1-8. An Example of a Multiple-Domain Network

Interconnected Networks

SNA network interconnection permits two or more distinct SNA networks to be interconnected. In this way, resources in one network can communicate with resources in another. Some reasons you might want your network to be interconnected with other networks are:

- To use data and application programs from other networks. Typical environments might be:
  - Customers and suppliers
  - Service bureaus and clients
  - Retailers and credit bureaus
  - Banks in currency-exchange unions
- To avoid the complexity and coordination of merging networks when separate entities such as companies or governmental agencies merge.
- Generally, to exchange data among networks whenever the networks cannot be merged for reasons such as organizational structure, geography, geopolitics, local politics, or the need for security.
- For a network in which there are address constraints, more available addresses could be gained by dividing the network into multiple interconnected networks.

Each network is independent of the others. Sessions can take place between resources in any two interconnected networks through the same session setup procedures now used in those networks. No change need be made in the structure of any network, except where they interface. Depending on your requirements, even these changes can be minimal. The changes are discussed below in the context of the functions described.

In discussing interconnected networks, we will be less concerned with the functions in ACF/VTAM, ACF/NCP, NCCF, and NLDM that support the interconnection than with the networks themselves. The functions provided within any network have already been described under "Single-Domain Networks" and "Multiple-Domain Networks." We will discuss SNA network interconnection functions within the following categories:

- Network structure
- Session flow
- Network operation
- Network performance
- Problem determination and network maintenance
- Network recovery

- Network security
- Configuration design

There are no application programming functions for SNA network interconnection beyond what has been described under "Single-Domain Networks."

Network Structure

Figure 12 illustrates three interconnected networks. Network A could be a service network for the other two. For example, it might perform specialized scientific computations for networks owned by high-technology concerns, or central clearing house services for banking networks, or information services for various insurance companies. Alternatively, the networks might be separate parts of a network that had been divided earlier.

In the figure, NCP1 can be thought of as part of a gateway through which data crosses from one network to another. Physically, such a gateway consists of a communication controller run by a Version 3 ACF/NCP and attached to at least one processor with a Version 2 Release 2 ACF/VTAM. The remaining ACF/VTAMs and ACF/NCPs may be of any level supported by these program products (see the list in Chapter 3). Note that NCP1 does not have to be used solely as a gateway among the networks; it can perform any of the usual functions of an ACF/NCP.

Ownership of Gateway ACF/NCP Resources

A gateway ACF/NCP may be shared by ACF/VTAMs in one or more networks. However, resources connected to or within the gateway ACF/NCP may only be owned by ACF/VTAMs within a single network.

These principles allow multiple gateway ACF/VTAMs to share network boundary processing, while maintaining the integrity of the resources owned by the ACF/NCP.

Session Flow

The same session flow described previously for single-domain and multiple-domain networks takes place within each interconnected network. For cross-network sessions, however, there are extra dimensions:

- Each session between an application program and an application program or terminal in another network requires additional sessions between each adjacent pair of gateway ACF/VTAMs along the session path.

  If not all the necessary SSCP-SSCP sessions in the session setup path are active, ACF/VTAM will not establish the cross-network session with the application program. However, ACF/VTAM will notify the operator of the session setup failure. The operator can try to establish the cross-network session later when the required SSCP-SSCP sessions are active.

- At each network boundary, the gateway ACF/VTAM and ACF/NCP communicate to provide additional information:
  - The session route through the next network.
  - Transformation addresses for the originator of the request and the receiver that are appropriate to the next network.
  - Names (if required) that will be recognizable in each of the participating networks owning the receiver. These are: the name of each session partner and the identity of the network in which each resides, the logon mode table proposed for conducting the session, and the name of the class of routing service.

    Some terminals or application programs in one network may have the same names as resources in other interconnected networks. Also, the name of a set of session protocols or class of routing service in one network may mean something entirely different in other interconnected networks. Gateway ACF/VTAMs can use the NCCF alias name translation facility to resolve these name conflicts.
- When an application program or terminal issues a session-initiation request, the resource requested as a session partner can be located in any one of the interconnected networks. Two methods of assuring correct routing can be used:
  - Resources that engage in cross-network sessions can be defined as CDRSCs, just as they are defined for cross-domain sessions, except that they are also associated with the networks in which they reside.
  - ACF/VTAMs can define CDRSCs dynamically and use predefined lists of default ACF/VTAMs. Session requests can be routed to each listed ACF/VTAM, including gateway ACF/VTAMs, until one accepts the request as relating to its network.

In this way, each network retains its own set of names and its own route structure.

Network Operation

For each interconnected network, network operation takes place as described under "Single-Domain Networks" and "Multiple-Domain Networks." For SNA interconnected networks:

- Existing ACF/VTAM operator commands have been enhanced to perform cross-network functions.
- New ACF/VTAM command operands are provided for cross-network functions.
- NCCF operators can start NCCF sessions in other networks and route commands to them.

Network operators using NLDM can obtain session awareness and routing data for session partners in different networks. They can also obtain response time information for those session partners for which response time data has been collected.

Network Performance

For each interconnected network, performance considerations for individual single- and multiple-domain networks are the same. For the program products at network boundaries there are new considerations:

- Cross-network sessions use ACF/NCP resources. As discussed below under "Configuration Design," heavy cross-network traffic might require multiple gateway ACF/NCPs. You may also wish to define the ACF/NCP not to control any devices, so that it can be entirely devoted to cross-network traffic.

- An ACF/VTAM at a network boundary can have similar considerations. If cross-network traffic is heavy, the following might be done:

  - Avoid using the ACF/VTAM as an intermediate routing node in its own network.

  - Avoid having the ACF/VTAM be responsible for application programs as in a communication management configuration.

- The various methods described for routing across networks can affect performance:

  - Where all names are unique and the names of session protocols and classes of service mean the same throughout the interconnected networks, session setup time is faster. Considerable coding of definition statements is required. However, the use of dynamic CDRSC definition, while it could lengthen the time of session setup, could reduce the time spent recovering from errors.

  - Where CDRSCs are not predefined, defining a default SSCP list requires less work, but session setup time could be longer.

Problem Determination and Network Maintenance

For SNA interconnected networks, problem determination and network maintenance considerations within the individual single- and multiple-domain networks are the same.

In addition, NLDM can provide significant network problem determination data. An NLDM in one network in session with NLDMs in other networks can provide the following:

- The status of cross-network sessions

- The configuration of the routes the sessions traverse

- Cross-network route connectivity tests

- Control data contained in messages transmitted during the sessions.

Network Recovery

In interconnected networks, network recovery considerations within single- and multiple-domain networks are the same. For SNA network interconnection itself, recovery can be considered from two points of view: what happens at network boundaries and what happens within individual networks.

Recovery at Network Boundaries

At network boundaries, some of the recovery actions applicable to single-domain and multiple-domain networks can be used, for example:

- Replacement ACF/VTAMs or ACF/NCPs
- Multiple-line transmission groups
- Multiple routes through different gateway ACF/NCPs.

An ACF/VTAM cannot take over the resources of a gateway ACF/NCP in another network. Any other ACF/VTAM is the same network can take over these resources. A gateway ACF/VTAM in any other network could take over the cross-network sessions.

Recovery within Individual Networks

The failure of an ACF/VTAM, ACF/NCP, or line in one network could affect cross-network sessions. Recovery procedures in all such networks should therefore include cross-network considerations.

Network Security

Unauthorized access to data in your network can be prevented. The following safeguards are available for cross-network sessions:

- ACF/VTAM provides a session management exit for which you can write a routine for authorizing access to an application program. This exit can be used for cross-network session-initiation requests, as well as for single- and multiple-domain requests. While it may replace the authorization exit previously available for single-domain and multiple-domain sessions, the original exit can still be used.
- You may have data encrypted for cross-network sessions. In addition to the ACF/VTAMs controlling each end of the session, each gateway ACF/VTAM along the route requires IBM cryptographic program products.
- You can specify to the NLDMs in your network that they will not report session or route configuration data to NLDMs in other networks. A route test between networks that are not adjacent, for example, will return only the fact that connectivity does or does not exist.

Configuration Design

This section discusses the merits of three different SNA network interconnections: the single-gateway, multiple gateway, and tandem configurations.

Single-Gateway Configuration

Figure 12 shows one ACF/VTAM and one ACF/NCP serving as a gateway between other networks. The figure shows three networks, but there could be many more, limited only by requirements of the gateway ACF/NCP. Network A could be a service network set up solely to provide network boundaries for other networks, or it could be one of many interconnected networks in which an ACF/VTAM and an ACF/NCP have been upgraded to act as the gateway.

Some advantages of this configuration are:

- It requires that only one ACF/VTAM and one ACF/NCP be upgraded.
- Network maintenance and problem determination are carried out at one host.

The configuration can have these disadvantages:

- The transformation addresses and storage available to an ACF/NCP at a network boundary are limited.
- If the gateway ACF/NCP fails, all cross-network traffic is disrupted until recovery occurs. If the gateway ACF/VTAM fails but the ACF/NCP does not, cross-network sessions continue, although new sessions cannot be initiated.

Multiple-Gateway Configurations

Figure 1-9 presents a configuration with multiple gateway ACF/NCPs, that is, network boundaries are situated so there is more than one route between each pair of networks. In this figure, a session between APPL1 in PROC1 and APPL2 in PROC2 could pass through gateway NCP1 or gateway NCP2.

The figure shows one ACF/VTAM (in PROC3) controlling multiple ACF/NCPs. However, there could be one gateway ACF/VTAM for each ACF/NCP. This configuration requires more upgraded ACF/NCPs, and possibly ACF/VTAMs. However, it has advantages over a single network boundary:

- Session traffic can be distributed among the gateway ACF/NCPs by writing a session management exit routine.
- More addresses are available.
- If there is a failure at one gateway ACF/NCP, sessions passing through it will fail. However, they can be reestablished and rerouted through the other gateway ACF/NCP.

Note: With a gateway ACF/VTAM in all interconnected networks, each cross-network resource is defined as owned by the gateway ACF/VTAM in its network. This permits each network to change its configuration as needed and only relect these changes in its gateway ACF/VTAM. The other networks are not required to know about the changes.

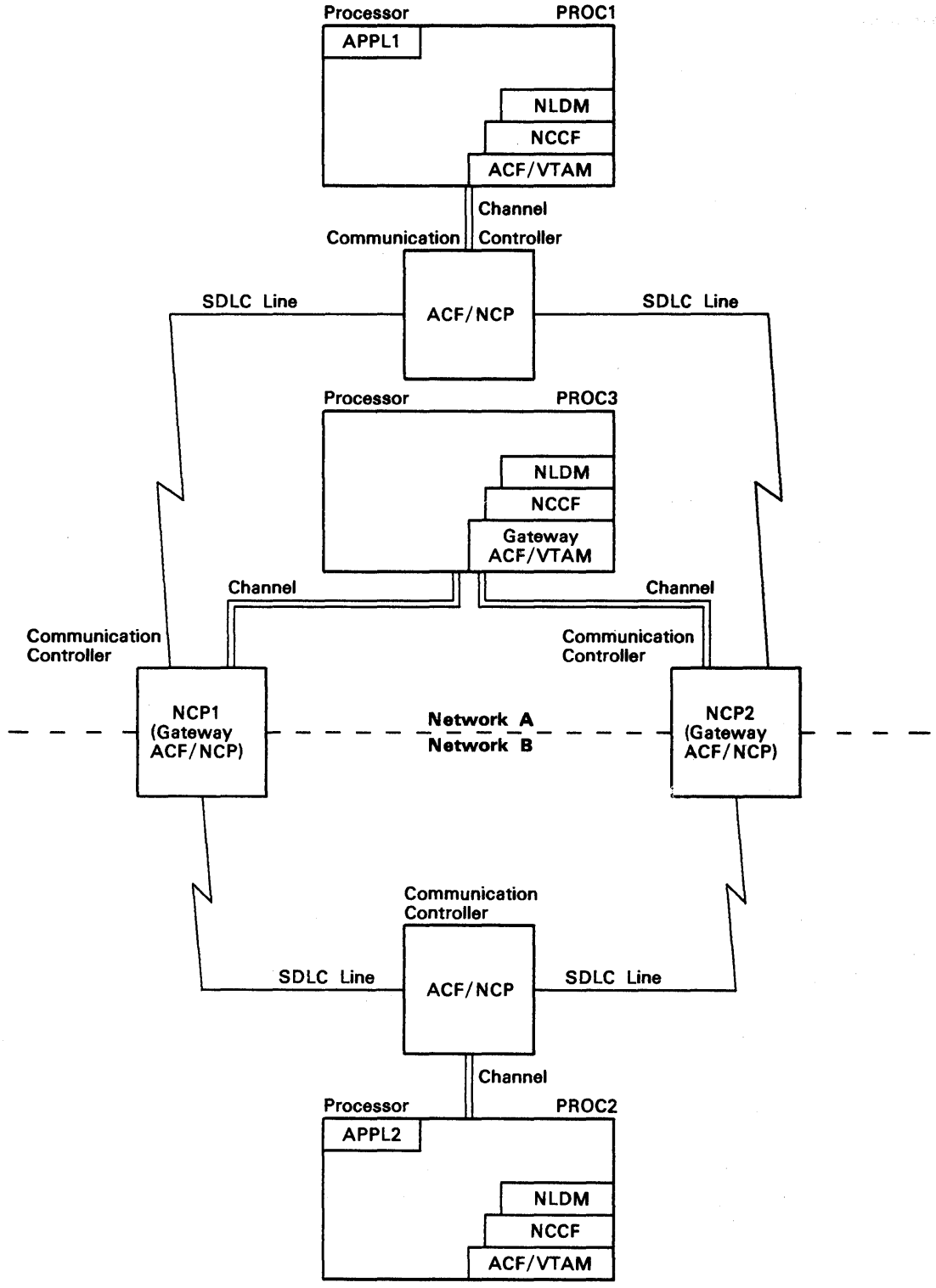


Figure 1-9. Example of Multiple ACF/NCPs Acting as Gateways

Figure 1-10 presents a configuration of networks in tandem. The ACF/VTAM in PROC2 serves with NCP1 as the gateway between networks A and B, and with NCP2 as the gateway between networks B and C. Note that the ACF/VTAMs in PROC1 and PROC3 do not have to be upgraded.

Figure 1-11 presents a configuration in which two networks are separated by a network without a gateway ACF/VTAM, that is, they are nonadjacent. In this illustration, networks A and C have more configuration isolation than if they were adjacent, since most of the information that must be exchanged when connecting networks only pertains to adjacent networks.

Tandem configurations can be used with networks that are geographical neighbors. For example, a series of networks for hospital associations in the northeastern, mid-Atlantic, and southeastern regions might use tandem interconnection. On the other hand, a nationwide network with the address constraints described earlier might be sectioned into a tandem configuration of eastern, midwestern, and western networks.

A tandem configuration requires more gateways than the configuration shown in Figure 12. Network maintenance and problem determination is less centralized and requires more coordination. Performance is not as good and tends to degrade further as the number of networks increases.

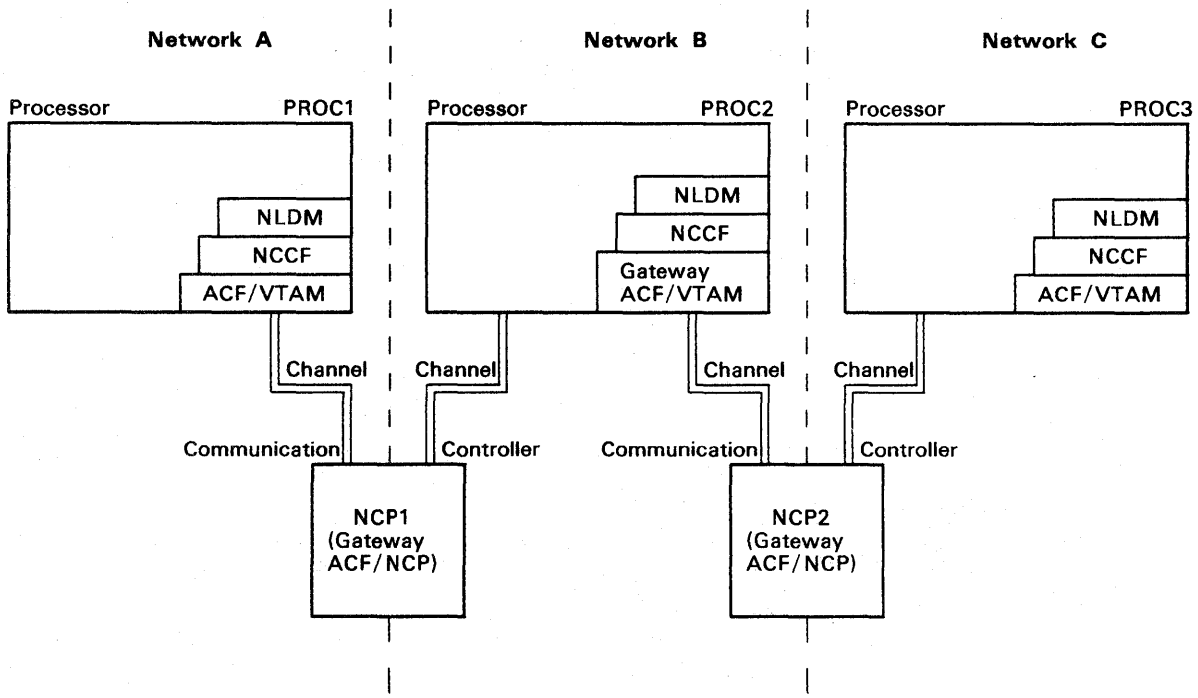


Figure 1-10. An Example of Tandem Interconnected Networks (Adjacent)

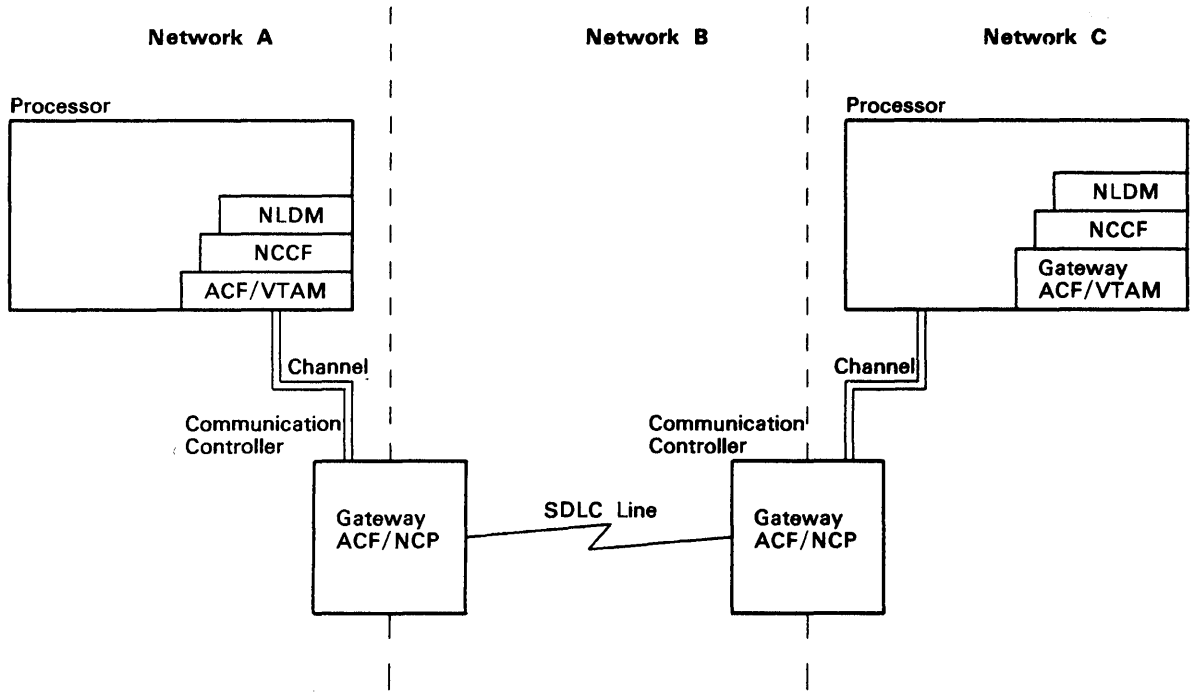


Figure 1-11. An Example of Tandem Interconnected Networks (Nonadjacent)

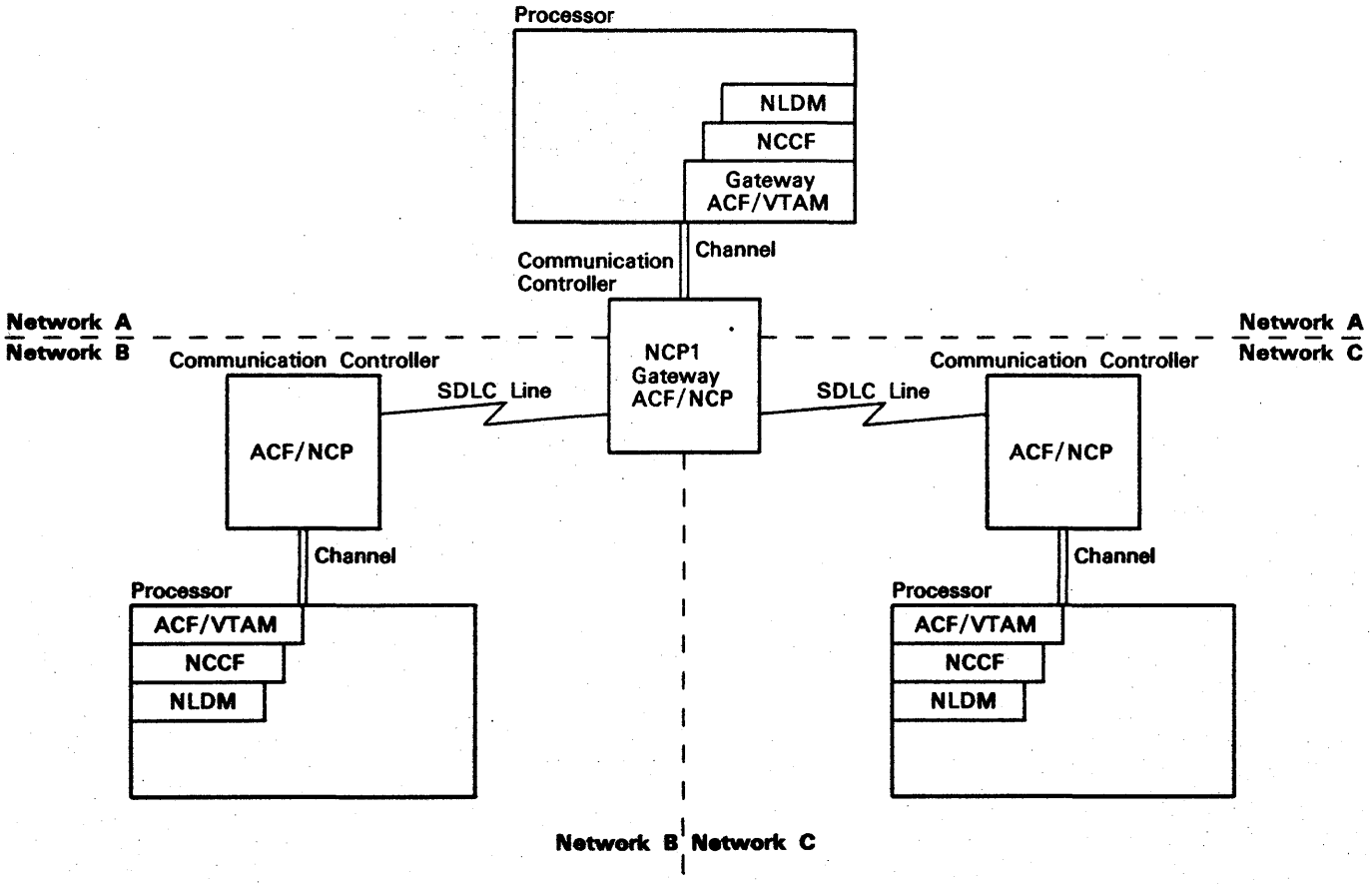


Figure 1-12. An Example of Interconnected Networks

Chapter 2. Network Program Product Functions

This chapter is primarily for users migrating to ACF/VTAM Version 2 Release 2 and the equivalent releases of ACF/NCP, ACF/SSP, NCCF, and NLDM. New customers can also use it for more details on functions mentioned in Chapter 1.

The program products are described in the following order;

- ACF/VTAM and ACF/NCP together
- ACF/SSP
- NCCF
- NLDM

ACF/VTAM and ACF/NCP Functions

This section contains general descriptions of ACF/VTAM and then ACF/NCP, followed by a description of the enhancements made to these program products since VTAM Level 2 and NCP Level 5.

Introduction to ACF/VTAM Functions

ACF/VTAM provides the interface between application programs in the host processor and other resources in the network. In order to do this, ACF/VTAM:

- Activates and deactivates resources in its domain, including application programs, ACF/NCPs and the devices they control, and devices to which ACF/VTAM is attached directly
- Establishes, monitors, and terminates sessions between application programs and devices or other application programs, forwarding the session data to and from each session partner
- Keeps records on the configuration in its domain, sessions under its control, and network conditions
- Receives commands from the ACF/VTAM operator to perform network services and keeps the operator informed about these services, as well as network conditions, with operator messages.

Basic functions relating to ACF/VTAM are described below under the categories:

- Network structure
- Network flow control
- Network operation
- Network performance
- Problem determination and network maintenance

- Network recovery
- Network security
- Application programs.

Network Structure

ACF/VTAM controls resources directly (through direct attachment) or indirectly (through an ACF/NCP). It owns resources that it has activated and you have defined it to own. It sends and receives session data over defined paths related to the lines and ACF/NCPs of the network configuration.

Session Flow

ACF/VTAM uses pacing to control the flow of data. It specifies the number of path information units (PIUs) that can be sent before a response from the receiver must be returned. ACF/VTAM also uses virtual route pacing, which limits the amount of data that can be sent over a route at any one time.

Network Operation

The ACF/VTAM operator controls ACF/VTAM through specific commands:

- Start and halt commands for starting and stopping ACF/VTAM
- DISPLAY commands for obtaining the status of network resources
- VARY commands for activating and deactivating resources
- MODIFY commands for changing the status of operations such as traces and the performance of utility functions.

The programmed operator interface (POI) enables application programs to perform ACF/VTAM operator functions. NCCF is an IBM program product that uses this interface.

Network Performance

ACF/VTAM buffers can be specified according to the needs of your installation. You can also specify the maximum size of path information units (PIUs) that are sent and received. You can specify ways for ACF/VTAM to save processor cycles.

Problem Determination and Network Maintenance

ACF/VTAM provides the following functions:

- A dump of ACF/NCP contents
- Traces of ACF/VTAM buffer use, line use, and I/O events
- Error recordings provided by the system.

Network Recovery

ACF/VTAM can notify its operator of failing resources and sessions and can reactivate them. In response to operator commands it can take over an ACF/NCP and its resources from a failing host. It can also reload and reactivate

an ACF/NCP and reactivate its resources. The ACF/NCP's configuration can be reactivated to its status just before the failure or to its status when the ACF/NCP was originally activated.

Network Security

The way you define an application program to ACF/VTAM can limit access to other application programs. Access can also be controlled through the ACF/VTAM authorization exit routine or session management exit routine.

You can also use the Encrypt/Decrypt Feature of ACF/VTAM with either the Programmed Cryptographic Facility program product or the Cryptographic Unit Support program product to encipher and decipher data sent between application programs and devices and to prevent data from appearing in traces or dumps.

Application Programs

An application program obtains telecommunication services from ACF/VTAM by using ACF/VTAM macro instructions. It receives notification from ACF/VTAM of events such as logon requests, completion of I/O requests, etc., either directly or through exits for which routines can be written.

Application programs can be coded to acquire logical units (LUs) as session partners and to pass them on to other application programs. You can also define LUs to be logged on by ACF/VTAM to an application program automatically when both have been activated.

Introduction to ACF/NCP Functions

The ACF/NCP controls a network of data links and devices, and routes data between access methods in host processors and the devices in the network. ACF/NCP controls the network by controlling the data links themselves and by selecting the routes over which data flows. To perform control and routing functions, ACF/NCP does the following:

- Accepts control requests from the access method and returns responses
- Receives data from the access method and routes it to designated devices in the network, often through other ACF/NCPs in the network
- Accepts requests from network devices and returns responses
- Receives data from network devices and routes it to the access method or to other network devices, often through other ACF/NCPs in the network
- Keeps records of network conditions and forwards the information to the access method upon request.

Basic functions relating to ACF/NCP are described under the following categories:

- Network structure
- Session flow
- Network operation

- Network performance
- Problem determination and network maintenance
- Network recovery
- Network security.

Network Structure

ACF/NCP enables networks of various configurations to operate effectively. It controls different types of data links in various arrangements, and routes data over these data links to many different types of network devices. From the communication controller where it resides, the ACF/NCP polls and addresses stations on nonswitched data links, and dials and answers stations on switched data links. It selects a route for data according to the network configuration design and the current conditions of the network.

The data links controlled by the ACF/NCP have many possible characteristics. A data link can use the synchronous data link control (SDLC), binary synchronous communication (BSC), or start-stop communication discipline. The link can be duplex or half-duplex, point-to-point or multipoint, or switched or nonswitched.

The configuration of a network is defined with ACF/NCP generation macros. With these macros, you can define such things as line addresses and speeds, data links and routing, and device types and names.

Session Flow

ACF/NCP uses pacing to control the flow of data in the network. Pacing determines the amount of data that can be sent before a response must be returned.

ACF/NCP controls data traffic between communication controllers in the network as well as between communication controllers and the network devices.

Network Operation

Network operations for the ACF/NCP are initiated through access method commands. The operator has no direct connection with ACF/NCP, except for functions that can be performed at the control panel of the 3705 and the console of the 3725.

Network Performance

Network performance is affected by several functions under control of the ACF/NCP. Some of these functions can be specified during ACF/NCP generation, and some can also be modified later during network operation.

ACF/NCP controls the number of times that devices on a multipoint BSC or start-stop data link can respond negatively before the link is rescheduled for other operations. You can specify the maximum number of times that these devices can respond negatively.

A channel attention delay option controls the interval that the ACF/NCP waits before presenting an attention interruption to the host processor channel to transfer a block of data.

Problem Determination and Network Maintenance

ACF/NCP provides the following functions related to problem determination and network maintenance:

- Tests of data links, modems, and network devices
- Traces of data links and channel adapter activity
- Recordings of errors and statistics for data links and devices
- A dump of communication controller storage.

Network Recovery

The ACF/NCP can recover from some types of transmission errors in the network by retransmitting data that has been sent incorrectly.

Network Security

The ACF/NCP verifies the identification of certain BSC devices before they can communicate with ACF/NCP over switched data links.

Functional Enhancements to ACF/VTAM and ACF/NCP

The functional enhancements to ACF/VTAM and ACF/NCP are described below in the categories listed earlier in this section.

For each group of functions, there is a table from which you can determine if each function is an addition to those in your current release of ACF/VTAM or ACF/NCP. Following the tables are brief descriptions of the functions.

Note: This chapter only tells you what the functions can do for you. Requirements for using the functions or the actions you must take to implement them are described in more detailed books. These books are described in Appendix B, "Library Summaries."

How to Use the Tables

Using Figure 2-1 as an example:

- Under "Type of Network" on the left, an "X" under the "S" column tells you that the function can be used in a single-domain network; under "M" it can be used across domains in a multiple-domain network; and under "I" that the function can be performed across interconnected networks.
- The functions are listed alphabetically in the center of the table; descriptions of the functions appear after the table in the same order.
- Under "Release Effected In" on the right, an "X" appears under each release of ACF/VTAM and ACF/NCP that has the function. "V1R1" means "Version 1 Release 1," "V1R2" means "Version 1 Release 2," etc.

Note: In the case of ACF/NCP, "V1R2" means "Version 1 Release 2.1," as well as "Version 1 Release 2."

If you are migrating from VTAM Level 2 and NCP Level 5, all the functions listed in the table are new to your installation. But if you are migrating to the current releases of ACF/VTAM and ACF/NCP from Version 1 Release 1, for example, and you have a single-domain network, the first new function that can be used in a single-domain network is "ACF/NCP ACB address extension." Under "Release Effected In" there is no "X" under "V1R1;" thus, the function is new for your installation and you may want to read the description of it below.

Network Structure

Figure 2-1 lists functions that affect network structure.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X	X	ACF/NCP ACB address extension		ACF/VTAM / ACF/NCP					X
	X		Channel-attachment ACF/NCPs		ACF/VTAM / ACF/NCP					X
	X		Channel-to-channel-attached hosts		ACF/VTAM / ACF/NCP				X	X
X	X	X	Data links operating at up to 230.4 kbps		ACF/VTAM / ACF/NCP		X	X	X	X
X	X	X	Downstream load		ACF/VTAM / ACF/NCP			X	X	X
	X	X	Dynamic cross-domain resource definition	Inbound logon to LU	ACF/VTAM / ACF/NCP			X	X	X
	X	X		Outbound logon to LU	ACF/VTAM / ACF/NCP					X
X	X		Extended ACF/NCP connection		ACF/VTAM / ACF/NCP			X / X	X / X	X / X
	X		Extended data link ownership		ACF/VTAM / ACF/NCP			X / X	X / X	X / X
X	X	X	High-speed link transmission enhancement (Modulo 128) for the 3725		ACF/VTAM / ACF/NCP					X
	X	X	Host intermediate routing node (IRN)		ACF/VTAM / ACF/NCP				X	X
X	X	X	Monitor mode	Channel	ACF/VTAM / ACF/NCP			X	X	X
X	X	X		SDLC link	ACF/VTAM / ACF/NCP			X	X	X
	X	X	Multisystem Networking Facility (MSNF) repackaging		ACF/VTAM / ACF/NCP				X	X
X	X	X	Non-SNA devices attached to ACF/NCP		ACF/VTAM / ACF/NCP		X / X	X / X	X / X	X / X
X	X	X	Parallel SDLC links		ACF/VTAM / AFC/NCP			X / X	X / X	X / X
X	X	X	Port swapping enhancement for the 3725		ACF/VTAM / ACF/NCP					X
X	X		Primary logical units attached to an ACF/NCP		ACF/VTAM / ACF/NCP				X / X	X / X
		X	SNA network interconnection		ACF/VTAM / ACF/NCP					X / X
X	X	X	Start-stop link transmission enhancement for the 3725		ACF/VTAM / ACF/NCP					X
X	X	X	Transmission groups		ACF/VTAM / ACF/NCP			X / X	X / X	X / X

Note: These functions are described below.

Figure 2-1. ACF/VTAM and ACF/NCP Functions Used in Network Structure

ACF/NCP Address Control Block Address Extension: The address of an Address Control Block (ACB) can be up to 17 bits long, which allows the maximum address of an ACB to be 128K. This higher address allows the ACB to reside in storage above 64K.

Channel-Attachment ACF/NCPs: Hosts no longer need to activate or have a Stage 1 definition deck of channel-attached NCPs in order to send messages through them. The host can still take over the ACF/NCP from an owner host that has failed.

Channel-to-Channel-Attached Hosts: Two host processors equipped with Version 2 ACF/VTAMs and channel-to-channel adapters can be connected by a channel, permitting direct transfer of data without an intervening NCP.

Data Links Operating at up to 230.4 kbps: The ACF/NCP allows data links attached to a communication controller to operate at data rates up to 230.4 kbps.

Downstream Load: The CNM interface (see "Problem Determination and Network Maintenance" in this chapter) has been expanded to allow loading programs into physical unit Type 2 devices where required.

Dynamic Cross-Domain Resource (CDRSC) Definition: ACF/VTAM can process session-initiation requests for terminals and application programs received from and directed to logical units in other domains or networks, without their being defined to it as cross-domain resources.

Extended ACF/NCP Connection: An ACF/NCP can perform the same network control functions, regardless of whether it was loaded into the communication controller over a channel attachment from a host processor or over an SDLC link from another communication controller.

For single-domain networks, extended ACF/NCP connection allows more than two communication controllers to be connected in tandem.

For multiple-domain networks, extended connection allows cross-domain SDLC links between ACF/NCPs in link-attached controllers. See Figure 2-2. Extended interconnection in multiple-domain networks also allows communication over cross-domain links between a single ACF/NCP and ACF/NCPs in multiple communication controllers. Thus, two or more access methods can share ownership of an ACF/NCP in a link-attached controller. See Figure 2-3.

Extended connection has two major benefits. First, the functions of an ACF/NCP are always the same, regardless of how the ACF/NCP is loaded. This allows controllers to be dispersed geographically without concern for whether the controllers are channel-attached or link-attached. Second, multiple access methods can share ownership of network devices. Thus, if failure occurs, more ACF/VTAMs are available to take over ownership of the devices.

Extended Data Link Ownership: Any SSCP in a network may activate, and thus own, any data link between ACF/NCPs, regardless of how distant the SSCP is from the link. The ACF/NCPs keep information about the number of SSCPs that can currently own the link, to a maximum of eight. Each SSCP can deactivate the link when it has no further use for the link, but the ACF/NCP does not deactivate the link until the last remaining owner deactivates the link.

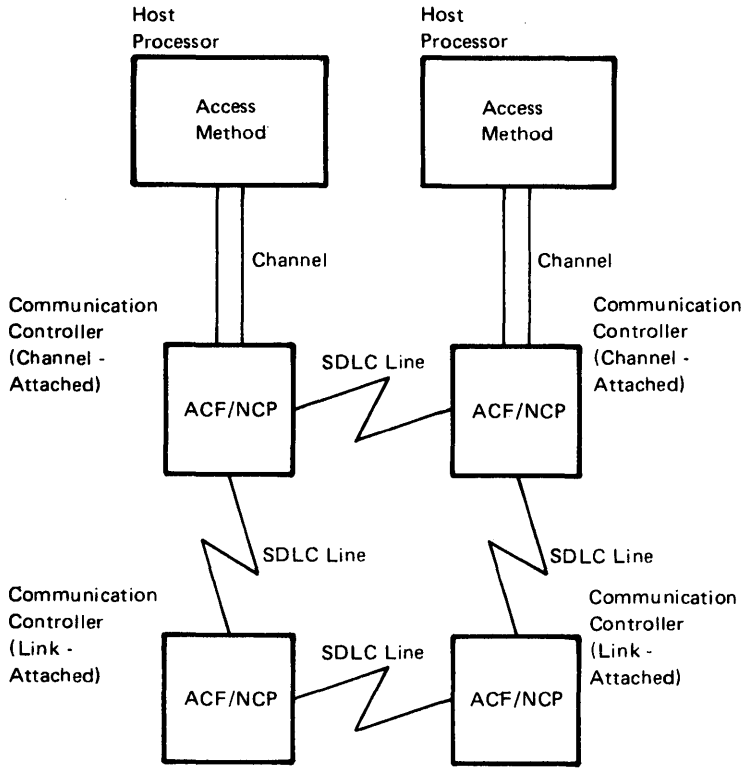


Figure 2-2. Cross-Domain Links between ACF/NCPs in Link-Attached Communication Controllers

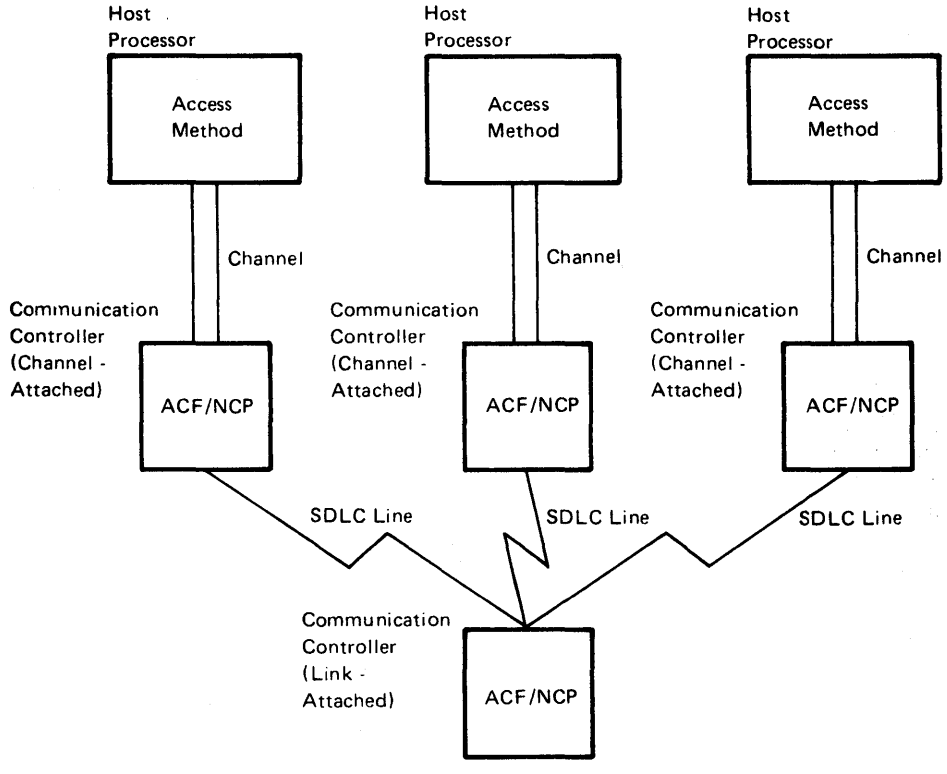


Figure 2-3. Shared Ownership of an ACF/NCP

High-Speed Link Transmission Enhancement (Modulo 128) for the 3725: The maximum amount of data the NCP can send over high-speed duplex links before it requires a transmission response is extended from 7 information frames (I-frames) to 127 I-frames. This option helps to minimize signal delay and is available on links between communication controllers and between communication controllers and cluster controllers.

Host Intermediate Routing Node (IRN): A host can transmit messages between two other hosts or between a host and an ACF/NCP.

Monitor Mode: ACF/NCP provides two types of monitor mode functions:

Channel Monitor Mode: An ACF/NCP attached to the host processor through certain types of adapters can accept a channel contact with an SSCP at any time. If such a channel adapter fails to become active when the ACF/NCP is initialized, the channel monitor function tries to activate it after a certain time interval.

SDLC Monitor Mode: An ACF/NCP can activate specified SDLC links when the ACF/NCP is initialized if no external SSCP is yet active. Under these conditions, the ACF/NCP can contact an adjacent ACF/NCP without SSCP or operator assistance.

Multisystem Networking Facility (MSNF) Repackaging: Modules of the Multisystem Networking Feature are now part of the ACF/VTAM program product.

Non-SNA Devices Attached to ACF/NCP: The Network Terminal Option (NTO) allows an ACF/NCP to provide SNA support for a select group of non-SNA devices. The IBM publication *Network Terminal Option General Information Introduction* tells what non-SNA devices are supported and provides more information about NTO.

Parallel SDLC Links: Parallel SDLC links can connect two ACF/NCPs. Data can flow over these links simultaneously. The number of parallel links that can be used depends on the link attachment capabilities of the communication controllers in which the ACF/NCPs reside. Parallel links can reduce session disruption caused by a failing link or the deactivation of a link.

Port Swapping Enhancement for the 3725: This enhancement allows you to transfer a data link from a failing port to a spare port without having to code a duplicate definition of the link during resource definition.

Primary Logical Units Attached to an ACF/NCP: Devices attached to an ACF/NCP can communicate with each other when the ACF/NCP is supplemented by the IBM program product Network Routing Facility (NRF) or a similar user-written program.

SNA Network Interconnection: Independent SNA networks can be interconnected so that sessions can be conducted between logical units (LUs) in one network and LUs in another without having to change network specifications, such as subarea addressing capability (MAXSUBA) or resource names.

Networks are connected through gateways, each consisting of one or more gateway ACF/VTAMs in session with a gateway ACF/NCP for message traffic.

Each such ACF/NCP must be at least Version 3 and it must be owned by at least one Version 2 Release 2 ACF/VTAM. Other nongateway ACF/VTAMs and ACF/NCPs in the connected networks need only be of a release level supported by Version 2 Release 2 (see Appendix A for the supported levels).

Start-Stop Link Transmission Enhancements for the 3725: Data sent over start-stop lines to the communication controller is now temporarily stored in a four-character burst prior to being processed. The start-stop enhancement shortens the path length in the scanner. This increases the number of lines that can be attached to one scanner and decreases the number of scanner interruptions.

Transmission Groups: Sets of one or more links between two NCPs can be defined logically as a transmission group over which messages can be sent. In TGs of more than one link, this allows larger band width and continued transmission without loss of data when one or more links in the transmission group fail.

Session Flow

Figure 2-4 lists functions that affect session flow.

Bidirectional Session Pacing: ACF/VTAM Version 2 Release 2 provides control over the rate at which the secondary end of a session can send data to the primary end. (Pacing from the primary end to the secondary end existed in VTAM Level 2.)

Cross-Domain Resource Managers (CDRMs): CDRMs establish, control, and terminate access to application programs and SNA terminals in other domains in a network.

Cross-Domain Sessions: Application programs in one domain can communicate with application programs and terminals controlled by other access methods in other domains.

Cross-Network Sessions: Application programs in one SNA network can communicate with application programs and terminals in other SNA networks that are interconnected.

Default and Adjacent SSCP Selection: Defining an adjacent SSCP table allows you to specify one or more ACF/VTAMs to which session-initiation requests can be sent successively until the proper ACF/VTAM is found. This table is used to find resources owned by other ACF/VTAMs, in either the same or another network.

Local Terminals in Cross-Domain and Cross-Network Sessions: Channel-attached devices can be in session with terminals and application programs in other domains or networks.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X	X	Bidirectional session pacing		ACF/VTAM ACF/NCP	X X	X X	X X	X X	X X
	X	X	Cross-domain resource managers		ACF/VTAM ACF/NCP	X	X	X	X	X
	X	X	Cross-domain sessions		ACF/VTAM ACF/NCP	X	X	X	X	X
		X	Cross-network sessions		ACF/VTAM ACF/NCP					X X
	X	X	Default and adjacent SSCP selection		ACF/VTAM ACF/NCP					X
	X		Local terminals in session	Cross-domain	ACF/VTAM ACF/NCP		X	X	X	X
		X		Cross-network	ACF/VTAM ACF/NCP					X
X	X	X	Multiple routes		ACF/VTAM ACF/NCP			X X	X X	X X
		X	Path selection exits	Gateways	ACF/VTAM ACF/NCP					X
X	X	X		Virtual routes	ACF/VTAM ACF/NCP			X	X	X
X	X	X	Transmission priorities		ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X	Virtual route pacing	Basic pacing algorithm	ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X		Window size calculation exit routine	ACF/VTAM ACF/NCP			X	X	X
X	X	X		Window size specified on PATH statement	ACF/VTAM ACF/NCP					X X
Note: These functions are described below.										

Figure 2-4. ACF/VTAM and ACF/NCP Functions Used in Session Flow

Multiple Routes: Messages can be sent over a selection of routes within a network, allowing traffic load-balancing and reducing the effect of failure by one of the nodes along a route. An *explicit route* defines the physical path connecting two subarea nodes. A *virtual route* defines a logical connection between two subareas that is realized over an explicit route.

For each virtual route, you can assign transmission priorities to different types of session traffic (see "Transmission Priorities" below).

Path Selection Exits: There are two exit routines with which you can alter the process of selecting a path at session activation. One is an exit routine for selecting virtual routes within single networks. The other is the session management exit routine, which allows you to alter selection of gateway ACF/NCPs for cross-network sessions.

Transmission Priorities: You can assign three levels of priority to each virtual route, allowing you to differentiate among types of message traffic, such as interactive or batch. All traffic over the route is handled according to these priorities, within limits set to assure that no message is queued indefinitely.

Virtual Route Pacing: The following functions apply to controlling the flow of data over a virtual route.

Basic Algorithm: Virtual route pacing is based on controlling the amount of data (called a "window") that is sent at one time from the virtual route endpoint.

Window Size Calculation Exit Routine: Pacing is maintained by the nodes along the route, but you can write an ACF/VTAM exit routine to modify the window size.

Window Size on PATH Statement: You have an added option in specifying the minimum and maximum window sizes for each virtual route in the appropriate PATH statements. If you have also coded the exit routine, it will override the PATH statement specifications.

Network Operation

Figure 2-5 lists functions that affect network operation.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
	X	X	Added DISPLAY capabilities	Adjacent SSCP tables	ACF/VTAM ACF/NCP					X
X	X	X		Buffer use for ACF/VTAM	ACF/VTAM ACF/NCP	X	X	X	X	X
X	X			Dynamic ACF/NCP storage display	ACF/VTAM ACF/NCP	X X	X X	X X	X X	X X
		X		Interconnected network information	ACF/VTAM ACF/NCP					X X
X	X	X		Pending activations	ACF/VTAM ACF/NCP	X X	X X	X X	X X	X X
X	X	X		Routes	ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X		Sets of resources	ACF/VTAM ACF/NCP	X X	X X	X X	X X	X X
X	X	X		Stations	ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X		TSO user ID status	ACF/VTAM ACF/NCP			X	X	X
X	X	X	Dynamic reconfiguration		ACF/VTAM ACF/NCP		X X	X X	X X	X X
X	X	X	Forced deactivation of a link		ACF/VTAM ACF/NCP					X X
X	X	X	Forced session termination		ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X	NLDM session awareness function support		ACF/VTAM ACF/NCP			X	X	X X
X	X	X	Operator command modification		ACF/VTAM ACF/NCP				X	X
X	X	X	Operator message modification		ACF/VTAM ACF/NCP				X	X
X	X		PEP load modules: loading over a link		ACF/VTAM ACF/NCP				X X	X X
X	X	X	Route verification and error notification		ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X	3036 console allocation as a terminal		ACF/VTAM ACF/NCP				X	X
Note: These functions are described below.										

Figure 2-5. ACF/VTAM and ACF/NCP Functions Used in Network Operation

Added DISPLAY Capabilities: New display capabilities are as follows:

Adjacent SSCP Tables: The adjacent SSCP tables for the domain, which are used for routing session-initiation requests through multiple-domain and interconnected networks, can be displayed.

Buffer Use for ACF/VTAM: The ACF/VTAM operator can display such same-domain information as the buffer size for each pool, number of buffers in the pool, and how many are available.

Dynamic ACF/NCP Storage Display: The ACF/VTAM operator can display up to 256 bytes of ACF/NCP storage for an ACF/NCP in session with ACF/VTAM while the ACF/NCP is running.

Interconnected Network Information: Information relating to interconnected networks will be included when cross-network resources currently defined in the operator's domain are displayed. For example, a display of application programs indicates the ID of the network containing them.

Pending Activations: The ACF/VTAM operator can display the name and status of each node in the domain for which session activation or termination is being processed but not completed.

Routes: The ACF/VTAM can display the status of any or all explicit and virtual routes in the domain.

Sets of Resources: The ACF/VTAM operator can display sets of resources by type, such as lines, major nodes, and paths.

Stations: The ACF/VTAM operator can display the status of all cross-subarea link stations within any or all major nodes in the domain.

TSO User ID Status: The ACF/VTAM operator can display the status of a TSO user ID and such information as the LU name.

Dynamic Reconfiguration: Nonswitched SNA devices can be added and deleted from an NCP configuration without bringing the NCP down and reloading it with an NCP generated for the new configuration. The dynamic reconfiguration remains in effect as long as either ACF/VTAM or the NCP are active.

Forced Deactivation of a Link: For certain resources (including links), when immediate and normal deactivation are not successful, the ACF/VTAM operator can force deactivation.

Forced Session Termination: The ACF/VTAM operator can terminate a particular session or set of sessions without deactivating either session partner.

NLDM Session Awareness Function Support: Session notification from ACF/VTAM and ACF/NCP allows NLDM to provide session awareness data. This includes session start time, session type, routes used, and the names of both session partners. For interconnected networks, added information is provided, such as transformation addresses and alias names.

Operator Command Modification: System programmers can change certain ACF/VTAM operator commands to satisfy installation needs. For example, you might want to replace the operator command "MODIFY" with "CHANGE," because most other programs at your installation use "CHANGE" for similar functions

Operator Message Modification: System programmers can change certain ACF/VTAM operator messages to satisfy installation needs. For example, if you have replaced the operator command "MODIFY" with "CHANGE," you will want to make a similar replacement in the operator message MODIFY FAILED-CONFLICTING OPTIONS.

PEP Modules: Loading Over a Link: The ACF/NCP Partitioned Emulation Program Extension load module can be loaded over a data link to a channel-attached communication controller.

Route Verification and Error Notification: An ACF/VTAM operator can test whether a route originating in the operator's host or in an ACF/NCP owned by the operator's host is operative by specifying the route number and the ends of the route. If not, information is returned to aid in finding the inoperative part of the route. Owners of any inactive or inoperative resources on the route are notified.

> **Note:** ACF/VTAM itself can test routes only through networks adjacent to its own network. The IBM program product NLDM can make a test of any route in a series of connected networks.

3036 Console Allocation as a Terminal: When a 3036 Console is not allocated as a system operator's console, it can be allocated as a user terminal.

Network Performance

Figure 2-6 lists functions that affect network performance.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
	X	X	Dynamic CDRSC definition retention		ACF/VTAM ACF/NCP			X	X	X
X	X	X	Maximum RU size replaceable constant in ACF/VTAM		ACF/VTAM ACF/NCP			X	X	X
X	X	X	Network Performance Analyzer		ACF/VTAM ACF/NCP				X	X
X	X	X	Processing time in ACF/VTAM	Message delay function	ACF/VTAM ACF/NCP	X	X	X	X	X
X	X	X		Subtasks	ACF/VTAM ACF/NCP			X	X	X
X	X	X	Storage use in ACF/VTAM	CSA limit	ACF/VTAM ACF/NCP		X	X	X	X
X	X	X		Dynamic buffering	ACF/VTAM ACF/NCP	X	X	X	X	X
X	X	X		Maximum active application storage use	ACF/VTAM ACF/NCP			X	X	X
X	X	X		Session initialization and termination	ACF/VTAM ACF/NCP		X	X	X	X
X	X	X		Session outage notification	ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X	Transmission group thresholds		ACF/VTAM ACF/NCP					X
X	X	X	Tuning statistics in ACF/VTAM	Communication controllers	ACF/VTAM ACF/NCP	X	X	X	X	X
X	X	X		Channel-attached hosts	ACF/VTAM ACF/NCP				X	X
X	X	X		Cluster controllers	ACF/VTAM ACF/NCP	X	X	X	X	X

Note: These functions are described below.

Figure 2-6. ACF/VTAM and ACF/NCP Functions Used in Network Performance

Dynamic CDRSC Definition Retention: You can specify the minimum amount of time ACF/VTAM is to retain a dynamic definition of a cross-domain resource after the last session with the resource has ended. This function allows you to balance the storage used for the CDRSC definition and processing time that would be used if the CDRSC had to be defined again.

Maximum RU Size Replaceable Constant in ACF/VTAM: You can set a maximum length for request units (RUs) in LU-to-LU sessions and a maximum for SSCP sessions (SSCP-to-LU, SSCP-to-PU, and SSCP-to-SSCP).

Network Performance Analyzer: The Network Performance Analyzer (NPA) program product collects performance data about various devices in the network. NPA can highlight causes of performance degradation, such as excessive activity

at certain periods or insufficient data link capacity. It can also help isolate performance problems resulting from high data link or cluster error rates caused by temporary errors or wide fluctuations in message rates. By analyzing NPA data, a user can tune his network for greater efficiency and improved response time.

In systems with the Partitioned Emulation Program, NPA collects data only from devices controlled by ACF/NCP. It ignores devices controlled by the emulation program. If a link is switched back and forth from network control mode to emulation mode, NPA collects data only when the link is in network control mode.

NPA collects performance data for the following devices:

- Communication controllers
- Switched or nonswitched SDLC data links
- Type 1 and type 2 physical units
- Logical units
- BSC links attached to components of the 3270 Information Display System.

Processing Time in ACF/VTAM: The following functions affect processing time:

Message Delay Function: ACF/VTAM automatically delays sending path information units (PIUs), in order to queue multiple PIUs for transmission in a single operation and thus save processor cycle time. You can override the delay default values for traffic with both channel-attached hosts and channel-attached ACF/NCPs.

Subtasks: You can specify the maximum number of concurrent subtasks to be used for loading an ACF/NCP, dumping an NCP, making a node list request, sending a write-to-operator request, activating SNA physical units, or establishing cryptographic sessions (Encrypt/Decrypt Feature only).

Storage Use in ACF/VTAM: The following functions affect ACF/VTAM's use of storage:

CSA Limit: At ACF/VTAM start time, you can adjust the maximum amount of common storage area (CSA) ACF/VTAM can allocate. You can also reset the maximum dynamically while ACF/VTAM is executing.

Dynamic Buffering: You can set smaller basic allocation values for buffer pools, and ACF/VTAM will meet larger peak demand on the pool dynamically. In this manner, buffer pools can expand and contract as needed, without your having to specify large values to meet the greatest possible demands.

Maximum Active Application Program Storage Use: You can limit the amount of storage that ACF/VTAM can allocate from the application private area.

Session Initialization and Termination: You can specify the combined number of session-initiation, session-termination, and unformatted systems services (USS) requests that ACF/VTAM can process simultaneously. Although the IBM default is good for most installations, in some cases overriding it can avoid an over-commitment of storage.

Session Outage Notification: You can specify the maximum number of fixed I/O buffers available for session outage notification processing request units (RUs). This is a control on fixed (real) storage.

Transmission Group Thresholds: You can specify thresholds to affect virtual route (VR) pacing for transmission groups. During ACF/NCP generation, you specify thresholds for the maximum amount of data queued for transmission. The ACF/NCP uses this threshold to determine when to change the VR pacing window size. ACF/NCP compares the specified threshold against the amount of data waiting to be sent over the transmission group. When a threshold is reached, ACF/NCP sends a response that changes the VR pacing window size.

Tuning Statistics in ACF/VTAM: You can have ACF/VTAM keep statistics on the state of data-transfer operations between ACF/VTAM and one channel-attached SNA cluster controller or communication controller, or between channel-to-channel attached processors.

Problem Determination and Network Maintenance

Figure 2-7 lists functions that affect problem determination and network maintenance.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X	X	Communication network management interface	Maintenance application programs	ACF/VTAM / ACF/NCP			X	X	X
X	X	X		Downstream Load Utility	ACF/VTAM / ACF/NCP			X	X	X
X	X	X		Default routing of requests	ACF/VTAM / ACF/NCP					X
X	X	X	Dump data set selection for ACF/NCPs		ACF/VTAM / ACF/NCP				X	X
X	X	X	Dumps for 3725 Communication Controllers		ACF/VTAM / ACF/NCP			X	X	X / X
X	X		Dynamic ACF/NCP storage display		ACF/VTAM / ACF/NCP	X / X	X / X	X / X	X / X	X / X
X	X		Intensive mode error recording (IMR)		ACF/VTAM / ACF/NCP		X / X	X / X	X / X	X / X
X	X	X	Line-to-port mapping for ACF/NCP		ACF/VTAM / ACF/NCP					X
X	X		Link Problem Determination Aid (LPDA)	Basic test commands	ACF/VTAM / ACF/NCP		X	X	X	X
X	X			Channelized and tailed modems	ACF/VTAM / ACF/NCP					X
X	X			Remote self-test command	ACF/VTAM / ACF/NCP					X
X	X		Logical unit connectivity test		ACF/VTAM / ACF/NCP		X / X	X / X	X / X	X / X
X	X	X	NLDM connectivity test support		ACF/VTAM / ACF/NCP					X / X
X	X	X	Operator messages with names of issuing ACF/VTAM modules		ACF/VTAM / ACF/NCP			X	X	X
X	X	X	PTF numbers with ACF/VTAM module names		ACF/VTAM / ACF/NCP				X	X
X	X	X	Route verification and error notification		ACF/VTAM / ACF/NCP			X / X	X / X	X / X
X	X		SDLC link level 2 test		ACF/VTAM / ACF/NCP		X / X	X / X	X / X	X / X
X	X	X	Time-out messages from ACF/VTAM		ACF/VTAM / ACF/NCP			X	X	X

Figure 2-7 (Part 1 of 2). ACF/VTAM and ACF/NCP Functions Used in Problem Determination and Network Maintenance

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X	X		ACF/NCP dispatcher trace	ACF/VTAM / ACF/NCP				X	X
X	X	X		ACF/NCP SVC trace	ACF/VTAM / ACF/NCP				X	X
X	X	X		ACF/VTAM internal trace	ACF/VTAM / ACF/NCP	X	X	X	X	X
X	X	X		ACF/VTAM replaceable constant for buffer use trace	ACF/VTAM / ACF/NCP			X	X	X
X	X		Traces	Generalized PIU trace	ACF/VTAM / ACF/NCP				X / X	X / X
X	X	X		I/O trace enhanced	ACF/VTAM / ACF/NCP				X	X
X	X	X		NLDM session trace support	ACF/VTAM / ACF/NCP			X	X / X	X / X
X	X	X		3725 Scanner interface trace	ACF/VTAM / ACF/NCP			X	X / X	X / X
X	X			Transmission group trace	ACF/VTAM / ACF/NCP			X / X	X / X	X / X
Note: These functions are described below.										

Figure 2-7 (Part 2 of 2). ACF/VTAM and ACF/NCP Functions Used in Problem Determination and Network Maintenance

Communication Network Management Interface: Authorized application programs can use the CNM interface to receive information from the network and perform network services.

Maintenance Application Programs: Maintenance application programs can request and receive status and maintenance data from physical units in the same domain.

Downstream Load Utility: The IBM program product Downstream Load Utility can receive and fulfill load requests from certain Type 2 physical units in the same domain.

Default Routing of Requests: IBM provides as an ACF/VTAM module a default CNM routing table containing an entry for each IBM program product authorized to use the interface. This relieves you of having to recode your own CNM table when you acquire programs such as NPDA and NLDM.

Dump Data Set Selection for ACF/NCPs: The ACF/VTAM operator can override the dump data set selection specified during NCP generation. The operator can specify a particular data set or ask ACF/VTAM to choose one.

Dumps for the 3725 Communication Controller: The 3725 operator can dump the microcode for the communication scanner processor (CSP) and maintenance and operator subsystem (MOSS). ACF/VTAM writes the dumps on specified files.

Dynamic ACF/NCP Storage Display: The ACF/VTAM operator can have up to 256 bytes of ACF/NCP storage displayed at a time without interrupting ACF/NCP execution.

Intensive Mode Error Recording (IMR): The ACF/VTAM operator can request detailed information on temporary SDLC line errors or other hardware error conditions. This information could eliminate the need to test the link to re-create the error condition. If the IBM program product Network Problem Determination Application (NPDA) is installed, ACF/VTAM can send it copies of the IMR records.

Line-to-Port Mapping for ACF/NCP: To help in problem determination, when an NLDM user specifies a station network name, ACF/NCP provides the communication controller port address of the line to which the device is attached.

Link Problem Determination Aid (LPDA) :LPDA (link problem determination aid): LPDA provides data about network components as follows:

Basic Test Commands: LPDA provides a set of test commands that are executed by an IBM 3863, 3864, or 3865 modem or by an IBM 3867 Link Diagnostic Unit. The ACF/NCP issues LPDA commands to determine which of various network components might be causing an error in the network. ACF/NCP issues LPDA commands when either:

- The Network Problem Determination Application (NPDA) program product in the host processor solicits data about network components.
- The ACF/NCP has quality and status information about network components to send to the NPDA for processing.

Channelized and Tailed Modems: ACF/NCP provides the LPDA function for channelized (multiplexed) IBM 3865 Model 1 modems. It also provides the LPDA function for tailed IBM 3863 and 3864 modems. Tailed modems are modems attached to a link-attached channelized 3865 modem.

Remote Self-Test Command: The ACF/NCP allows an application program at the host processor to issue a remote self-test command to an IBM 3863, 3864, or 3865 modem. The results from the command contain information on modem configuration, engineering change level, and failing field-replaceable units. This information is sent to the application program that issued the command.

Logical Unit Connectivity Test: Terminal users can test the physical path between their terminals and ACF/VTAM by issuing a command from their terminals.

NLDM Connectivity Test Support: ACF/NCP provides session virtual-route-to-explicit-route mapping to NLDM. It also provides to NLDM the configuration of the explicit route (ER) from one end of the session to the other end, including the hosts, ACF/NCPs, and transmission groups that make up the route. When an NLDM user requests a path test, ACF/NCP sends an ER test to the other end of the session. The ER test reply contains the data requested by the user.

Operator Messages with Names of Issuing ACF/VTAM Modules: You can specify that ACF/VTAM messages will contain the last five characters of the names of the modules issuing the messages.

PTF Numbers with ACF/VTAM Module Names:The latest PTF number is placed next to each module name appearing in a dump of ACF/VTAM.

Route Verification and Error Notification: Route verification allows a network operator to verify that a given route can be used for data transmission before assigning it to message traffic. Route verification also allows the operator to take corrective action for an inoperative route and to verify that a previously inoperative route can again be used for data transmission after being reactivated.

The route verification function identifies the physical element in the route that failed and notifies, through the access method, the operator requesting the verification and the network operators for all host processor subareas that share ownership of the subarea in which the inoperative element is located.

Owners of any inactive or inoperative resources on the route are notified.

SDLC Link Level 2 Test: The ACF/VTAM operator can test for faulty transmission over an SDLC line between an ACF/NCP and one of its physical units or between two ACF/NCPs.

Time-out Messages from ACF/VTAM: You can specify the number of seconds before ACF/VTAM issues an informational time-out message relating to a pending response to a request unit sent by ACF/VTAM to another ACF/VTAM, a physical unit, or a logical unit.

Traces: You can use the following to trace information:

ACF/NCP Dispatcher Trace: A dispatcher trace records the control flow activity in program level 5 of an ACF/NCP. It is started whenever ACF/NCP is loaded into the communication controller.

ACF/NCP SVC Trace: The supervisor call (SVC) trace records certain registers in Level 5 of ACF/NCP code each time an SVC is issued. This trace is activated from the 3705 control panel or the 3725 console.

ACF/VTAM Internal Trace: You can have events in ACF/VTAM processing traced, such as channel I/O, use of locks, and storage management services.

ACF/VTAM Replaceable Constant for Buffer Use Trace: You can specify the frequency with which snapshot dumps are taken for the buffer use (SMS) trace.

Generalized PIU Trace: You can trace the data flow to or from a physical unit or logical unit attached to a communication controller without including link-level protocol data.

I/O Trace Enhanced: Previously, the ACF/VTAM I/O trace had provided details of PIU traffic among components of ACF/VTAM, as well as traffic between ACF/VTAM and rest of the network. The internal tracing has turned out to be extraneous and has been removed.

NLDM Session Trace Support: ACF/VTAM provides session-activation parameters for the NLDM session trace, as well as the leading characters of the data portions of PIUs transmitted during a session. ACF/NCP provides the contents of selected control block fields associated with the ACF/NCP's logical units, as well as the PIU's last sequence numbers used for transmission.

3725 Scanner Interface Trace: The ACF/NCP for a 3725 Communication Controller forwards data collected by the communication scanner processor (CSP) line scanner to ACF/VTAM, which writes it on a specified file.

Transmission Group Trace: The ACF/VTAM line trace has been expanded to include transmission groups.

Network Recovery

Figure 2-8 lists functions that affect network recovery.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X		Forced deactivation of a link	Basic function	ACF/VTAM ACF/NCP	X X	X X	X X	X X	X X
X	X			Enhancement	ACF/VTAM ACF/NCP					X
X	X	X	Forced session termination		ACF/VTAM ACF/NCP				X X	X X
	X	X	Nondisruptive ACF/NCP takeover		ACF/VTAM ACF/NCP			X X	X X	X X
	X	X	Nondisruptive SSCP restart		ACF/VTAM ACF/NCP			X X	X X	X X
X	X	X	Session outage notification		ACF/VTAM ACF/NCP			X X	X X	X X
	X	X	SSCP-to-SSCP resynchronization		ACF/VTAM ACF/NCP			X	X	X

Note: These functions are described below.

Figure 2-8. ACF/VTAM and ACF/NCP Functions Used in Network Recovery

Forced Deactivation of a Link: The following functions are related to forced deactivation of a link:

Basic Function: The ACF/VTAM operator can force deactivation of a link. This allows the operator to reset a resource that does not respond to normal deactivation commands, without having to re-IPL the ACF/NCP.

Enhancement: The enhancement requires fewer I/O operations and thus reduces the chance of "hung" conditions. Deactivation takes place regardless of other shared owners of the resource, although they are notified of the deactivation.

Forced Session Termination: The ACF/VTAM operator can terminate a session or a set of sessions without deactivating either of the session partners. This is useful after SSCP restart or after an SSCP-to-SSCP session has failed, when the SSCP owning a logical unit in session no longer has enough information to provide session termination services.

Nondisruptive ACF/NCP Takeover: Another host can become owner of an ACF/NCP and its resources if the host that owns the ACF/NCP fails. The process involves deactivation and reactivation of each resource by the new owner, and ordinarily this means disruption of any sessions associated with those resources. However, if the devices support nondisruptive activation commands, their session will continue.

Nondisruptive SSCP Restart: A session with a nonswitched LU that continues when the associated SSCP-to-PU and SSCP-to-LU sessions fail can continue when the SSCP reactivates the PU and LU, provided that they support the nondisruptive activation commands. Otherwise, the sessions are terminated.

Session Outage Notification: If a virtual route becomes inoperative, the primary and secondary LUs for the sessions it is supporting are notified of the outage. The LUs can then try alternative routes.

SSCP-to-SSCP Resynchronization: A cross-domain LU-to-LU session normally continues when the associated SSCP-to-SSCP session fails and is restarted. (The exception occurs when the failure was due to route failure and both sessions were on that route.)

Figure 2-9 lists functions in ACF/VTAM Version 2 Release 2 that affect network security.

Type of Network			Function		Release Effected In				
S	M	I			V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X	X	Encrypt/Decrypt program product support	ACF/VTAM ACF/NCP	X	X	X	X	X
		X	Preventing ACF/NCP activation by another network	ACF/VTAM ACF/NCP					X
X	X	X	Session management exit routine	ACF/VTAM ACF/NCP					X
Note: These functions are described below.									

Figure 2-9. ACF/VTAM and ACF/NCP Functions Used in Network Security

Encrypt/Decrypt Program Product Support: Using the IBM program products ACF/VTAM Encrypt/Decrypt Feature and Programmed Cryptographic Facility, you can have selected messages encrypted before passing over public links and decrypted upon arriving at their destination.

Preventing ACF/NCP Activation by Another Network: You can prevent the ACF/VTAMs in another network from activating an ACF/NCP in your network. Parameters can be specified during definition of the ACF/NCP to prevent activation by all SSCPs of other networks. This function provides security for a network that is to control a gateway ACF/NCP.

Session Management Exit Routine: ACF/VTAM has a session management exit for which you can write a routine to provide authorization of logons to application programs.

The exit provides cross-network information and capabilities that the current exits do not have. You can also use it to perform the same single-network functions, however.

Application Programming

Figure 2-10 lists functions that affect ACF/VTAM application programs.

Type of Network			Function			Release Effected In				
S	M	I				V1 R1	V1 R2	V1 R3	V2R1 V2	V2R2 V3
X	X	X	Application program ACB	Level of access method support	ACF/VTAM / ACF/NCP				X	X
		X		Level of access method support (cross-network)	ACF/VTAM / ACF/NCP					X
X	X	X		User field	ACF/VTAM / ACF/NCP				X	X
X	X	X	Application program-to-application program session pacing		ACF/VTAM / ACF/NCP	X	X	X	X	X
X	X	X	Application program-to-application program sessions in the same host		ACF/VTAM / ACF/NCP	X	X	X	X	X
X	X	X	Large message performance enhancement option		ACF/VTAM / ACF/NCP				X	X
X	X	X	Negotiable session-initiation parameters		ACF/VTAM / ACF/NCP		X / X	X / X	X / X	X / X
X	X	X	Noncontiguous buffers for messages		ACF/VTAM / ACF/NCP				X	X
X	X	X	Parallel sessions		ACF/VTAM / ACF/NCP		X	X	X	X
X	X	X	User RH		ACF/VTAM / ACF/NCP				X	X
Note: These functions are described below.										

Figure 2-10. ACF/VTAM and ACF/NCP Functions Used in Application Programming

Application Program ACB: The following functions are effected through the ACB of an application program:

Level of Access Method Support: After its ACB is opened, an application program can determine the level of support it can expect from the ACF/VTAM it is using. This information includes a list of application program-related ACF/VTAM functions provided, as well as the access method release number. The function can lessen the coordination a system programmer must do when installing either ACF/VTAM or the application program.

Level of Access Method Support (Cross-Network): Cross-network information is also provided for the ACF/VTAM in this domain, that is, the network ID, the name used for the ACF/VTAM, and the name and address used for the ACF/VTAM host subarea PU.

User field: The ACB for an application program contains a pointer that may be used for establishing user control block addressability in user exit routines.

Application Program-to-Application Program Session Pacing: Bidirectional pacing is available for sessions between two application programs.

Application Program-to-Application Program Sessions in the Same Host: Application programs can be in session with other applications in the same host, as well as in other hosts.

Large Message Performance Enhancement Option: Application programs can send messages of any length with a single ACF/VTAM instruction, simplifying application program code and reducing its path length. Generally, application programs can ignore the maximum RU requirements of its session partners. Larger messages also improve ACF/VTAM performance overall for sending and receiving messages.

Negotiable Session-Initiation Parameters: The primary end of a session can send a negotiable Bind request, which the secondary LU and its boundary function can reply to with a changed Bind image. The primary end either agrees to the new session parameters or sends an Unbind. This function allows network components to have more control over the session-initiation process.

Noncontiguous Buffers for Messages: Application programs can send messages stored in noncontiguous buffers.

Parallel Sessions: Two application programs can have more than one session between them at a time.

User RH: Application programs can specify RH indicators for each request it sends, whether the requests are sent separately or as a set of multiple requests.

ACF/SSP Functions

The Advanced Communications Function for System Support Programs (ACF/SSP) program product helps you create, install, use, and maintain an ACF/NCP and consists of the following:

- An ACF/NCP generation procedure
- A communication controller assembler program
- A loader utility
- A dump utility
- A dynamic dump utility
- A trace analysis program
- A configuration report program.

ACF/NCP Generation Procedure

The generation procedure creates an ACF/NCP load module that meets the special requirements for your network. A generation language is used to specify network configurations and program options; source statements are expanded from a library of macro definitions.

Generation Language

The generation language provides a simple means for creating an ACF/NCP load module and is designed to minimize the programming required for even the most complex configurations of data links and devices. It is made up of five types of macro instructions: system macros, configuration definition macros, network configuration macros, block-handling macros, and generation delimiter macros.

Generating Multiple ACF/NCPs

As many ACF/NCP load modules as desired can be generated for a communication controller. Each program requires a separate generation, and each must have a different symbolic name to enable the loader to identify the load module to be transferred into the communication controller.

Multiple load modules are useful for installations that have several distinct applications for the network at different times.

Communication Controller Assembler

A communication controller assembler is available to assemble programs written in controller assembler language. It is used for assembling the ACF/NCP generation macros and application-dependent modules during the generation process. It is also used for preassembling user-written block-handling routines.

The assembler enables you to add to the ACF/NCP modules block-handling routines unique to your installation's applications. You use the controller assembler language to code the block-handling routines, and then you use the assembler to create object modules. Your object modules are stored in the library with the IBM-supplied ACF/NCP object modules. If the appropriate ACF/NCP macros have been coded, then, during program generation, the modules with the block-handling routines are link-edited with IBM modules to form the ACF/NCP load module.

Conditional Assembly Removal

Before ACF/NCP Version 3, some modules were conditionally assembled during ACF/NCP generation based on which functions were requested. In ACF/NCP Version 3, all conditional assembly has been removed. The modules are now preassembled and shipped in object code form. The preassembly reduces the time required for ACF/NCP generation.

To remove conditional assemblies, code that had been included only if a function was requested is now a standard part of the module. This code will be present whether or not the associated options are present in the generation input source. The storage impact due to conditional assembly removal depends on the previous size of the ACF/NCP configuration. An ACF/NCP generation with few options specified will have a larger storage increase than a generation with many options. A user can expect a storage increase between 5K bytes and 30K bytes, with the average being 15K bytes.

Loader Utility

The loader utility has two functions: (1) testing the communication controller with an initial test routine and (2) transferring the ACF/NCP load module from the host processor to the communication controller.

You can use the loader utility to load a channel-attached communication controller only. To load a link-attached controller, you must use an access method loader routine. (You can also use the access method loader routine to load a channel-attached controller.)

The initial test routine of the loader utility is used before the ACF/NCP is loaded. The test routine tests the hardware for conditions that, if not detected could result in the failure of the communication controller during network operations. If exceptional conditions are detected during testing, the loader utility cancels the loading of the ACF/NCP from the host processor to the controller.

The loading function of the utility loads the ACF/NCP load module into the communication controller when the controller is started or when it fails because of an error condition. The operator starts the loader utility with job control statements in the job stream. When the loader is invoked, the initial test routine is started automatically unless its operation is suppressed by a utility control card entered as input to the loader.

Dump Utility

The dump utility dumps the contents of communication controller storage. If desired, you can specify the limits of the storage area to be printed, or you can request a formatted dump. If the limits are not specified, the utility prints the complete dump. If a formatted dump is requested, the utility labels certain control blocks and prints them at the beginning of the dump.

Both formatted and unformatted dumps show the hexadecimal representation of controller storage. All dumps include the contents of the general registers and the EBCDIC representation of all letters and numbers in the dump.

You can run the dump utility as a stand-alone job under OS/VS systems, or the access method can invoke it.

Dynamic Dump Utility

The dynamic dump utility can be used only when ACF/NCP is executed in emulation mode. The contents of communication controller storage are transferred from the controller to the host processor without interrupting operation of the ACF/NCP. After the transfer, you can display, at the console, either all of the storage, portions of the storage, or emulation mode line trace tables.

Trace Analysis Program

The Advanced Communications Function/Trace Analysis Program (ACF/TAP) helps in analyzing certain trace data produced by ACF/NCP, ACF/VTAM, and ACF/TCAM. ACF/TAP merges and formats SNA and SDLC trace data into formatted output reports.

The primary ACF/TAP report has up to four different formats and shows the following:

- Input control parameters and error messages
- Summary of the Generalized Trace Facility (GTF) and the ACF/VTAM, ACF/TCAM, or ACF/NCP line trace header information that precedes trace data
- Input records in standard hexadecimal and alphanumeric dump format
- ACF/TAP-processed trace data and ACF/TAP interpretation of the SNA and SDLC header information from the trace data.

Besides the primary ACF/TAP report, ACF/TAP can produce eight other reports describing the contents of input trace files:

- Line trace detail report
- Line trace summary report
- Line trace, with option, report
- SNA detail report
- SNA summary report
- Generalized PIU Trace summary report
- Network data traffic report
- Network error report.

Unusual conditions that may indicate error situations are highlighted in the reports.

Configuration Report Program

The Configuration Report Program is a stand-alone program that produces a detailed report of the resources and resource attributes of your network configuration. The report presents information separately for SNA and non-SNA devices. You can tailor the report to include various characteristics about network resources, such as resource name, network address, control unit type, line type and speed, and line control protocol.

NCCF Functions

This section contains a general description of NCCF followed by a description of the enhancements made to this program product since NCCF Version 1 Release 1.

Introduction to NCCF Functions

The Network Communications Control Facility (NCCF)) lets you control, record, and automate various operator tasks. NCCF can be used as an operator's interface to various levels of ACF/VTAM or ACF/TCAM or both in a data communication network. NCCF provides optional logging of operator commands and messages on either disk or printers. NCCF is a program base for communication network management (CNM). To provide additional functions beyond those given by NCCF, you can customize your network by writing your own command lists, command processors, exit routines, and subtasks to run on NCCF.

NCCF operates as an application program under a telecommunication access method. It uses 3270 devices as operator terminals and hard-copy printers.

NCCF and Communication Network Management (CNM)

NCCF provides CNM functions such as network operation, services for processing VSAM files, and operator authorization, data security, and auditing.

NCCF can automate many operator tasks and processes. It is also a program base for the following CNM functions:

- Problem determination
- Configuration management

- Change management
- Problem management.

These CNM functions are provided by IBM program products that run with NCCF or by programs that you write. NCCF lets network management be centrally located. Using these NCCF and CNM functions, an installation can make its network easier to manage. For more information on CNM and its related products, see the section for NCCF in "Appendix A. Supported Products."

Basic NCCF Functions

Specific functions available under NCCF Version 1 Release 1 are described in the following text. The section on NCCF in "Appendix A. Supported Products" lists the access methods supported for each function.

- *CNM Interface Support*: NCCF gives you input, output, and recovery functions that let command processors request problem determination data from the access method across the CNM interface. A CNM processor, such as the Network Problem Determination Application (NPDA), may be used to retrieve and format error data.

- *Operator Control*: You can have multiple network operators, each one having assigned responsibilities. These operators can be at various locations throughout a network. NCCF terminal operators can enter access method control commands to modify and display your network's configuration.

- *Cross-Domain Communication*: A NCCF operator can communicate with an NCCF in another domain and also cause execution of commands in other domains. NCCF also lets you send commands to other domains for execution and then return the responses from these domains to the issuing operator.

- *Span of Control*: You can restrict an operator's control to a subset of the network's resources. Spans can overlap, so that more than one operator can control the same resource.

- *Command Lists*: A command list (CLIST) is a sequence of access method commands, NCCF commands, and your own commands that are stored in a file and invoked by name for execution when required. A CLIST can also be invoked by a solicited or unsolicited access method message. (A solicited message is in response to a command. An unsolicited message reports an unexpected event, such as the failure of a network resource.) Command lists can be used by an installation to automate and simplify network operations.

- *Data Security and Auditing*: NCCF gives you data security by checking operator logons. You can also define your own exit routines at various points throughout the program to screen and edit data traffic.

- *Data Services*: An optional NCCF data services task gives you VSAM support for disk files. You can use these data services as a part of CNM support on all access method levels supported by NCCF or as part of the CNM processor.

- *Customization*: Using NCCF's macro services, you can manage access method-independent screens and process terminal input and output with your own command lists, command processors, exit routines, and subtasks. These provide additional functions beyond those that NCCF gives you. For more information on how to customize your network operation, see the publication *NCCF Customization*.

- *Screen Modes*: Version 1 Release 1 of NCCF has two screen modes:

  - Standard NCCF mode, with a 12-character preface, followed by 68 data characters with 68-character continuation lines.

  - Full-line mode, with 80-character output. This mode is used by application programs such as NPDA to present data in a tabular manner.

Functional Enhancements to NCCF

Figure 2-11 lists NCCF functional enhancements since Version 1 Release 1. Use the table as follows:

- Under "Type of Network" on the left, an "X" under the "S" column tells you that the function can be used in a single-domain network; under "M" it can be used in a multiple-domain network; and under "I" with interconnected networks.

- The functions are listed alphabetically in the center of the table; descriptions of the functions appear after the table in the same order.

- Under "Release Effected In" on the right, an "X" appears under each release of NCCF that has the function.

If you are migrating from NCCF Version 1 Release 1, all the functions listed in the table are new to your installation. But if you are migrating from Version 1 Release 2 and you have a single-domain network, the first function that can be used in a single-domain network is "ASCII-8 support." Under "Release Effected In" there is no "X" for "Version 1 Release 2;" thus, the function is new to your installation and you may want to read about it in the description following the table.

Type of Network			Function		Release Effected In	
S	M	I			Version 1 Release 2	Version 2
	X	X	Alias name translation (ACF/VTAM only)			X
X	X	X	ASCII-8 support			X
X	X	X	Commands	Initial	X	X
X	X	X		Scope of	X	X
X	X	X		Timer-initiated	X	X
X	X	X	Command lists (CLISTs)	Command entry while in CLIST PAUSE or WAIT		X
X	X	X		Conditional	X	X
X	X	X		Continuation statements		X
X	X	X		Enhanced network automation		X
X	X	X		Initial	X	X
X	X	X		Timer-initiated	X	X
X	X	X	Katakana translate table			X
X	X	X	Logon authorization extension		X	X
X	X	X	Long-running command support			X
X	X	X	Multiple data services tasks		X	X
X	X		Operator control extension (ACF/TCAM only)		X	X
	X	X	Presentation services enhancement		X	X
X	X	X	Storage savings			X
X	X	X	Terminal Access Facility	Separate program product	X	X
X	X	X		Integrated into NCCF		X
X	X	X	Usability	DSILGMOD requirement eliminated		X
X	X	X		Extended authorized receiver control		X
X	X	X		Multiple-line input	X	X
X	X	X		Nondeletable messages		X
X	X	X		Predefined definitions and JCL	X	X
X	X	X		Program function key support		X
X	X	X		Timed autowrap		X
X	X	X		VSAM disk log	X	X

Note: These functions are described below.

Figure 2-11. Functional Enhancements to NCCF Since Version 1 Release 1

Alias Name Translation (ACF/VTAM Only): NCCF provides support to allow sessions between two or more networks to maintain their own network naming conventions even though there may be conflicts between duplicate names. Network names do not have to be redefined to ensure uniqueness in the case of LUs, or name correspondence in the case of class of service (COS) and logmode (MOD) names. This support acts as a service for gateway ACF/VTAMs. It can also be used as a directory of domains for cross-domain session setup within the same network.

ASCII-8 Support: NCCF checks the BIND image at logon time to determine the type of translation to be used for terminal I/O processing on a session basis.

Commands: The following functions relate to commands:

Initial: You can define NCCF so that a command executes automatically when NCCF starts.

Scope of: You can restrict operator use of the IBM-supplied commands, access method commands, and your own commands and operands. When you define NCCF operators and commands, you can limit the use of them to one operator or a group of operators. Commands not specifically restricted are available to all operators.

Timer-Initiated: You can start commands with a timer, at a certain time of the day or at regular intervals. The NCCF operator does not have to be logged on at the time the command is set to execute. An operator can list or purge pending timer-initiated commands.

Command Lists (CLISTs): The following functions relate to command lists:

Command Entry while in CLIST PAUSE or WAIT: With the new STACK and UNSTACK commands, an operator can enter commands and CLISTs while in CLIST PAUSE or WAIT state.

Conditional: You can control the execution sequence in a CLIST with control statements. You can code variables in CLISTs and substitute values at execution time. NCCF predefines some of these values. CLISTs can send messages to the NCCF operator and receive input while executing.

Continuation Statements: You can continue command list statements for as many lines as required. That is, a CLIST statement is no longer confined to text that can fit in one record.

Enhanced Network Automation: A new WAIT function enables a CLIST to wait for messages that would be displayed at the operator's terminal or for certain types of events to occur. This allows you to write CLISTs that require the synchronization of commands with expected responses and events.

Initial: You can define NCCF so that a command list executes automatically when NCCF starts.

Timer-Initiated: You can start command lists with a timer, at a certain time of the day or at regular intervals. The NCCF operator does not have to be logged on at the time the command list is set to execute. An operator can list or purge pending timer-initiated command lists.

Katakana Translate Tables: The standard NCCF EBCDIC translate tables used for terminal input, terminal and hard-copy output, and printing the log data set can be overridden with an NCCF definition statement to identify an alternate translate table. NCCF also provides a Katakana translate table you can use as the alternate table for Japanese-language applications.

Logon Authorization Extension: You can define NCCF so that a specific number of operators may log on to terminals that have not been otherwise identified to NCCF. This allows you to have a pool of NCCF terminals rather than having to define each terminal specifically to NCCF.

Long-Running Command Support: This function can be used by a command processor that must:

1. Return to NCCF before finishing in order to be redriven when a certain event has completed.

2. Be notified of task abends or logoffs.

3. Be able to save and retrieve storage addresses across multiple invocations.

Multiple Data Services Tasks: You can define multiple data services tasks to process CNM data or VSAM data bases.

Operator Control Extension (ACF/TCAM Only): An NCCF terminal can also act as an ACF/TCAM extended operator control station under ACF/TCAM Version 2 Releases 2, 3, and 4. The ACF/TCAM operator can have full ACF/TCAM use, as well as NCCF.

Presentation Services Enhancement: You can have full-screen, as well as the standard NCCF and full-line modes. In the full-screen mode 3270 commands, orders, and data are sent to the NCCF screen. This gives the command processors full control of the mode and contents of the screen.

Storage Savings: The amount of virtual storage required by NCCF can be reduced as follows:

- You can define command processors as nonresident so that NCCF will load and delete them as needed.

- NCCF now loads initialization code when needed and then deletes it.

- NCCF has a message scheme for reducing the size of NCCF message DSECTs. Lesser-used messages are now kept in members of partitioned data sets.

Terminal Access Facility: This optional feature of NCCF Version 1 Release 2 has been integrated into NCCF Version 2. You can start sessions from an NCCF terminal to:

- Customer Information Control System/Virtual Storage (CICS/VS)

- Information Management System/Virtual Storage (IMS/VS)

- Host Command Facility Version 2
  - 8100 Distributed Processing Program Executive (DPPX)
  - 8100 Distributed Processing Control Executive (DPCX)
- Time Sharing Option (TSO)
- Remote NCCF systems
- Distributed System Executive (DSX) Version 2.

Once in session with these products from the NCCF network operator, you can have greater control of network resources and use the individual applications that each subsystem provides. With ACF/VTAM, or ACF/TCAM using the Multisystem Networking Facility, the Terminal Access Facility can also be in cross-domain session with CICS/VS, IMS/VS, TSO, remote NCCF systems, and HCF.

The Terminal Access Facility supports two types of operation: full-screen sessions and operator-control sessions:

- In full-screen sessions, the facility acts as an SNA 3278 Model 2 in session with CICS/VS, IMS/VS, HCF, DSX, TSO, and remote NCCF systems. The Terminal Access Facility temporarily allocates the NCCF display screen to display-oriented applications that execute on those systems.
- In operator-control sessions, the facility acts as an SNA 3767 in a session with CICS/VS, IMS/VS, HCF, or DSX. It lets any transaction that can be entered from a 3767 attached directly to one of these subsystems be entered from the standard NCCF screen.

Support for the subsystems under the various access methods is shown in the section on NCCF in "Appendix A. Supported Products."

Usability: Several usability enhancements are now available:

DSILGMOD Requirement Eliminated: NCCF will accept any logmode with the required values. This allows you to consolidate your logmode tables and to use default values (such as those supplied by ACF/VTAM) if desired and applicable. With this change, you can also take advantage of the class of service (COS) function provided by ACF/VTAM for your NCCF operator terminals.

Extended Authorized Receiver Control: An installation can route unsolicited access method messages to multiple operators and define a search priority for message routing. The ASSIGN command is provided for this function.

Multiple-Line Input: You can adjust the NCCF command entry area to one, two, or three continuous 80-character lines. This allows operators to enter commands exceeding 80 characters.

Nondeletable Messages: A definition statement, HOLDMSG, can be used to define to NCCF those messages that are not to roll off the operator's screen. To delete these messages from the screen, the operator must key in a delete character next to the message.

Predefined Definitions and JCL: A set of basic definition statements and job control language (JCL) statements help you install and start NCCF more easily.

Program Function (PF) Key Support: PF and PA keys can be set to any command or CLIST by an operator using the SET command. The LIST function allows you to list the settings of your PF and PA keys.

Timed Autowrap: The AUTOWRAP command has been expanded to allow the operator to specify the length of time the screen will be held while in autowrap.

VSAM Disk Log: The NCCF log is maintained on a disk in a primary VSAM data set. When the primary data set is filled, logging is automatically switched to a secondary data set, if one has been defined. The primary data set can be printed offline while NCCF is still logging to the secondary data set. The SWITCH command is provided to control log switching from one log data set to another.

Logical Overview of NCCF Processing

Figure 2-12 illustrates how NCCF operates.

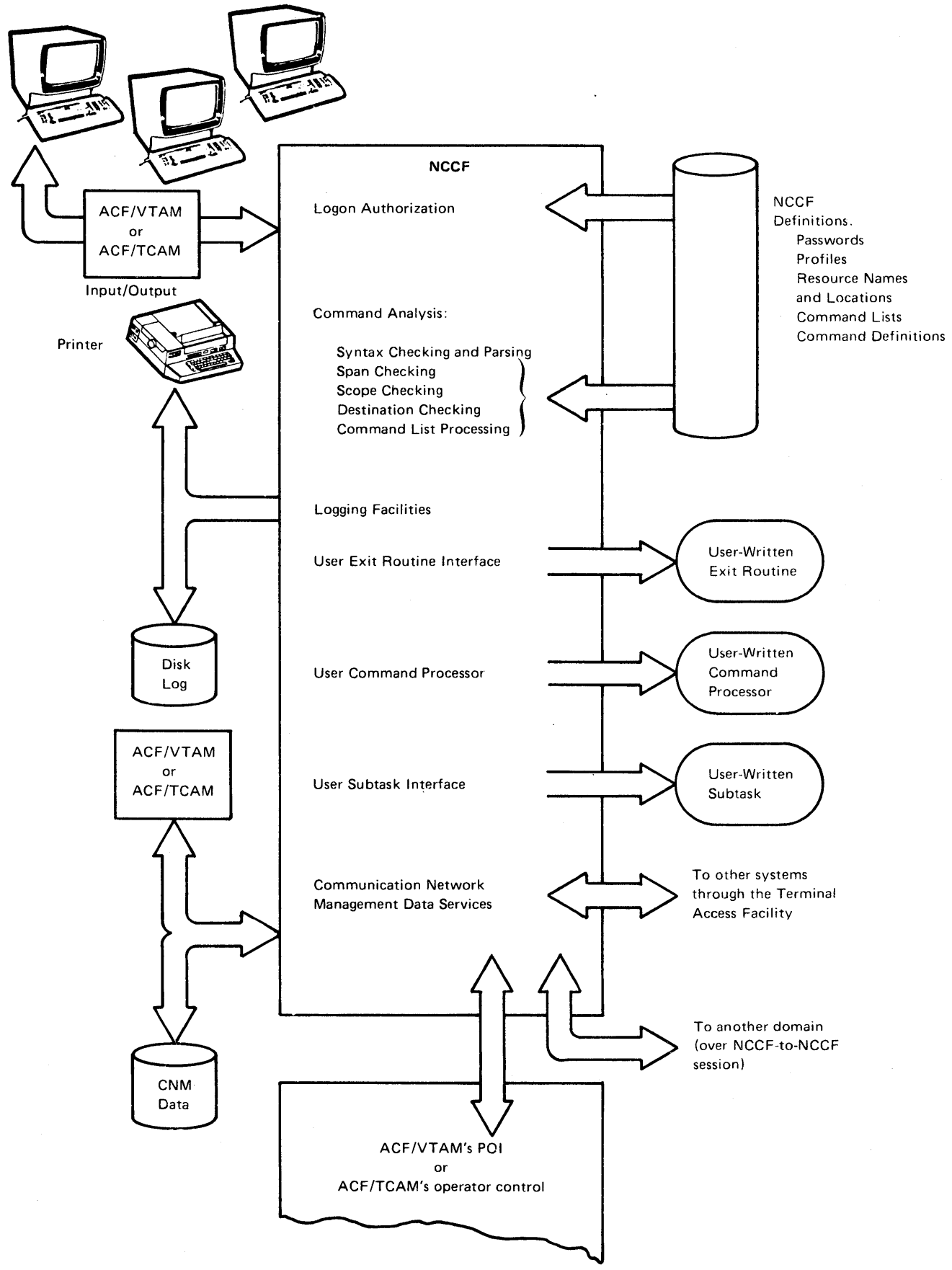


Figure 2-12. Overview of NCCF Operation

NLDM Functions

The Network Logical Data Manager (NLDM) Release 2 program product collects and correlates data about sessions and provides users with online access to the collected data. It allows a user at a central control point to examine information related to specific sessions and to identify network problems.

NLDM may be used in several ways, depending on the needs of a particular system or installation.

You may start NLDM either before or after the network is activated. To use NLDM to help identify the first occurrence of a problem, NLDM should be running all the time.

To use NLDM to help identify a subsequent occurrence of a problem, be sure that NLDM is initialized and that the network is activated. Then, begin traces of sessions involving the resources with which there is a problem.

NLDM collects data about same-domain, cross-domain, and cross-network sessions and maintains the collected session data on a session basis. Session awareness and routing data may involve non-SNA terminals supported by the IBM program product, Network Terminal Option (NTO), which appear to the host to be SNA devices. In addition, NLDM collects data relating to the data flows for BSC 3270 devices. Collecting data for cross-domain sessions requires NLDM in both domains. Collecting data for cross-network sessions requires NLDM in each network.

NLDM collects session data from ACF/VTAM and from ACF/NCP. The session data includes information about the session partners, session activation and deactivation, the physical configuration associated with the session, access method PIU data, and network control program (NCP) data.

NLDM collects response time data that has been measured by the Response Time Monitor (RTM) feature of a 3274. This data is measured within response time ranges specified by the customer.

NLDM runs as an application program under the Network Communications Control Facility (NCCF). Access to NLDM can be controlled by using security functions provided by NCCF. NLDM can coexist with the Network Problem Determination Application (NPDA) program product and with the IBM Threshold Analysis and Remote Access feature.

NLDM uses system functions provided by NCCF to communicate with the SNA access method and with the Virtual Storage Access Method (VSAM) data base in which the collected session data is stored. For more information about NCCF functions, refer to the section about NCCF.

Figure 2-13 lists NLDM functions in Releases 1 and 2. Use the table as follows:

- Under "Type of Network" on the left, an "X" under the "S" column tells you that the function can be used in a single-domain network; under "M" it can be used in a multiple-domain network; and under "I" with interconnected networks.
- Descriptions of the functions appear after the table in the same order.
- Under "Release" on the right, an "X" appears under the release of NLDM that has the function.

If you are migrating from NLDM Release 1, the first new function is "Initialization (with interconnected networks)." Under "Release" there is no "X" for "Release 1;" thus, the function is new to your installation and you may want to read about it in the description following the table.

Type of Network			Function		Release Effected In	
S	M	I			Release 1	Release 2
X	X		Initialization	No interconnected networks	X	X
		X		Interconnected networks		X
X	X		Collect session data	No interconnected networks	X	X
		X		Interconnected networks		X
X	X		Put data in the data base	No interconnected networks	X	X
		X		Interconnected networks		X
X	X		Start or stop collection of session awareness data	No interconnected networks	X	X
		X		Interconnected networks		X
X	X		Activate or deactivate session traces	No interconnected networks	X	X
		X		Interconnected networks		X
X	X		Display session data	No interconnected networks	X	X
		X		Interconnected networks		X
X	X		Test session connectivity	No interconnected networks	X	X
		X		Interconnected networks		X
X	X	X	Collect reponse time data			X
X	X	X	Display response time data			X
X	X	X	Display NLDM help information		X	X
X	X	X	Display the port address of a station			X
X	X	X	Display and change program function key settings			X
Note: These functions are described below.						

Figure 2-13. Functions in NLDM Releases 1 and 2

Initialization: NLDM is initialized whenever NCCF is initialized. During initialization the NLDM start-up parameters specified by the customer in an NCCF parameter definition data set are processed. One parameter which may be specified is the option to begin the collection of session awareness data at initialization. These start-up parameters provide the customer with the ability to use NLDM based on individual needs. For additional information about requests that may be included in the parameter definition data set, refer to the *NLDM Installation and Operation* manual.

Collect Session Data: NLDM collects data about SNA sessions involving logical units (LUs), physical units (PUs), or system services control points (SSCPs). SNA sessions for which NLDM can collect data are LU-LU, SSCP-LU, SSCP-PU, and SSCP-SSCP.

NLDM can collect two types of data about a session: session awareness data and session trace data.

- Session awareness data is collected for all active sessions. It includes:
  - The session type
  - The names of the session partners
  - The session activation status
  - Information about session and route configuration:
    - Addresses and names of subareas on the explicit route assigned to the session
    - Transmission group numbers
    - Addresses or names of SSCPs that own links in the transmission groups.

  For more information see "Session Awareness Data".

- Session trace data is collected only for sessions involving a resource for which a session trace has been started. It consists of:
  - Session activation parameters
  - Access method path information unit (PIU) data
  - ACF/NCP data.

  For more information see "Session Trace Data".

NLDM can collect response time data from a 3274 controller with the response time monitor feature. Response time is measured by the 3274 for each SNA transaction associated with it. NLDM collects response time only from each 3274 for which collection has been started. For more information see "Response Time Data".

Put Data in the Data Base: NLDM stores collected session data in a VSAM data base. The user specifies the name and size of the data base during the installation of NLDM. Session data associated with an active session is kept in main storage. When the session ends, the session data is copied from main storage into the VSAM data base. The user may also request that the data be transferred from main storage to the data base while the session is still active.

Session awareness data (including session termination notifications) is provided and kept by each ACF/VTAM that owns at least one session partner or is the gateway ACF/VTAM for a cross-network session.

Figure 2-14 shows the types of resources for which NLDM can collect session data.

Resource	Session Awareness Data	Session Trace Data	
		PIU Data and Session Activation Parameters	NCP Data
Channel-attached SNA terminals	X	X	
Channel-attached non-SNA terminals	X	X	
ACF/NCP-attached SNA terminals (includes BSC 3270 terminals)	X	X	X
NTO terminals (including BSC and start-stop terminals other than 3270s)	X	X	
Host LUs associated with user application programs	X	X	
Host SSCP	X	X	
ACF/NCP (PU Type 2)	X	X	X

Figure 2-14. Resources that Can Have Sessions Traced

Start or Stop Collection of Session Awareness Data: The user can start or stop the collection of session awareness data. When the collection of session awareness data is started, NLDM receives information about active sessions as well as about sessions subsequently started. NLDM collects session awareness data from each ACF/VTAM (Version 2 Release 2) that owns a session partner or that acts as a gateway ACF/VTAM in setting up a cross-network session.

The initiation of session awareness notifications from ACF/VTAM may begin upon initialization of NLDM or be deferred until the ENABLE command is issued. With this enhancement NLDM collects session awareness data for existing as well as subsequently started sessions. The user may stop the collection of session awareness data by use of the DISABLE command.

Activate or Deactivate Session Traces: NLDM begins collecting session trace data only after a session trace is started. Session traces may be started during or after NLDM initialization. Session traces are started at NLDM initialization for resources specified in the NCCF parameter definition data set; resources that can be specified in that data set are all LUs, all SSCPs, or both.

Once NLDM is initialized and enabled, the user may start or stop session traces for specific network resources, or all network resources. In a multiple-domain network, a user in one domain may start a session trace for a resource in another domain if NLDM has been initialized in that domain. Session trace data is collected for a session involving two resources in the same domain when a session trace is started for either session partner. In a multiple-domain network, all session trace data for a cross-domain session is collected only when session traces are started in both domains.

Activation of response time data collection: At initialization of NLDM, the customer defines performance classes, each with its own:

- Response time ranges for measuring response time
- Response time definition
- Response time objective (such as 80% of transactions should take under 5 seconds).

After defining performance classes, the customer maps sessions into performance classes.

Based on the initialization information, the RTM feature of the 3274 begins to measure response times and stores the information for collection by NLDM. The user collects response time data from the 3274 by either invoking an explicit collect command, or by defining an NCCF command list.

Display Session Data: The user can display the collected session data using a set of panels organized in a hierarchy. If the user wants to display information about an active session, NLDM retrieves the session data from main storage. If the user wants to display information about a previously active session, NLDM gets the session data from the VSAM data base.

NLDM provides cross-domain support to allow you to view session data where one session partner resides in another domain. You may also view session data where both partners reside in a different domain from the one containing your terminal. A user can view data involving a session partner in another network, although he may be denied access to specific session configuration information about cross-network sessions.

Session awareness data is displayed in the following ways:

- SNA resource lists
- A list of the most recent sessions for a resource
- Domain lists
- Session configuration
- Explicit route configuration
- Transmission group information.

Session trace data is displayed in the following ways:

- Session activation parameters
- Access method PIU data
- NCP data.

Response time data is displayed in the following ways:

- Response time summaries
- Response time trends
- Response time for a session by collection period.

Test Session Connectivity: The user can test the session connectivity for any active session. NLDM requests the access method to issue an ER test to check the physical path for a particular session. For a cross-network session, NLDM requests the adjacent NLDM to request an ER test in its network. If several networks are involved, each NLDM requests the NLDM in the adjacent network to request its access method to issue an ER test for that network. In an interconnected network environment this would be very difficult to accomplish without NLDM. The ACF/VTAM route test can test the route into an adjacent network. If more than two networks are involved, ACF/VTAM route testing is limited. NLDM allows the entire route to be tested with only one command.

As a result of initiating a session connectivity test an appropriate NLDM message will be issued indicating the results. If the test fails, the failing network, domain, and subarea are identified.

Display NLDM Help Information: The NLDM user can display a set of panels describing NLDM commands. The user may also display what session traces are active and what the keep settings currently are. The keep settings are the user-specified number of PIUs kept while tracing, and the number of historical sessions kept on the VSAM data base.

Display the Port Address of a Station: The user can issue a command to verify the NCP line port address associated with a station attached to an NCP within the domain of the NLDM.

Display and Changing Program Function Key Settings: The NLDM user can display or change the program function (PF) key settings for NLDM commands.

Session Awareness Data

NLDM collects session awareness data whenever a session begins or ends and when NLDM is initialized and enabled. Session awareness data includes information from the access method about:

- Session activation status
- Session type
- Session partners
- Session start and end times

It also includes information from the ACF/NCP about session and route configuration for LU-LU sessions, SSCP-LU sessions, SSCP-PU sessions, and SSCP-SSCP sessions.

Session awareness data is displayed as:

- SNA resource lists
- Lists of the most recent sessions for specific resources
- Domain lists
- Session configuration diagrams
- Explicit route configuration diagrams
- Transmission group information.

Resource Lists: The user can display lists of all SNA resources (LUs, PUs, and SSCPs) known to NLDM. The user can display lists showing the session partner names of all secondary logical units (SLUs), all primary logical units (PLUs), all LUs, all PUs, or all SSCPs. A resource list indicates which resources are involved in active sessions.

Most Recent Sessions List: The user can display a list of the most recent sessions in which a specific resource was a partner. Currently active sessions appear first on the list, then in top down order, the most recent sessions first. The information displayed includes the name, type, and domain of each session partner. Cross-network sessions are also identified, in which case the network ID will be provided. The session activation and deactivation times are shown for sessions that have ended; the session activation time is shown for an active session.

Domain Lists: The user can display a list of the domains known to NLDM. The list provides the name (CDRM) as known in this domain, the name of the ACF/VTAM associated with the named domain and the name that ACF/VTAM is known by in the domain of the current NLDM. It also contains information about the NLDM-to-NLDM session between the NLDM in the current domain and the NLDM in each domain listed, such as the status of the session, the time the session was activated, and the time the session was last used.

Session Configuration: The user can display the physical configuration of the parts of the network in which the primary and secondary ends of a specific session are located. The configuration includes the network names of the resources shown. All NLDM panels use real names. However the configuration panels will also provide the alias names and addresses when they apply. Also displayed are the names and addresses of the session partners and the names of the domains in which the session partners are located. To see the entire configuration for cross-network sessions, a user displays two or more panels; each panel identifies one of the networks and shows the part of the path in that network. NLDM provides a security function that can prevent other nonadjacent NLDMs from viewing their configuration data.

Explicit Route Configuration: The user can display the configuration of an explicit route, including information about subareas (intermediate network nodes) in the path of the explicit route such as names and addresses of the subareas.

Transmission Group Information: The user can display detailed data about a specific transmission group connecting two subareas in the path of an explicit route. The information shown includes the addresses of the two subareas, the number of the transmission group connecting the subareas, and the names of the ACF/VTAMs.

Session Trace Data

A session trace data is collected by NLDM whenever a session trace is started. Session trace data consists of session activation parameters, access method PIU data, and ACF/NCP data.

Session Activation Parameters: The user can display the parameters used for session activation if a trace is started for a session before the session is activated and if the session is successfully activated. Session activation parameters are those parameters included in the SNA command used to activate the session (Bind Session, Activate Physical Unit, Activate Logical Unit, or Activate CDRM). The session activation parameters can be displayed in either hexadecimal or text representation.

Access Method PIU Data: The user can display access method PIU data for all sessions for which NLDM collects session data. PIU data includes the transmission header (TH), the request/response header (RH), and the first 11 bytes of the request unit (RU). PIU data may be displayed in either hexadecimal or text representation.

NCP Data: The user can display ACF/NCP data for sessions involving ACF/NCP-attached resources. NCP data consists of selected fields from ACF/NCP control blocks that relate to the specific resource involved in the session. Except for SSCP-LU sessions and SSCP-PU session involving an ACF/NCP, NCP data includes the last two inbound and last two outbound PIU sequence numbers.

Response Time Data

Response time can be measured only by 3274s that have the Response Time Monitor feature. The measured response times are accumulated by the 3274s into ranges of time that were previously specified when the customer defined the performance classes (each with its response time definitions and response time objectives). The customer can specify which sessions are to be associated with which performance class.

NLDM can collect, via command, the response time data from the 3274s. If response time objectives are specified, graphics (optionally in color) are used in the displays to show how the response times compare to the specified objective. The customer can also specify that response time and configuration data be written to the SMF log as the response time data is collected, allowing other programs to process it.

Response time data is displayed as:

- Response time summaries
- Response time trends
- Response time for a session by collection period.

Response Time Summaries: The user can display a graph for a specified terminal LU and period of time, showing the percentage of transactions that fall into each response time range. If an objective has been specified, the display will show, numerically and graphically, how the actual response times compare to the objective.

Response Time Trends: The user can display a graph for a specific terminal LU showing the percentage of transactions with response times under a specified maximum for each data collection period. If the specified maximum time is the same as the time specified in the performance class objective, the display will show graphically how the actual response times compare with the objective for each collection period. Thus, the response times experienced by a user can be viewed in comparison to the performance objective over a period of time.

Response Time for a Session by Collection Period: The user can display a graph for each collection period of a specified session, showing the percentage of transactions that fall into each response time range. If an objective has been specified, the display will show, numerically and graphically, how the actual response times compare to the objective.

Chapter 3. Requirements and Compatibilities

This chapter describes, for each program product, its requirements in the following categories:

- Real storage
- Hardware
- Programming requirements

This chapter also discusses compatibilities between the current release of each program product and other IBM program products.

For a list of terminals supported by each program product, see Appendix A.

ACF/VTAM

Storage Requirements

Requirements for host processor storage and for disk storage for ACF/VTAM data sets can be calculated by using *Network Program Products Planning*, when available.

Hardware Requirements

ACF/VTAM runs in a virtual storage environment in any IBM host processor that supports one of the operating systems as specified in the "Programming Requirements" section below.

The host processor instruction set must include the Compare and Swap and the Compare Double and Swap instructions.

For remote communication, ACF/VTAM can use a 3705-I, 3705-II, 3705-80, or 3725 Communication Controller with the appropriate level of ACF/NCP.

See Appendix A for a list of supported terminals.

Programming Requirements

ACF/VTAM Version 2 Release 2 needs one of the following operating systems:

OS/VS2 (MVS) Release 3.8, including SP 1.2 and SP 1.3

MVS/XA SP 2.1

ACF/VTAM will also operate with subsequent releases or modifications of these operating systems, unless otherwise stated in the announcement documentation for these releases or modifications. ACF/VTAM does not support prior releases of these operating systems.

The Time Sharing Option of ACF/VTAM (TSO/VTAM) operates under MVS.

The use of certain ACF/VTAM facilities (such as delayed configuration restart :delayed configuration restart requirements or the ACF/VTAM Encrypt/Decrypt Feature) requires the current level of Virtual Storage Access Method (VSAM).

The optional feature, ACF/VTAM Encrypt/Decrypt Feature, requires the Programmed Cryptographic Facility program product, and operates under MVS.

The following functions are supported when ACF/VTAM Version 2 Release 2 operates with ACF/NCP Version 1 Release 3:

- Cross-domain communication for channel-attached devices
- Simultaneous multiple sessions between application programs
- Negotiable session parameters between application programs
- Enhanced operator control of session termination
- LU connection test
- Dynamic display of NCP storage
- Dynamic dump of NCP storage
- Enhanced link-level 2 test
- Intensive mode recording of NCP SDLC link errors
- Dynamic reconfiguration of nonswitched SNA devices
- Simplified cross-domain resource definition
- Multiple routes between subareas
- Multiple SDLC links (transmission groups between adjacent NCPs)
- Extended interconnection of communication controllers
- Multiple transmission priority levels
- Enhanced notification of session outages
- Enhanced network flow control
- Route verification and error notification facilities
- Enhanced recovery capabilities.

The following functions are supported only when ACF/VTAM Version 2 Release 2 operates with ACF/NCP Version 2 or 3:

- Generalized PIU trace (GPT)
- Notification of session establishment and termination (through NLDM)

- Continuous trace of PIU data passing between selected network resources (through NLDM).

The following functions are supported only when ACF/VTAM Version 2 Release 2 operates with ACF/NCP Version 3:

- SNA network interconnection
- Channel-attachment ACF/NCPs
- Enhanced configuration and session awareness for data for NLDM Release 2
- Forced deactivation of an NCP link.

The following functions are supported only when ACF/VTAM Version 2 Release 2 operates with an ACF/NCP Version 2 or 3 for the 3725:

- CSP and MOSS dumps
- SIT trace

Compatibility

ACF/NCP

ACF/VTAM Version 2 Release 2 operates with ACF/NCP Version 3, ACF/NCP Version 2, and ACF/NCP Version 1 Release 3.

Some of the functions of ACF/VTAM Version 2 require the appropriate release of ACF/NCP, as indicated in the previous section of this chapter.

ACF/VTAM Version 2 Release 2 supports only record-mode sessions. The Network Terminal Option program product (or a similar user-written program) can be used to support selected non-SNA devices in record-mode sessions.

ACF/VTAM Application Programs

As each new release of ACF/VTAM was developed, new application program facilities were added, obsolete facilities were deleted, and errors were corrected. Internal changes were also made to improve performance, reliability, availability, and serviceability. In this activity, the goal was to allow application programs that ran on a prior release of ACF/VTAM or on VTAM Level 2 to run on the new release of ACF/VTAM without modification or reassembly of the application program. However, in certain cases an application program must be modified.

The table in Figure 3-1 lists the factors to consider when moving an application program from a prior release of ACF/VTAM or VTAM Level 2 to ACF/VTAM Version 2 Release 2. Each factor is discussed in detail in *ACF/VTAM Programming*.

You may want to change a current program if it depends on the way a particular release of ACF/VTAM or VTAM Level 2 operates, such as the sequence of steps when processing an operator command or synchronous SIMLOGON macro instruction. You might also like to change a program to make use of the ACF/VTAM's networking capabilities.

Programming Factors To Be Considered:	When Migrating to ACF/VTAM Version 2 Release 2 From: [1]				
	VTAM Level 2	ACF/VTAM Version 1 Release 1	ACF/VTAME or ACF/VTAM Version 1 Release 2	ACF/VTAM Version 1 Release 3	ACF/VTAM Version 2 Release 1
Sequence Number Dependencies for LU Type 0 3270 Terminals	X	X	X	X	
Logon Mode Names for Non-SNA 3270 Terminals	X				
Search of Default Logon Mode Table	X				
Bracket Protocols for Non-SNA 3270 Terminals	X				
Reporting Segmenting Errors	X				
Removal of Basic-Mode Support	X	X			
LOSTERM Exit Reason Codes	X	X			
Reporting Failures When NIB USERFLD IS Specified	X	X			
Parallel Sessions and the Use of NIBCID	X	X			
CLEAR Not Sent Before UNBIND	X	X			
SETLOGON OPTCD=QUIESCE	X	X			
SIMLOGON OPTCD=CONALL	X	X			
COS Name and Logon Mode Name	X	X	X		
Increase of ACB Size	X	X	X	X	
Application Program Minor Node Name in BIND	X	X	X	X	

[1] You should also consider functions in this table that are available in the release of ACF/VTAM you are migrating from and you are intending to use for the first time with Version 2 Release 2. For example, you might be migrating your system from ACF/VTAM Version 1 Release 2 and also adding parallel session capability to a current application program.

Figure 3-1. Factors for Moving Programs from Prior Releases of ACF/VTAM or VTAM Level 2

Programmed operator application programs can run unchanged, provided they do not depend on the structure or content of the ACF/VTAM message table ISTCFCMM. That is, no change is required for a programmed operator if it depends only on the documented programmed operator interface and on the content, structure, and meaning of the messages received through this interface. However, any programmed operator that depends on the structure or content of ISTCFCMM might need changes.

BTAM Application Programs

Existing application programs that use BTAM macros directly must be rewritten to operate with ACF/VTAM Version 2 Release 2. BTAM application programs that use an IBM application subsystem such as CICS/VS or IMS should require few changes, if any, to run on ACF/VTAM Version 2 Release 2. Considerations for converting from BTAM to ACF/VTAM are discussed in the *Network Program Products Planning*.

Related IBM Programs

If unformatted system services (USS) facilities are used to change ACF/VTAM messages, any NCCF customization code may need to be modified to ensure the correct routing of messages. Refer to *Network Program Products Planning* for more information. Related IBM programs such as CICS/VS, IMS/VS,

POWER/VS, JES1/RES, JES2/RJE, TSO, VSPC, and SSS that are compatible with VTAM Level 2 or ACF/VTAM Version 1 are compatible with ACF/VTAM Version 2 Release 2 on the appropriate operating system release. Recompilation of these programs is not required.

TCAM through VTAM is not provided with ACF/VTAM. However, ACF/TCAM can exist in the same host processor as ACF/VTAM.

Cross-Domain Communication

ACF/VTAM Version 2 Release 2 can support cross-domain communication for the following types of configurations:

- Multiple host processor configurations, operating with any combination of MVS or VSE operating systems, where each host processor has a network controlled by ACF/VTAM Version 2 Release 2 and ACF/NCP. Optionally, some of the host processors may have networks controlled by the following currently supported access methods:
  - ACF/VTAM Version 1 Release 3 with its Multisystem Networking Facility or ACF/VTAM Version 2 Release 1, and ACF/NCP
  - ACF/TCAM Version 2 Release 3 or 4 with its Multisystem Networking Facility and ACF/NCP
  - ACF/VTAME.
- A network controlled by a single host processor with two access methods, ACF/VTAM Version 2 Release 2 and ACF/TCAM Version 2 Release 3 or 4 with its Multisystem Networking Facility, in conjunction with ACF/NCP.
- Combinations of the previous types of configurations.

In a multiple-domain network with both ACF/VTAM and ACF/TCAM, ACF/VTAM's access to device characteristics of the terminals controlled by ACF/TCAM is limited to those indicators defined and maintained by ACF/TCAM. In particular, ACF/VTAM cannot determine and, therefore, cannot provide to the application program the physical device address (used in the copy function) of an IBM 3271 Model 11 or 12 or any compatible device controlled by ACF/TCAM.

Two host processors can be attached through a channel-to-channel connection provided that both contain ACF/VTAM Version 2 and an OS/VS operating system.

In MVS only, the ACF/VTAM Encrypt/Decrypt Feature in one domain operates with an ACF/VTAM Encrypt/Decrypt Feature or ACF/TCAM Version 2 (or subsequent releases) in another domain to establish cross-domain cryptographic sessions. (Encryption/decryption is included in ACF/TCAM Version 2). The Encrypt/Decrypt Feature does not operate with VTAM, TCAM, ACF/VTAME, nor with ACF/TCAM Version 1.

Initially, host processor locations that are to participate in a multiple-domain network can install ACF/VTAM with single-domain networks, and the domains can be connected later with cross-domain links. This permits an existing domain to continue to operate while the multiple-domain network is being developed. It

should be noted that once a feature such as the optional Encrypt/Decrypt Feature has been installed, it is difficult to remove. Removing a feature requires regenerating the system and reapplying all of the features you wish to retain.

Cross-Network Communication

ACF/VTAM Version 2 Release 2 can support cross-network communication, as long as the ACF/NCP with which it provides a gateway between networks is Version 3. It can also communicate with an ACF/VTAME. The configuration within each network can be any of those described above under "Cross-Domain Communication."

Cross-network encryption and decryption is available with the use of the Encrypt/Decrypt Feature at the gateway ACF/VTAMs, as well as at the hosts owning the session partners.

The complexity of the migration of a network to SNA network interconnection depends on the configuration chosen and the methods of identifying cross-network resources. See the "Configuration Design" section under "Interconnected Networks" in Chapter 1 for a short review of the factors involved.

Conversion

ACF/VTAM Application Programs

User-written application programs that use the macro language and control block record-mode interface of VTAM Level 2, ACF/VTAM Version 1, or ACF/VTAME will continue to operate on the same operating system with ACF/VTAM Version 2. This can be done without changes (except those listed in Figure 3-1) and without recompilation, provided that these programs do not depend on the internal processing characteristics of the access methods. ACF/VTAM application programs generally will not need to be changed to operate with the Encrypt/Decrypt Feature. However, several SNA sense codes that deal with unrecoverable errors associated with the Encrypt/Decrypt Feature have been introduced; existing application programs may need to be changed to handle these codes properly. For more information about converting to ACF/VTAM Version 2 Release 2, see *Network Program Products Planning* and *ACF/VTAM Programming.*

BTAM Application Programs

User-written application programs that use BTAM macros directly must be rewritten to operate with ACF/VTAM Version 2 Release 2. You may redesign these programs to use an IBM application subsystem such as CICS/VS or IMS or recode them to use ACF/VTAM macros directly. For more information about designing application programs to use an IBM application subsystem, see the appropriate subsystem programming manual. For information about coding ACF/VTAM application programs, see *ACF/VTAM Programming.* For a comparison of ACF/VTAM and BTAM macro instructions, see the *Network Program Products Planning* manual.

Converting BTAM application programs that already use an IBM application subsystem should involve few changes in most cases. Refer to the appropriate subsystem programming manual for details.

Data Security, Auditability, and Control

ACF/VTAM enables the installation to establish and maintain the integrity of the data communication network. The installation can control sessions between application programs and terminals. The installation can also control access to data and the use of data within the network. ACF/VTAM provides a confidential text capability. The data on sessions defined by the user to contain confidential text is not included in buffer traces. Moreover, buffers containing confidential text are cleared before being returned to the buffer pool. User management is responsible for the selection, application, adequacy, and implementation of these features and for the appropriate application and administrative control.

ACF/NCP and ACF/SSP

Storage Requirements

ACF/NCP requirements for communication controller storage and processor disk storage on which the ACF/NCP can be installed for loading can be calculated using *Network Program Products Planning*, when available.

Hardware Requirements

ACF/NCP Version 3 requires one of the following communication controllers:

- A 3705-II Communications Controller
- A 3705-80 Communications Controller
- A 3725 Communication Controller

ACF/SSP Version 2 Release 2 can operate in any processor that supports ACF/VTAM.

Programming Requirements

ACF/SSP Version 2 Release 2 requires one of the following operating systems in the host processor:

- OS/VS2 (MVS) Release 3.8 (including SP 1.2 and SP 1.3)
- MVS/XA SP 2.1.

The full range of ACF/NCP Version 3 functions are available with the following programs:

- ACF/SSP Version 2 Release 2
- ACF/VTAM Version 2 Release 2

If you are migrating from a PEP environment, you can use EP/3705 or EP/3725 with ACF/NCP Version 3 to support your BSC and start-stop terminals.

Compatibilities

compatibility

ACF/NCP Version 3 can also communicate with the programs listed below. However, the full range of Version 3 functions may not be available when operating with these releases of program products.

- Other ACF/NCPs
  - ACF/NCP Version 1 Release 2.1
  - ACF/NCP Version 1 Release 3
  - ACF/NCP Version 2 (for the 3705)
  - ACF/NCP Version 2 (for the 3725)
- Access methods
  - ACF/VTAM Version 1 Release 3 (OS/VS2 (MVS) only)
  - ACF/VTAM Version 2 Release 1 (OS/VS2 (MVS) and MVS/XA in compatibility mode only)
  - ACF/TCAM Version 2 Release 4
- NTO Release 2
- NRF
- X.25 Network Control Program Packet Switching Interface
- EP (Emulation Program)
  - For the 3705 (EP/3705)
  - For the 3725 (EP/3725)
- Non-SNA Interconnection (NSI) Release 1

NCCF

Storage Requirements

Requirements for host processor storage, including the Terminal Access Facility and the alias name translation facility, can be calculated using *Network Program Products Planning*, when available.

Hardware Requirements

NCCF runs in a virtual storage environment in any IBM host processor that satisfies the requirements of ACF/VTAM or ACF/TCAM.

Programming Requirements

NCCF runs with any operating system that satisfies the requirements of the level of ACF/VTAM or ACF/TCAM it is operating with. However, some functions are not available under certain access method releases. Figure 3-2 lists these functions.

Operator control sessions are not available for certain subsystems with the Terminal Access Facility. Figure 3-3 lists this support.

Access Method	Version 1 NCCF Functions	Version 2 NCCF Enhancements
ACF/VTAM Version 1 Release 3	All	All except alias name translation
ACF/VTAM Version 2 Release 1	All	All except alias name translation
ACF/VTAM Version 2 Release 2	All	All
ACF/TCAM Version 2 Release 4	All except span of control	All except alias name translation

Figure 3-2. NCCF Functions Available with ACF/VTAM and ACF/TCAM

Access Method	Subsystem	DPPX/DPCX	Session Type: Operator Control	Session Type: Full-Screen
ACF/VTAM	CICS/VS		X	X
	IMS/VS		X	X
	HCF		X	X
				X
	TSO			X
	Remote NCCF			X
ACF/TCAM Version 2 Release 4	CICS/VS		X	X
	IMS/VS		X	X
	HCF	DPPX	X	X
		DPCX		X

Figure 3-3. Subsystem Sessions Supported by the Terminal Access Facility

Compatibilities

NCCF Version 1 commands are compatible with NCCF Version 2.

Command processors and exit routines you may have coded to run with NCCF Version 1 are source-code compatible with NCCF Version 2. However, the code must be reassembled using the Version 2 NCCF macro library.

NCCF Version 2 will operate with NCCF Version 1 definition decks, providing equivalent function. NCCF Version 2 functions that require additional definition will not operate until defined.

Cross-domain communication is supported between NCCF Version 1 Release 2 and NCCF Version 2.

NLDM

Storage Requirements

The NLDM virtual and disk storage requirements depend on the number and kinds of sessions traces, and the amount of session and response time data kept for each session traced. See *Network Program Products Planning*, when available, for storage estimates.

Hardware Requirements

NLDM may be run in any host processor supported by NCCF. An NLDM user may access the NLDM program product through any terminal supported by NCCF.

NLDM will monitor the response time of any response time monitor supported keyboard/display devices attached to the following SNA control units that support the RTM feature:

- 3274 Models 31A and 41A (local SNA)
- 3274 Models 31C, 41C, 51C, and 61C (SDLC/SNA only)

These control units must have the RTM feature installed and be running with the "C" or "D" microcode configuration. The RTM feature of the 3274 does not provide a mechanism for host data retrieval for non-SNA devices.

Programming Requirements

NLDM Release 2 requires NCCF Version 2.

To obtain the new functions, NLDM Release 2 also requires the following programs:

- ACF/VTAM Version 2 Release 2
- ACF/NCP Version 3

NLDM runs as an application program under NCCF. Refer to "NCCF" in this chapter for additional dependencies and prerequisites.

The response time data function of NLDM R2 requires:

- MVS/SP Version 1 for System/370
- MVS/SP Version 2 for System 370/XA (Extended Architecture) processors in 24 bit mode.

The SMF logging feature of NLDM R2 requires:

- MVS/SP Version 1.3.3 or higher for System/370 with an SMF SPE
- MVS/SP Version 2.1.1 or higher for System 370/XA with an SMF SPE.

Compatibilities

Although NLDM Release 2 can run in a single-domain network with the programs listed below, the new functions are not available.

- ACF/VTAM Version 1 Release 3 (MVS only)
- ACF/VTAM Version 2 Release 1 (MVS only)
- ACF/TCAM Version 2 Release 4
- ACF/NCP Version 2 Release 1

In a multiple-domain or SNA network interconnection environment, NLDM Release 2 cannot communicate with NLDM Release 1. An NLDM Release 2 cannot communicate with another NLDM Release 2, if either one is running under ACF/VTAM Version 1 Release 3 or any release of ACF/TCAM. When NLDM Release 2 is operating under ACF/TCAM, it only provides the functions available under NLDM Release 1.

Appendix A. Supported Products

This appendix lists the terminals and programs supported by ACF/VTAM Version 2 Release 2, TSO/VTAM, ACF/NCP Version 3, NCCF Version 2, and NLDM Release 2.

Products Supported by ACF/VTAM Version 2 Release 2

Figure A-1 lists the terminals supported by ACF/VTAM Version 2 Release 2. These terminals are channel-attached or link-attached. Channel-attached terminals are attached directly to the host processor. Link-attached terminals are attached on SDLC links or, for the BSC 3270, on BSC links, to either a channel-attached or link-attached communication controller. If the Network Terminal Option program product is installed in a communication controller, selected non-SNA devices can be attached over BSC or start-stop lines. These products are grouped as:

- Channel-attached SNA terminals
- SDLC terminal products
- Channel-attached non-SNA terminals
- BSC terminals
- Start-stop terminals.

The figure also shows whether a terminal can be used on switched or nonswitched lines (or both) and the PU type by which the terminal or terminal subsystem is defined to ACF/VTAM and the ACF/NCP.

Terminals that are functionally equivalent to those specifically supported may also function satisfactorily. The user is responsible for establishing equivalency.

Where the figure states that a terminal is "supported as" another terminal, it means that these terminals are defined to ACF/VTAM and use ACF/NCP facilities in the same manner. This does not mean that the terminals have similar processing capabilities or physical characteristics. For example, a 3274 Model 1B is supported as a channel-attached 3272 cluster controller. However, the data exchanged between an application program and the 3274 and the disposition of the data after it reaches the 3274 are not necessarily the same as for a 3272.

Figure A-2 lists the terminals supported by TSO/VTAM.

Network Terminal Option (NTO)

ACF/VTAM and ACF/NCP support some non-SNA terminals, other than the channel-attached and link-attached BSC 3270s, through the Network Terminal Option program product. NTO, which resides in the ACF/NCP, allows these terminals to be attached to the network as ACF/NCP logical units. Through an interface with NTO, ACF/VTAM supports them as SNA 3767 Communication Terminals. For information about NTO and the terminals it supports, see *Network Terminal Option General Information*, GC27-0429.

Device or Subsystem Name	Controlling Device-Model	PU Type	Switched	Non-Switched	Notes
Channel-Attached SNA					
3270 Information Display System	3274-1A,21A,31A,41A	2			
3790 Communication System	3791	2			
3730 Distributed Office Communication System	3791	2			
Link-Attached (SDLC) SNA					
3232 Keyboard Printer Terminal	3232-1	2	X	X	
3270 Information Display System	3271-11,12	1		X	Supported as a PU Type 1 3270
	3274-1C,21C,31C,41C	2		X	
	3274-51C,61C	2	X	X	
	3274-52C	2	X	X	
	3275-11,12	1		X	Supported as a PU Type 1 3270
	3276-1,2,3,4	2		X	With SDLC/BSC switch set to SDLC
	3276-11,12,13,14	2	X	X	Can support cryptographic sessions
3600 Finance Communication System	3601,3602	2	X	X	
	3614,3624	2		X	
3630 Plant Communication System	3631,3632	2		X	
3650 Retail Store System	3651-A50,B50	2	X	X	
3660 Supermarket System	3651-A60,B60	2	X		
	3661	2	X		
3680 Programmable Store System	3684	2	X	X	
3694 Document Processor	3694-1A,1B,1C,1D, 2A,2B,2C,2D	2	X	X	
3730 Distributed Office Communication System	3791	2	X	X	
3767 Communication Terminal	3767	1	X	X	Can support cryptographic sessions
3770 Data Communication System	3771,3773	2	X	X	
	3774,3775	2	X	X	
	3776,3777	2	X	X	
3790 Communication System	3791	2	X	X	
4700 Finance Communication System	4701	2	X	X	
5280 Distributed Data System	5285	2	X	X	
5520 Administrative System	5525	2	X	X	
5937 Industrial Terminal	5937-S1	1		X	Supported as a PU Type 1 3270
6580 Displaywriter	6580-A08,B08	2	X	X	
6670 Information Distributor	6670	1	X	X	
7428 Terminal Interface Unit	7426-2	2	X	X	Supported as a 3276-12 with up to four 3278 displays and or 3287 printers
8100 Information System (DPCX)	8130,8140	2	X	X	
8100 Information System (DPPX)	8130,8140	2	X	X	
8775 Display Terminal	8775-11,12	2	X	X	
8815 Scanmaster I	8815-1,3,4	2	X	X	
IBM Personal Computer	5150-14,64,74	2	X	X	Supported as a 3278-2 attached to a 3274-51C
IBM Personal Computer XT	5160-87	2	X	X	Supported as a 3278-2 attached to a 3274-51C

Figure A-1 (Part 1 of 2). Terminal Products Supported by ACF/VTAM Version 2 Release 2

Device or Subsystem Name	Controlling Device-Model	PU Type	Switched	Non-Switched	Notes
Link-Attached (SDLC) SNA (con't)					
Series/1	Series/1	2	X	X	
System/32	System/32	2	X	X	
System/34	System/34	2	X	X	
System/38	System/38	2	X	X	
Channel-Attached Non-SNA					
3036 Console	3036				Supported as a 3272-1,2
3270 Information Display System	3272-1,2				
	3274-1B,1D,21B, 21D,31D,41D				Supported as a 3272-1,2
Link-Attached (BSC) Non-SNA					
3270 Information Display System	3271-1,2			X	
	3274-1C,21C,31C			X	Supported as a 3271-1,2
	41C,51C,61C			X	Supported as a 3271-1,2
	3275-1,2			X	Supported as a 3271-1,2
	3276-1,2,3,4			X	Supported as a 3271-1,2
3780 Data Communications Terminal	3780	1		X	Supported through the Network Terminal Option Program Product
5275 Direct Numerical Control Station	5275			X	Supported as a 3276-1,2
5937 Industrial Terminal	5937-S1			X	Supported as a 3271-1,2
8100 Information System (DPPX)	8130,8140			X	Supported as a 3271-1,2
IBM Personal Computer	5150-14,64,74			X	Supported as a 3271-1,2
IBM Personal Computer XT	5160-87			X	Supported as a 3271-1,2
Link-Attached (Start-Stop) Non-SNA					
2740 Communications Terminal	2740-1	1	X	X	Start-stop non-SNA terminals are supported through the Network Terminal Option Program Product. See the Network Terminal Option General Information manual for details.
2741 Communications Terminal	2741	1	X	X	
3767 Communications Terminal	3767-1,2	1	X	X	
World Trade Teletypwriter Terminal (WTTY)	WTTY	1		X	
Western Union Teletypwriter Exchange Services Terminal	TWX Model 33/35	1	X	X	
3101 Display Terminal	3101	1	X	X	Supported as a TWX Model 33/35

Figure A-1 (Part 2 of 2). Terminal Products Supported by ACF/VTAM Version 2 Release 2

Device or Subsystem Name	Controlling Device-Model	Terminal-Model	LU Type
Channel-Attached SNA			
3270 Information Display System	3274-1A, 21A, 31A, 41A	3178	2
		3277-1, 2	2
		3278-1, 2, 3, 4, 5	2
		3279-2A, 2B, 3A, 3B	2
		3290	2
3790 Communication System	3791-1A, 1B, 1C, 2A, 2B	3277-1, 2	2
	3276-12	3178	2
		3278-2	2
Link-Attached (SDLC) SNA			
3101 Display Station	7426-2	3101-10, 13, 20, 23	2
3232 Keyboard Printer Terminal	3232-1		2
3270 Information Display System	3271-11, 12	3277-1, 2	0
	3274-1C, 21C, 31C, 41C, 51C, 61C	3178	2
		3277-1, 2	2
		3278-1, 2, 3, 4, 5	2
		3279-1A, 1B, 2A, 2B	2
		3290	2
	3275-11, 12		0
	3276-11, 12, 13, 14	3178	2
		3278-1, 2, 3, 4	2
		3279-2A, 2B, 3A, 3B	2
3767 Communication Terminal	3767-1, 2, 3		1
3770 Data Communication System	3771-1, 2, 3		1
	3773-1, 2, 3		1
	3774-1, 2		1
	3775-1		1
3790 Communication System	3791-1A, 1B, 1C, 2A, 2B	3277-1, 2	2
6580 Displaywriter			2
8130 Processor (DPCX)	8130-A21, A22, A23, A24	3277-1, 2	2
		8775-1, 2	2
	3276-11, 12, 13, 14	3178	2
		3278-1, 2, 3, 4	2
		3279-2A, 2B, 3A, 3B	2
8140 Processor (DPCX)	8140-A31, A32, A33, A34, A41, A42, A43, A44, A51, A52, A53, A54	3277-1, 2	2
		8775-1, 2	2
	3276-11, 12, 13, 14	3178	2
		3278-1, 2, 3, 4	2
		3279-2A, 2B, 3A, 3B	2
8775 Display Terminal	8775-11, 12		2
IBM Personal Computer	5150-14, 64, 74		2
IBM Personal Computer XT	5160-87		2

Figure A-2 (Part 1 of 2). Terminals Supported by TSO/VTAM

Device or Subsystem Name	Controlling Device-Model	Terminal-Model	LU Type
Channel-Attached Non-SNA			
3270 Information Display System	3272-1, 2	3277-1, 2	0
	3274-1B, 1D, 21B, 21D, 31D, 41D	3178	0
		3277-1, 2	0
		3278-1, 2, 3, 4, 5	0
		3279-2A, 2B, 3A, 3B	0
		3290	0
Link-Attached Non-SNA (BSC)			
3270 Information Display System	3271-1, 2	3277-1, 2	0
	3274-1C, 21C, 31C, 41C, 51C, 61C	3178	0
		3277-1, 2	0
		3278-1, 2, 3, 4, 5	0
		3279-2A, 2B, 3A, 3B	0
		3290	0
	3275-1, 2		0
	3276-1, 2, 3, 4	3278-1, 2, 3, 4	0
		3279-1A, 1B, 2A, 2B	0
8130 Processor (DPPX)	8130-A21, A22, A23, A24	3277-1, 2	0
		8775-1, 2	0
	3276-11, 12, 13, 14	3178	0
		3278-1, 2, 3, 4, 5	0
		3279-2A, 2B, 3A, 3B	0
8140 Processor (DPPX)	8140-A31, A32, A33, A41, A42, A43, A44, A51, A52, A53, A54	3277-1, 2	0
		8775-1, 2	0
	3276-11, 12, 13, 14	3178	0
		3278-1, 2, 3, 4, 5	0
		3279-2A, 2B, 3A, 3B	0
IBM Personal Computer	5150-14, 64, 74		0
IBM Personal Computer XT	5160-87		0

The Network Terminal Option allows TSO/VTAM users to communicate with selected non-SNA devices that are not supported by TSO/VTAM in VTAM Level 2 and ACF/VTAM Version 1 Release 1. These non-SNA devices are the IBM 2741, IBM 3101, IBM 3767, WTTY, and TWX Model 33/35.

Figure A-2 (Part 2 of 2). Terminals Supported by TSO/VTAM

Communication Controllers Supported by ACF/VTAM Version 2 Release 2

ACF/VTAM and ACF/NCP support the following IBM communication controllers:

- 3705-II Communications Controller
- 3705-80 Communications Controller
- 3725 Communication Controller

Each communication controller must have a network control program (NCP) in network control mode either alone or with partitioned emulation programming

(PEP). The communication controllers can be link-attached through another communication controller or channel-attached. ACF/VTAM does not support the 2701, 2702, or 2703, or the emulation mode functions of the NCP, alone or with PEP.

Programs Supported by ACF/VTAM Version 2 Release 2

Figure A-3 lists the IBM program products supported by ACF/VTAM Version 2 Release 2. When a specific release of a related program or product appears in this figure, it is the earliest release supported by ACF/VTAM Version 2 Release 2. For more information about these programs, see your IBM marketing representative.

Type	Programs
DB/DC	CICS/VS IMS/VS
Job Entry	FTP JES2/RJE JES2/NJE JES3/RJP
Interactive	IIPS/IIAS IIS TSO,TSO/E VSPC VS/APL [1]
Device Support	BTP Version 4 DSLU DSX Release 2 GDDM [2] Host Command Facility Host Prep (8100/DPCX Support) MVS/IDWS Network Routing Facility NTO Release 2.1 Programmable Store System Host Support SSS Release 5 3600/4700 Finance Communication System Host Support
Systems and Communication Network Management	Information/System [3] NCCF Version 1 Release 2 and Version 2 NPDA Version 2 NLDM Releases 1 and 2 [5]
Distributed Data Processing	DISOSS/370 [4] MVS/OCCF [5]

Notes:

[1] Supported through CICS/VS, TSO/VTAM, or VSPC
[2] Supported through CICS/VS, IMS/VS, TSO/VTAM, or VSPC
[3] Supported through NCCF or TSO/VTAM
[4] Supported through CICS/VS or IMS/VS
[5] Supported through NCCF

Figure A-3. IBM Program Products Supported by ACF/VTAM Version 2 Release 2

Products Supported by ACF/NCP

The following lists show the data processing products that can be attached to a 3705 or 3725 with an ACF/NCP Version 3 installed.

SDLC Control Units and Display Stations

The following SDLC control units and display stations are supported:

IBM 3270 Information Display System
IBM 3275 Display Station
IBM 3277 Display Station attached to a 3271 Model 11 or 12
IBM 3278 Display Station attached to a 3274
IBM 3279 Color Display Station attached to a 3274
IBM 3284 Printer attached to a 3271 Model 11 or 12
IBM 3286 Printer attached to a 3271 Model 11 or 12
IBM 3287 Printer attached to a 3271
IBM 3290 Information Panel attached to a 3274 Model 31C or Model 51C
IBM 3600 Finance Communication System attached to a 3601 or 3602
IBM 3614 Consumer Transaction Facility
IBM 3650 Retail Store System attached to a 3651 Model A50 or B50
IBM 3660 Supermarket System attached to a 3651 Model A60 or B60 or a 3661
IBM 3730 Distributed Office Communications System supported as a 3790
IBM 3760 Dual Key Entry Station attached to a 3790
IBM 3767 Communication Terminal Model 1, 2, or 3
IBM 3770 Data Communications System made up of the following terminals:
- IBM 3771 Communication Terminal Model 1, 2, or 3
- IBM 3773 Communication Terminal Model 1, 2, P1, P2, or P3
- IBM 3774 Communication Terminal Model 1, 2, P1, or P2
- IBM 3775 Communication Terminal Model 1 or P1
- IBM 3776 Communication Terminal Model 1 or 2
- IBM 3777 Communication Terminal Model 1

IBM 3790 Communication System attached to a 3791
IBM 4700 Financial System
IBM 6670 Information Distributor
IBM 8100 Information System.

BSC Control Units and Display Stations

The following BSC control units and display stations are supported:

IBM 2770 Data Communications System attached to a 2772
IBM 2780 Data Transmission Terminal
IBM 2972 General Banking Terminal System (U.S.A. only) made up of the following terminals (not supported by a 3725 Communication Controller):
- IBM 2980 Teller Station Models 1 and 4
- IBM 2980 Administrative Station Model 2

IBM 3270 Information Display System (nonswitched lines only) made up of the following terminals:
- IBM 3275 Display Station
- IBM 3277 Display Station attached to a 3271 Model 1 or 2
- IBM 3278 Display Station attached to a 3274 Model 1C or 51C
- IBM 3284 Printer attached to a 3271 Model 1 or 2
- IBM 3286 Printer attached to a 3271 Model 1 or 2
- IBM 3287 Printer attached to a 3271 Model 1 or 2

IBM 3650 Retail Store System attached to a 3651 Model A50 or B50
IBM 3651 Retail Store System attached to a 3651 Model A60 or B60 or a 3661
IBM 3671 Shared Terminal Control Unit
IBM 3735 Programmable Buffered Terminal
IBM 3740 Data Entry System made up of the following terminals:
- IBM 3741 Data Station Model 2
- IBM 3741 Programmable Work Station Model 4
- IBM 3747 Data Converter

IBM 3770 Data Communications System supported as a 2772 and made up of the following terminals:
- IBM 3771 Communication Terminal Model 1, 2, or 3
- IBM 3773 Communication Terminal Model 1, 2, P1, P2, or P3
- IBM 3774 Communication Terminal Model 1, 2, P1, or P2
- IBM 3775 Communication Terminal Model 1 or P1
- IBM 3776 Communication Terminal Model 1 or 2
- IBM 3777 Communication Terminal Model 1

IBM 5275 Direct Numerical Control Station supported as a 3271 Model 1 or 2
IBM 5937 Industrial Terminal supported as a 3270 Model 1 or 2
IBM 6240 Mag Card Typewriter
IBM 6640 Document Printer
IBM 6670 Information Distributor
IBM 8100 Information System
Office System 6 (420, 430, 440, 442, 450, 452).

Start-Stop Stations

The following start-stop stations are supported:

IBM 1050 Data Communication System
IBM 2740 Communications Terminal Model 1 or 2
IBM 2741 Communications Terminal
IBM 3101 Display Terminal supported as a TWX 33/35
IBM 3767 Communications Terminal Models 1 and 2 supported as a 2740 Model 1 or 2 or a 2741
IBM 3767 Communications Terminal Model 3 supported as a 2740 Model 2
IBM 5100 Portable Computer supported as a 2741
IBM Communicating Magnetic Card Selectric Typewriter supported as a 2741 (switched line only)
Teletype 33/43
World Trade Teletypewriter Terminals that use CCITT No. 2 or No. 5 on nonswitched point-to-point lines
Terminals using AT&T 83B3 or WU 115A start-stop code over nonswitched telegraph lines using a multipoint discipline (device not supported by 3725 Communication Controllers)
Terminals using WU CPT-TWX (Model 33/35) start-stop code over switched lines.

Programs Supported by ACF/NCP

Programs supported by ACF/NCP are listed in Chapter 3: "Requirements and Compatibilities."

Products Supported by NCCF Version 2

Controllers

IBM 3271 Model 2 (BSC)
IBM 3271 Model 12 (SNA/SDLC remote)
IBM 3272 Model 2 (Local)
IBM 3274 Models 1A, 21A, 31A, and 41A (Local SNA)
IBM 3274 Models 1B, 1D, 21B, 21D, and 31D (Local non-SNA)
IBM 3274 Models 1C, 21C, 31C, 41C, 51C, and 61C (SNA/SDLC, BSC) (See note 1.)
IBM 3791, configuration support 9169 (See note 2.)
IBM 8100 with DPPX or DPCX (See note 2.)
IBM 5551 (with 3270 Emulation Program) (see note 3.)

Notes:

1. ASCII-8 is supported on 3274 controller level only for SNA/SDLC
2. 3270 data stream compatibility is required.
3. Kanji is not supported.

Controllers/Display Units

NCCF supports SNA display units as LU type 2 logical units.

The Katakana character set is supported as an NCCF option.

IBM 3275 Model 2 (BSC)
IBM 3275 Model 12 (SNA/SDLC)
IBM 3276 Models 2, 3, and 4 (BSC, SNA/SDLC) (See note.)
IBM 3276 Models 12, 13, and 14 (SNA/SDLC)

Note: For use with SNA/SDLC, you must have the SDLC/BSC switch feature.

Display Units

NCCF supports SNA display units as LU type 2 logical units.

The Katakana character set is supported as an NCCF option.

IBM 3277 Model 2
IBM 3278 Models 2, 3, 4, and 5 (See notes 1 and 2.)
IBM 3279 Models 2A, 2B, 2C, 3A, 3B, and 3C (See notes 2 and 3.)
IBM 3290 (See note 1.)
IBM 3178 (See note 1.)
IBM 8775 Models 1, 2, 11, and 12 (See notes 4 and 5.)
IBM 5555 (Attached to 5551) (See note 6.)

Notes:

1. The IBM 3278 Model 5, 3290, and 3178 are supported as a 3278 Model 2.

2. The Terminal Access Facility will log on to the application program as a 3278 Model 2. Thus, a 3278 Model 3 or 4 and a 3279 Model 3A or 3B will only format the Model 2 screen size when a full-screen session is being presented.

3. The IBM 3279 Models 2A and 2B are supported as 3278 Model 2. The IBM 3279 Models 3A and 3B are supported as 3278 Model 3. One color (monochrome) or base color mode is supported. Use of NCCF full-screen processing can support extended color and programmable symbol sets.

4. IBM 8775 Models 1, 2, 11, and 12 are supported as 3278 Models 2, 3, and 4.

5. 3270 data stream is required.

6. Kanji is not supported.

Printers

NCCF supports printers attached to SNA controllers as LU type 1 logical units. All other printers are supported as LU type 0 logical units.

The Katakana character set is supported as an NCCF option.

IBM 3284 Models 1 and 2 (See note 1.)
IBM 3286 Models 1 and 2 (See note 1.)
IBM 3287 Models 1, 1C, 2, 2C, 11, and 12 (See note 2.)
IBM 3288 Models 1, 2, 4
IBM 3289 Models 1, 2, 4
IBM 3262 Models 1, 11, 3, and 13
IBM 3230 Model 2
IBM 3268 Model 2
IBM 5553 (Attached to 5551) (See note 3.)

Notes:

1. When attached to an IBM 3274 Model 1C or 51C controller, this printer is supported in BSC mode only.

2. The IBM 3287 requires the SCS Support Feature 9660 when operating with controllers in SNA mode. The IBM 3287 Model 1C is supported as Model 1; the Model 2C is supported as a Model 2. Only one color (monochrome) is supported.

3. Kanji is not supported.

Access Methods

NCCF Version 2 supports the following access methods:

- ACF/VTAM Version 1 Release 3
- ACF/VTAM Version 2 Release 1
- ACF/VTAM Version 2 Release 2
- ACF/TCAM Version 2 Release 4.

CNM Products

NCCF is a program base upon which you can add other IBM program products or your own programs. This base provides functions collectively called communication network management (CNM). Descriptions of the IBM-supplied CNM programs follow.

Network Problem Determination Application (NPDA)

You can use NPDA to determine the cause of hardware problems in the network. Data is sent from the network (spontaneously or by request) across the CNM interface to NPDA. NCCF operators can retrieve and examine the data at a terminal.

Threshold Analysis and Remote Access Feature: Working with NCCF, this separately-orderable feature of NPDA can notify a central operator about network problems and errors. It also provides remote control of IBM 3600 and 4700 controllers. The feature can record, analyse, and display data on IBM 3600 and 4700 Finance Communication System performance and status.

Network Logical Data Manager (NLDM)

NLDM runs under NCCF. It helps you trace, collect, and correlate data related to sessions and gives you online access to the data. It helps you identify logical network problems and isolate errors.

The session data is for single- and multiple-domain sessions, as well as cross-network sessions. It comes from either the access method or an ACF/NCP. A set of full-screen panels displays the data.

Multiple Virtual Storage/Operator Communication Control Facility (MVS/OCCF)

MVS/OCCF is designed to be operated from a host system. In multiple-domain networks, the NCCF operator can control one or more MVS systems. In a single-domain network, an NCCF terminal can be used as an additional operator console.

Information/Management Feature of Information/System Release 2

The Information/Management feature of Information/System Release 2 works with NCCF to report and track problems at a data processing installation. It can also help you plan, coordinate, and monitor network changes and maintain information about the system inventory of hardware and software components.

Working also with NPDA, Information/Management can help network operators transfer error data from NPDA to Information/Management, and thus automatically create a new problem record.

Products Supported with NLDM

An NLDM user may access the NLDM program product through any terminal supported by NCCF. If an IBM 3279 Display Station Model 2A or 3A is used, the NLDM panels are displayed in base colors. If an IBM 3279 Display Station Model 2B or 3B is used, the NLDM panels are displayed in 7 colors. NLDM uses the large screen capability of the IBM 3278 Model 3 or 4.

Appendix B. Library Summaries

This appendix is designed to help you choose the books you need for further information on the five network program products described in this book. It first describes the organization of the libraries and then presents abstracts of the books' contents. Included also is a list of books on operation systems, subsystems, and program products that are related to telecommunication.

Organization of the Libraries

The libraries for the network program products described in this book are "task oriented." That is, each book in a library provides the information you need to perform a specific task. The tasks are briefly described below.

Evaluation

This task involves deciding whether the program product meets the requirements of your business.

Planning

This task consists of planning how to install and use the program products. You must choose program product options and decide what procedures are to be followed during the tasks described below.

Installing the Program Product

This task consists of the following functions:

- Defining the program products to your operating system
- Placing the program products on the system library
- Adding program product facilities and options
- Applying PTFs.

Resource Definition

This task involves defining characteristics of network resources to the program product. These resources can be:

- Processor cycles
- Real or virtual storage
- Networks
- Terminals
- Input/output paths
- Data bases
- Date files
- Programs
- User profiles
- Queues.

Customization

This task involves enhancing, extending, or otherwise altering the product by using facilities offered by the product itself. These facilities include:

- Tables that you can alter or replace entirely
- Executable code that you can alter or replace entirely
- Options that you can invoke when the program starts.

Writing ACF/VTAM Application Programs

This task involves planning, designing, and coding ACF/VTAM application programs, if required for your business.

Operating ACF/VTAM

This task consists of starting and stopping ACF/VTAM, monitoring and controlling it, and reacting to critical events. System programmers use the books shown in Figure 33 under "Operating ACF/VTAM" as background for creating documentation for ACF/VTAM operators.

Diagnosing Problems

This task consists of detecting, diagnosing, and correcting program product problems. It is performed by you and/or IBM programming service representative. It includes:

- Collecting and examining problem-related facts
- Organizing significant details into a problem description
- Resolving the immediate problem
- Developing a permanent solution, if needed.

Normally, you would not be involved in the last activity.

In problem diagnosis, you would first read the diagnosis guide to help you identify the problem; read the diagnosis reference to locate the module or phase of code at fault; and, for reading dumps, use the data areas book. For some program products, guide and reference information is in the same diagnosis manual.

Abstracts of Publications

This section summarizes the contents of each book in the network program products libraries in the following order: ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM.

ACF/VTAM Publications

Figure B-1 shows the books in the ACF/VTAM Version 2 Release 2 library, arranged according to their related tasks. Following the figure are abstracts of each book.

Following the abstracts of the books are diagrams showing the evolution of the ACF/VTAM library from VTAM Level 2 to ACF/VTAM Version 2 Release 2.

Using the ACF/VTAM Library

Network Program Products
General Information
GC27-0657

Network Program Products
Bibliography and
Master Index
GX27-0216

Evaluation and Education

Network Program Products
General Information
GC27-0657

Planning

Network Program Products
Planning
SC27-0658

Installing ACF/VTAM and Resource Definition

ACF/VTAM
Installation and
Resource Definition
SC27-0610

ACF/VTAM
Reference Summary
SX27-0027

Customizing ACF/VTAM

ACF/VTAM
Customization
SC27-0613

ACF/VTAM
Reference Summary
SX27-0027

Writing ACF/VTAM Application Programs

ACF/VTAM
Programming
SC27-0611

ACF/VTAM
Reference Summary
SX27-0027

Operating ACF/VTAM

ACF/VTAM
Operation
SC27-0612

ACF/VTAM
Messages and Codes
SC27-0614

ACF/VTAM
Reference Summary
SX27-0027

Diagnosing ACF/VTAM Problems

ACF/VTAM
Diagnosis Guide
SC27-0615

ACF/VTAM
Diagnosis Reference
SC27-0621

ACF/VTAM
Data Areas
LY38-3054

ACF/VTAM
Logic
LY27-8034

ACF/VTAM
Logic:
Encrypt/Decrypt Feature
LY38-3055

Figure B-1. The ACF/VTAM Version 2 Release 2 Library

Network Program Products General Information (GC27-0657)

This book provides an overview of the facilities of ACF/VTAM Version 2 Release 2 and of the major tasks involved in using it. It contains information on the hardware and software requirements for the use of ACF/VTAM, and other information on the use of ACF/VTAM with which you can determine whether or not you need this product.

Network Program Products Bibliography and Master Index (GX27-0216)

This book contains a list of other books that might be useful to someone planning, installing, or using a network that contains ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, or NLDM. It also contains a listing of topics discussed in the ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, and NLDM libraries. Each entry in the listing is followed by the titles of the books discussing that topic.

Network Program Products Planning (SC27-0658)

The objective of this book is to help you plan a network containing ACF/VTAM, ACF/NCP, ACF/SSP, NCCP, or NLDM. After reading this book, system planners will be able to select the options that best suit the needs of your business.

This book provides information about planning an ACF/VTAM-based network for MVS systems. (It also has NCCF and ACF/NCP planning information for ACF/TCAM.) This book discusses planning for:

- Deciding what kind of network you want
- Installing ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM
- Defining the network to ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM
  - Defining routes
- Operating an ACF/VTAM-based network
  - Starting ACF/VTAM and ACF/NCP
  - Using NCCF as a program operator
  - Operating in the same network with ACF/TCAM
- Testing an ACF/VTAM-based network
- Customizing an ACF/VTAM-based network
  - Establishing and terminating sessions
  - Tuning the network
  - Installation exit routines and replaceable modules
- ACF/VTAM application programs
- Using TSO/VTAM
- NCCF and CNM planning considerations for ACF/VTAM
- NCCF and CNM planning considerations for ACF/TCAM
- Planning considerations for using NCCF Version 2 with ACF/TCAM
- SSP planning considerations
- ACF/NCP planning considerations
- NLDM planning considerations
- Planning considerations for SNA network interconnection.

ACF/VTAM Installation and Resource Definition (SC27-0610)

The objective of this book is to enable a systems programmer to install ACF/VTAM, under MVS systems, and define a network to it. The book discusses:

- Installing ACF/VTAM
- Coding start options
- Defining the network to ACF/VTAM
- Testing ACF/VTAM definitions.

This book has appendixes to enable systems programmers to quickly locate the detailed syntax of the macro instructions and definition statements used to define a network to ACF/VTAM, as well as ACF/VTAM start options.

ACF/VTAM Customization (SC27-0613)

The objective of this book is to enable a systems programmer to customize ACF/VTAM and tune it for better performance under MVS systems. It discusses:

- Modifying ACF/VTAM messages
- Modifying ACF/VTAM USS commands
- Installation exit routines and replaceable modules
- Tuning ACF/VTAM

ACF/VTAM Programming (SC27-0611)

This book describes how to use ACF/VTAM macro instructions to send data to and receive data from (1) a terminal in either the same or a different domain, or (2) another application program in either the same or a different domain. Also included is a dictionary of ACF/VTAM macro instructions. This book assumes that the reader is familiar with assembler language and the programming facilities of the operating system.

ACF/VTAM Operation (SC27-0612)

This book is a reference manual for operators who run an ACF/VTAM network. It is also a guide for system programmers who must supply operators with the detailed information that they need to run the ACF/VTAM network.

This book includes:

- An introduction to operating ACF/VTAM
- A description of ACF/VTAM commands
- A description of how to use ACF/VTAM commands to perform network control functions.

ACF/VTAM Messages and Codes (SC27-0614)

This book contains, in alphanumeric order, all messages and codes issued by ACF/VTAM. These include all operator messages with IST prefixes, TSO/VTAM messages, and terminal user and operator messages issued by

ACF/VTAM's unformatted system services (USS). This book can be inserted into the operating system messages manual, if desired, or used as a stand-alone book.

ACF/VTAM Diagnosis Guide (SC27-0615)

This book describes an approach to debugging ACF/VTAM. This book helps the reader determine the failing ACF/VTAM function, and develop a keyword string of symptoms that accurately describe the problem. It presents guidelines, tools, and other information that the reader can use as ACF/VTAM debugging aids. These aids can help to isolate an error or failure to ACF/VTAM, to the ACF/NCP, or to an ACF/VTAM application program or device (logical unit). This book also summarizes serviceability aids described in other books and directs the reader to detailed descriptions of these aids. It also includes a foldout diagram of the major ACF/VTAM control blocks.

This book is intended for customer system programmers and IBM programming service representatives (PSRs) who maintain systems and application programs that use ACF/VTAM.

ACF/VTAM Diagnosis Reference (SC27-0621)

This book contains reference information to use with the *ACF/VTAM Diagnosis Guide*. The first section contains an overview of the logic of ACF/VTAM, an overview of the control blocks of ACF/VTAM, and an overview of the components of ACF/VTAM. The second section is an alphanumeric listing of modules, a summary of the functions performed by each module, and any major input/output.

ACF/VTAM Data Areas (LY38-3054)

This book describes all of the data areas used by ACF/VTAM and can be used to read an ACF/VTAM dump. It is intended for IBM programming service representatives and customer personnel who are diagnosing problems with ACF/VTAM.

The map of each ACF/VTAM data area is divided into four parts. First is a reference list giving a function description of the data area, its boundary alignment, its length in bytes, a list of control blocks containing pointers to the data area, control blocks embedded within the data area, and where in storage the data area is found. Second is a diagram of the data area, showing the offsets, type, length, name, and description of each field in the data area. Third is a cross-reference list of all fields in the data area. Fourth is a list of constant fields in the data area, if any. The constants are listed by field name, value, and meaning.

Information about categories of ACF/VTAM data areas and control block relationships is included in *ACF/VTAM Diagnosis Reference*.

ACF/VTAM Logic (LY27-8034)

This book describes the logic of the base ACF/VTAM program product. It is intended to help IBM programming service representatives and customer system programmers to quickly locate failing ACF/VTAM modules. There are three sections of diagnosis information. The first section describes the major functions of the ACF/VTAM components. It shows the input to each function, the modules and macro instructions involved in performing that function, and the output from the function. The second section shows the flow of module control for each major function. The third section shows the processing of ACF/VTAM operator commands, application program macro instructions, and request/response unit (RUs). Additionally, a module directory lists all of the ACF/VTAM modules in alphanumeric order, and, for each module, gives its descriptive name, its load module or library, and the diagrams in which the module appears.

This book contains only information about ACF/VTAM without the optional Encrypt/Decrypt Feature. For logic information about this feature, see *ACF/VTAM Logic: Encrypt/Decrypt Feature*, LY38-3055.

ACF/VTAM Logic: Encrypt/Decrypt Feature (LY38-3055)

This book describes the logic of the Encrypt/Decrypt Feature of ACF/VTAM. It should be used in conjunction with *ACF/VTAM Logic*, LY27-8034, which describes the high-level logic of ACF//VTAM including the Encrypt-Decrypt Feature. This book is intended primarily to help IBM programming service representatives and customer system programmers to quickly locate failures in ACF/VTAM.

Included in this book are module flow diagrams that describe the logic of this feature's components and show the flow of control between modules. It also contains summaries of key information (name, function, input, and output) on each module of this feature.

This information should enable the reader to determine the module that performs a particular function and how control passes to and from that module.

This book should be used along with *ACF/VTAM Data Areas*, LY38-3054, which contains maps of the data areas used by ACF/VTAM, including the Encrypt/Decrypt Feature.

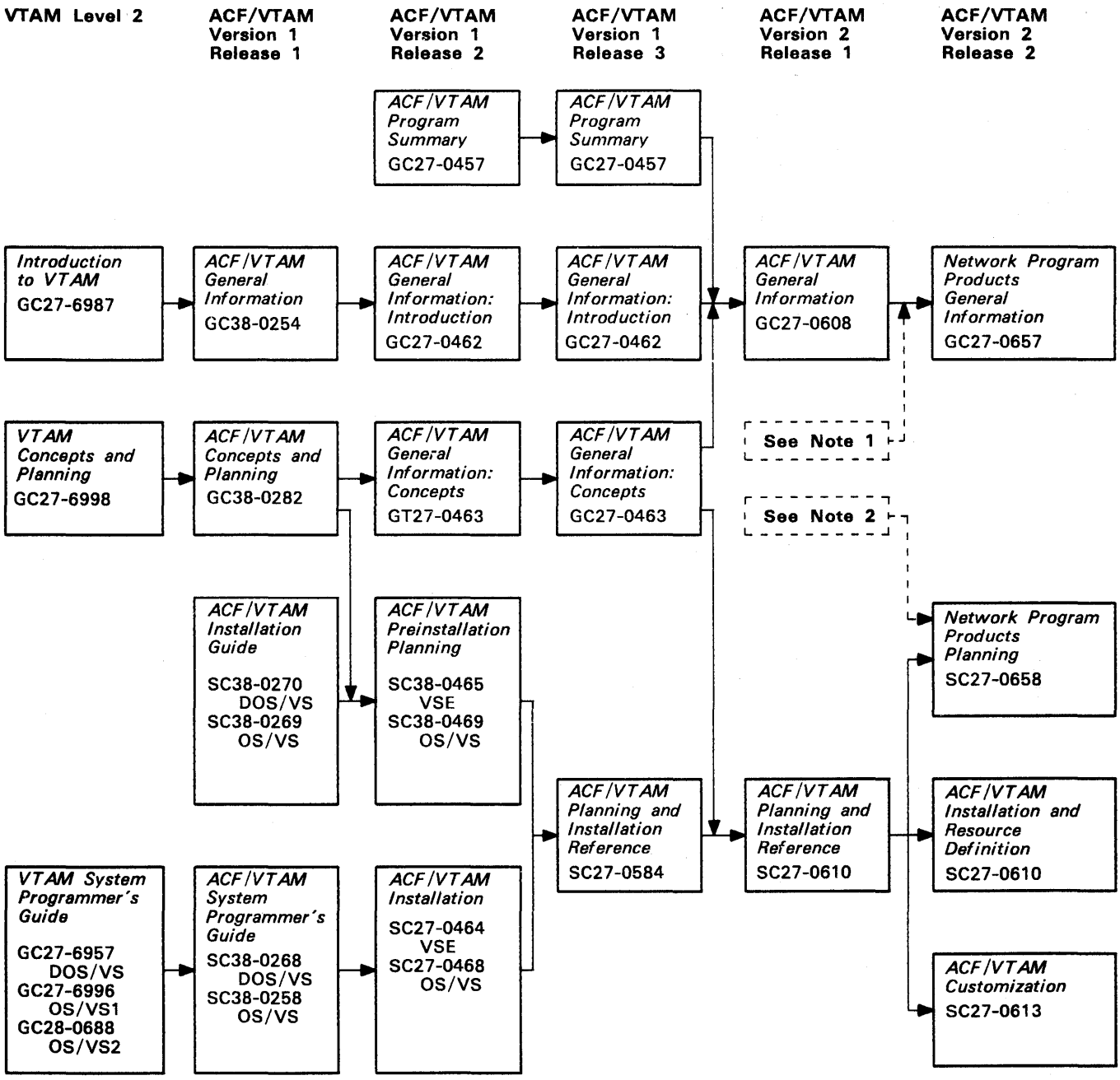
Evolution of the ACF/VTAM Library

This section illustrates the relationship of each book in the ACF/VTAM Version 2 Releases 2 library to its predecessor books in earlier ACF/VTAM libraries. It is intended primarily to help ACF/VTAM users migrating from earlier releases of the access method by identifying the ACF/VTAM Version 2 Release 2 book that contains information included in books from earlier ACF/VTAM libraries.

Figure B-2 shows the titles and form numbers for the books in the libraries for VTAM Level 2; ACF/VTAM Version 1 Releases 1, 2, and 3; and ACF/VTAM Version 2 Releases 1 and 2. The arrows between the books for each library represent the evolution of the books, that is, the movement of information from a book in one library to a book in another library.

For example, information contained in *ACF/VTAM Installation Guide*, a book in the ACF/VTAM Version 1 Release 1 library, can be found in the Version 2 Release 1 book, *ACF/VTAM Planning and Installation Reference*. The Version 1 Release 2 book containing that information is *ACF/VTAM Pre-Installation Planning*.

Related information from more than one book is often combined into a single book for the convenience of the user. For example, information from three Version 1 Release 2 books is now combined in the Version 2 book, *ACF/VTAM Diagnosis Reference*. There are times, however, when information on a particular function or product is more readily usable if it is spread out among several books. Hence, information from the Version Release 1 book, *ACF/VTAM TOLTEP*, was divided between two Version 1 Release 2 books (and their Version 2 successors): *ACF/VTAM Messages and Codes*, and *ACF/VTAM Diagnostic Techniques*.



Notes:

1. ACF/VTAM information has been combined with material from general information manuals for ACF/NCP and ACF/SSP, NCCF, and NLDM.
2. ACF/VTAM information has been combined with information from installation manuals for ACF/NCP and ACF/SSP, NCCF, and NLDM.

Figure B-2 (Part 1 of 4). Evolution of the ACF/VTAM Version 2 Release 2 Library

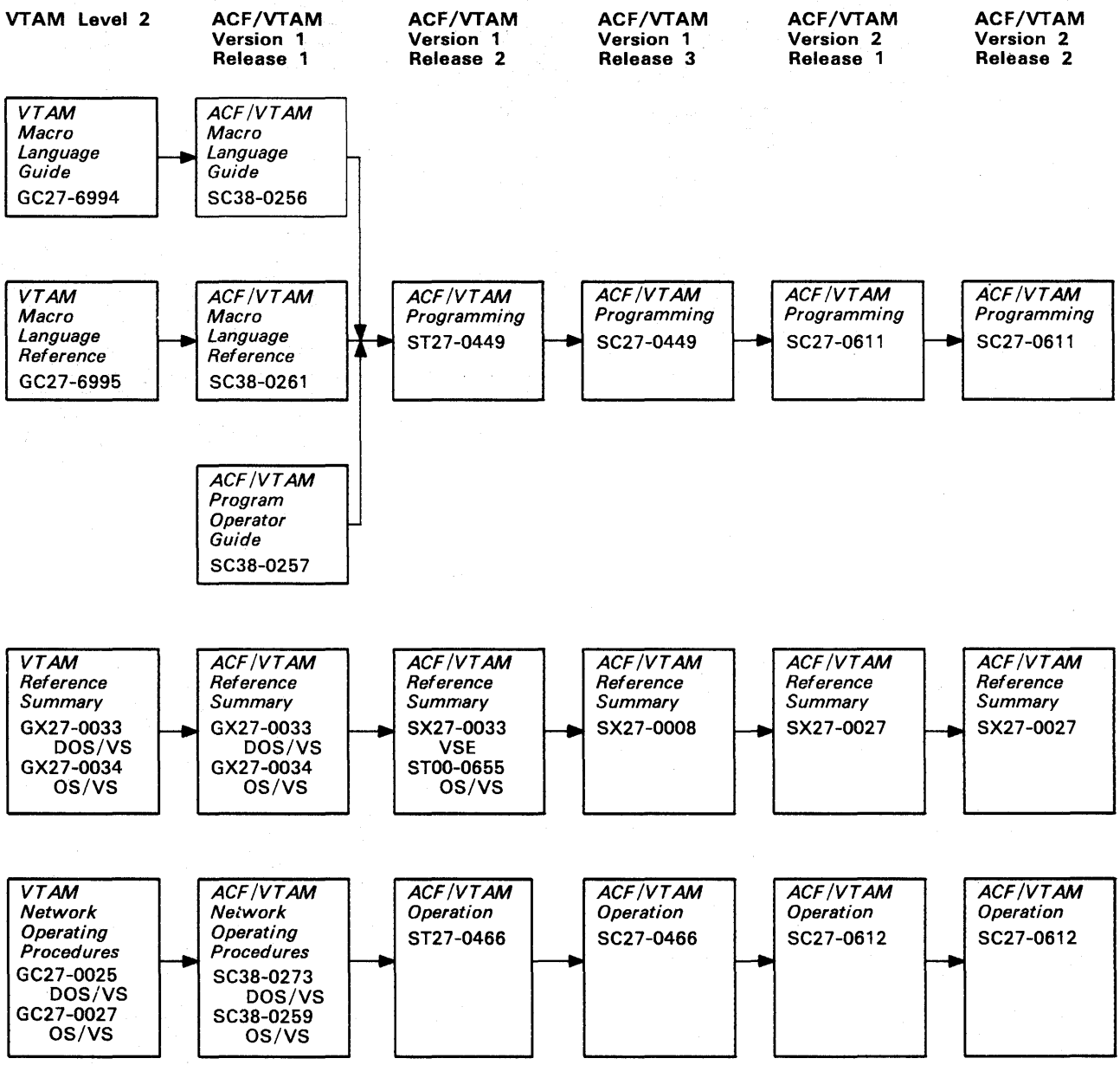


Figure B-2 (Part 2 of 4). Evolution of the ACF/VTAM Version 2 Release 2 Library

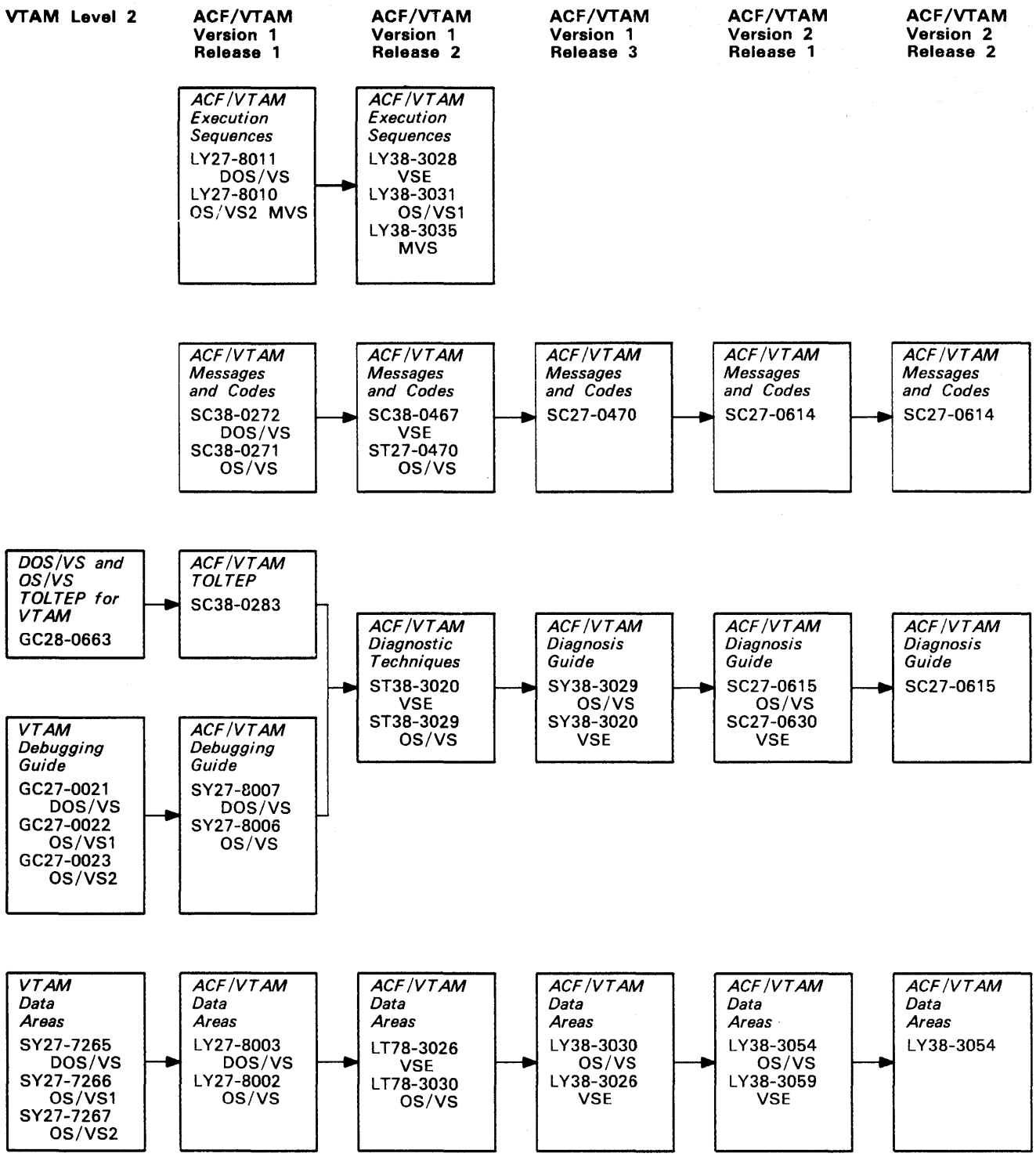


Figure B-2 (Part 3 of 4). Evolution of the ACF/VTAM Version 2 Release 2 Library

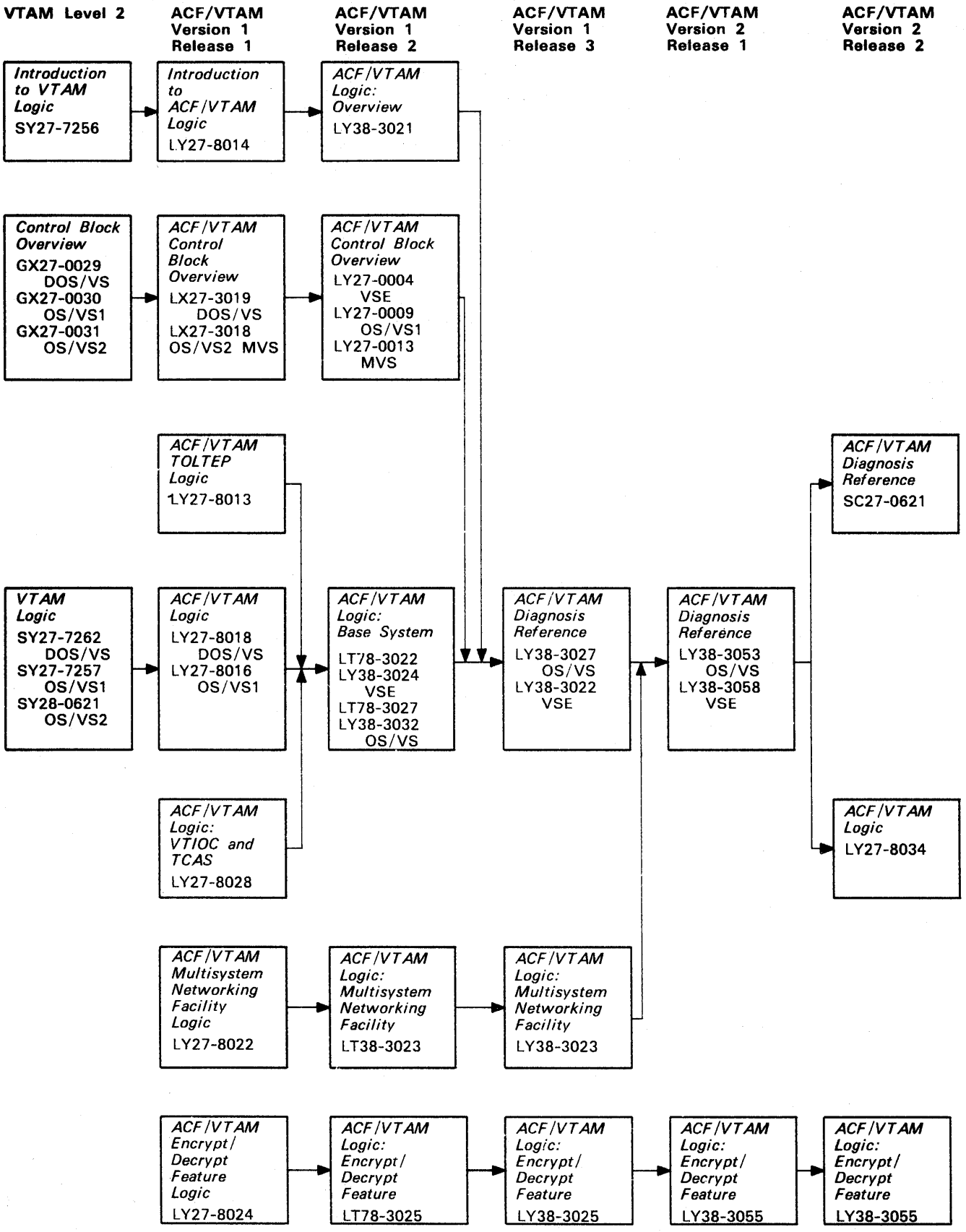


Figure B-2 (Part 4 of 4). Evolution of the ACF/VTAM Version 2 Release 2 Library

ACF/NCP Publications

Figure B-3 shows the books in the ACF/NCP Version 3 library, arranged according to their related tasks. Following the figure are abstracts of the books.

Following the abstracts of the books are diagrams showing the evolution of the ACF/NCP library from NCP Level 5 to ACF/NCP Version 3.

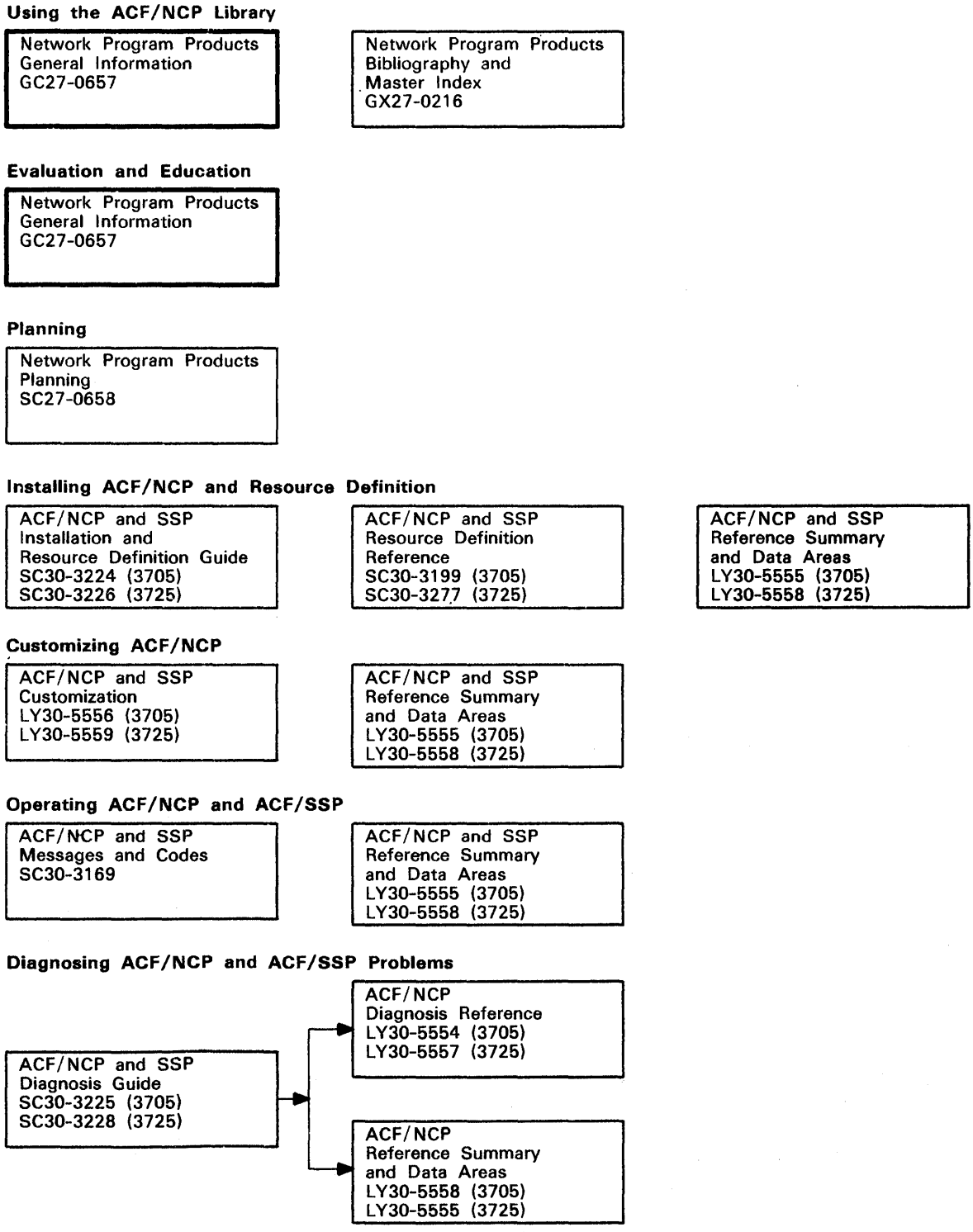


Figure B-3. The ACF/NCP Version 3 Library

Network Program Products General Information (GC27-0657)

This book provides an overview of the facilities of ACF/NCP Version 3 and of the major tasks involved in using it. It contains information on the hardware and software requirements for the use of ACF/NCP, and other information on the use of ACF/NCP with which you can determine whether or not you need this product.

Network Program Products Master Bibliography and Master Index (GX27-0216)

This book contains a list of other books that might be useful to someone planning, installing, or using a network that contains ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, or NLDM. It also contains a listing of topics discussed in the ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, and NLDM libraries. Each entry in the listing is followed by the titles of the books discussing that topic.

Network Program Products Planning (SC27-0658)

The objective of this book is to help you plan a network containing ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, and NLDM. After reading this book, system planners will be able to select the options that best suit the needs of your business.

This book provides information about planning an ACF/VTAM-based network for MVS systems. (It also has NCCF and ACF/NCP planning information for ACF/TCAM.) This book discusses planning for:

- Deciding what kind of network you want
- Installing ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM
- Defining the network to ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, and NLDM
  - Defining routes
- Operating an ACF/VTAM-based network
  - Starting ACF/VTAM and ACF/NCP
  - Using NCCF as a program operator
  - Operating in the same network with ACF/TCAM
- Testing an ACF/VTAM-based network
- Customizing an ACF/VTAM-based network
  - Establishing and terminating sessions
  - Tuning the network
  - Installation exit routines and replaceable modules
- ACF/VTAM application programs
- Using TSO/VTAM
- NCCF and CNM planning considerations for ACF/VTAM
- NCCF and CNM planning considerations for ACF/TCAM
- Planning considerations for using NCCF Version 2 with ACF/TCAM
- ACF/SSP planning considerations
- ACF/NCP planning considerations
- NLDM planning considerations
- Planning considerations for SNA network interconnection.

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3705: Installation and Resource Definition Guide (SC30-3224-0)

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3725: Installation and Resource Definition Guide (SC30-3226-0)

These manuals contain information to help users produce an operating Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication Controllers. The manuals cover the following four major areas:

- Installing the program
- Defining the program
- Generating the program
- Loading the program.

The primary purpose of the manuals is to help programmers determine which macros and operands they need to code to define their particular NCPs.

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3705: Resource Definition Reference (SC30-3199-0)

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3725: Resource Definition Reference (SC30-3227-0)

These manuals contain detailed descriptions of the macro instruction statements used to define the Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication Controllers. These manuals are directed to system analysts and system programmers. These manuals will help them prepare an ACF/NCP to be used in communicating with an IBM System/370 in which one or more of the following access methods are being executed: ACF/TCAM, ACF/VTAM, TCAM, or VTAM.

Also, these manuals provide information on the partitioned emulation programming extension to ACF/NCP, which permits the 3705 or 3725 to emulate the operation of an IBM 2701 or 2703 Transmission Control Unit for specified communication lines. Stations on these lines communicate in emulation mode with application programs in the System/370 via BTAM, QTAM, TCAM, or equivalent access methods that can be used with the transmission control units mentioned.

Advanced Communications Function for Network Control Program for the IBM 3705: Emulation Program for the 3705: Reference Summary and Data Areas (LY30-5555-0)

Advanced Communications Function for Network Control Program for the IBM 3725: Emulation Program for the IBM 3725: Reference Summary and Data Areas (LY30-5558-0)

These manuals contain reference information about the Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communications Controllers. The manuals are intended for system programmers and IBM program support representatives. Their primary purpose is to provide quick access to often-used diagnostic and debug information. If more comprehensive information is needed about ACF/NCP, refer to one of the other manuals for the program.

Advanced Communications Function for Network Control Program for the IBM 3705: Customization (LY30-5556-0)

Advanced Communications Function for Network Control Control Program for the IBM 3725: Customization (LY30-5559-0)

These manuals provide information for users who want to modify the IBM-provided Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication Controllers. These manuals are intended for programmers who are familiar with the operation of the NCP.

The manuals enable the programmer to customize the NCP by adding line control for stations that are not supported by the NCP, and by adding programmed System Network Architecture (SNA) resources. The following information is presented in the manual:

- The facilities provided for customizing an NCP
- How to add routines to the NCP to provide character service, timer interruption handling, and XIO service
- How to add programmed SNA links and programmed network addressable units to the NCP
- The resources and NCP macro instructions provided for customizing the NCP
- Coding and system generation examples.

Advanced Communications Function for Network Control Program and System Support Programs: Messages and Codes (SC30-3169-2)

This is a manual of messages issued by the Advanced Communications Function for System Support Programs (ACF/SSPs) Version 2 Release 2. These SSPs are associated with the Advanced Communications Function for

Network Control Program (ACF/NCP) Version 3 that operates in the IBM 3705 and 3725 Communication Controllers. The SSPs for which messages are issued are:

- The Advanced Communications Function/Trace Analysis Program (ACF/TAP)
- The independent loader utility provided as an NCP SSP under OS/VS
- The dynamic dump utility provided as an NCP SSP (for emulation mode only) under OS/VS
- The configuration report program provided as an NCP SSP under OS/VS.

This manual also includes messages issued by the communication controller assembler program during stage 1 of NCP generation.

Advanced Communication Function for Network Control Program and System Support Programs for the IBM 3705: Diagnosis Guide (SC30-3225-0)

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3725: Diagnosis Guide (SC30-3228-0)

These manuals contain information to help user diagnosticians and program support representatives isolate and define problems in the Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication Controllers. The primary purpose of the manuals is to help the user interact with the IBM Support Center to resolve a user's problem. Procedures in these manuals describe how to:

- Determine whether the problem is with ACF/NCP
- Use relevant information to describe the problem
- Gather appropriate documentation about the problem
- Report the problem to the IBM Support Center

Advanced Communications Function for Network Control Program for the IBM 3705: Diagnosis Reference (LY30-5554-0)

Advanced Communications Function for Network Control Program for the IBM 3725: Diagnosis Reference (LY30-5557-0)

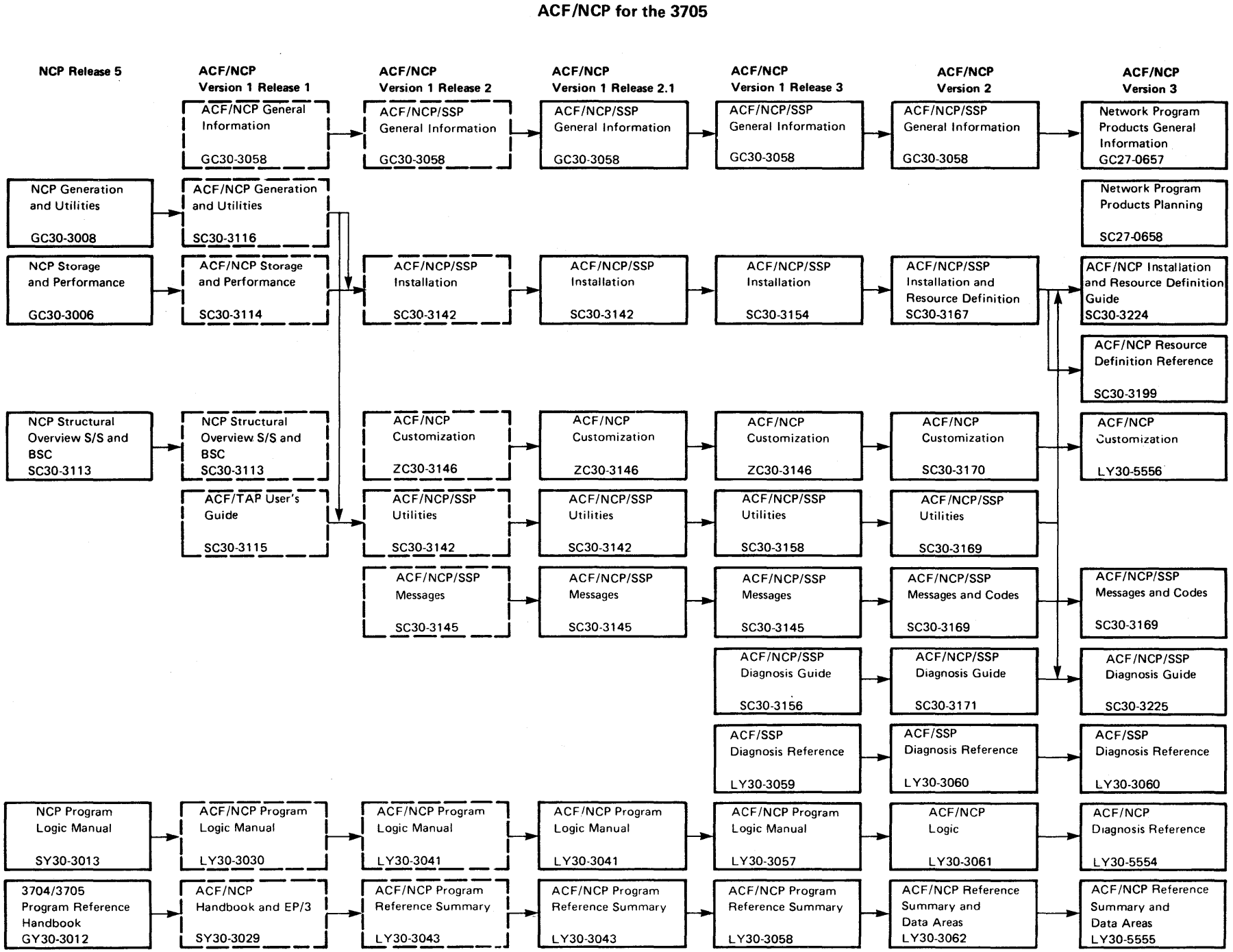
These manuals describe the internal operations of the advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication Controllers. The manuals supplement the program listings of the ACF/NCP.

These manuals are directed to the IBM program support representatives and system engineers who provide program maintenance and who need information on the internal organization and operation of ACF/NCP.

Evolution of the ACF/NCP Library

Figure B-4 shows the evolution of the ACF/NCP library to the current release.

Figure B-4 (Part 1 of 2). Evolution of the ACF/NCP Version 3 Library



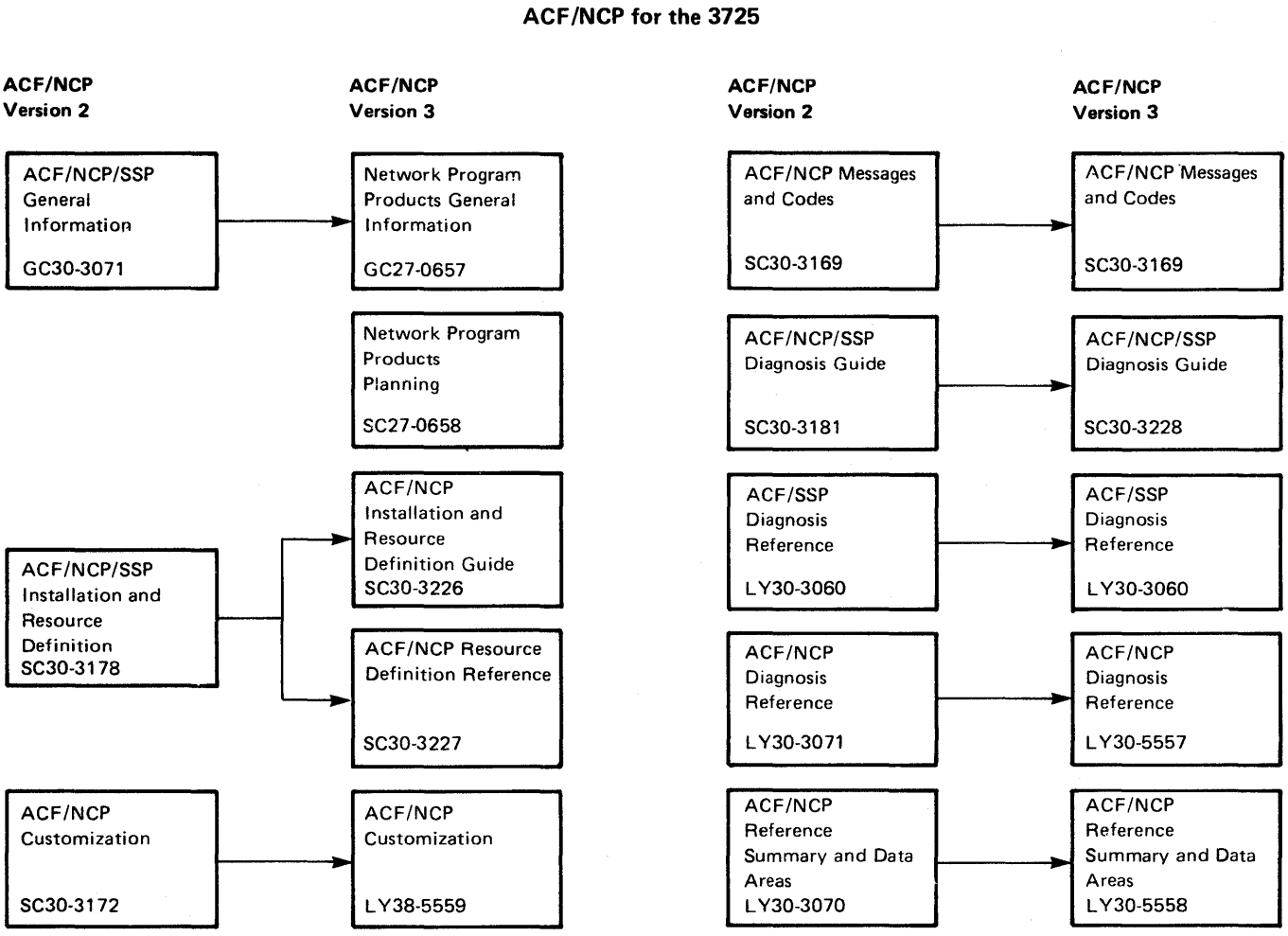


Figure B-4 (Part 2 of 2). Evolution of the ACF/NCP Version 3 Library

Figure B-5 shows the books in the ACF/SSP library, arranged according to their related tasks. Following the figure are abstracts of the books.

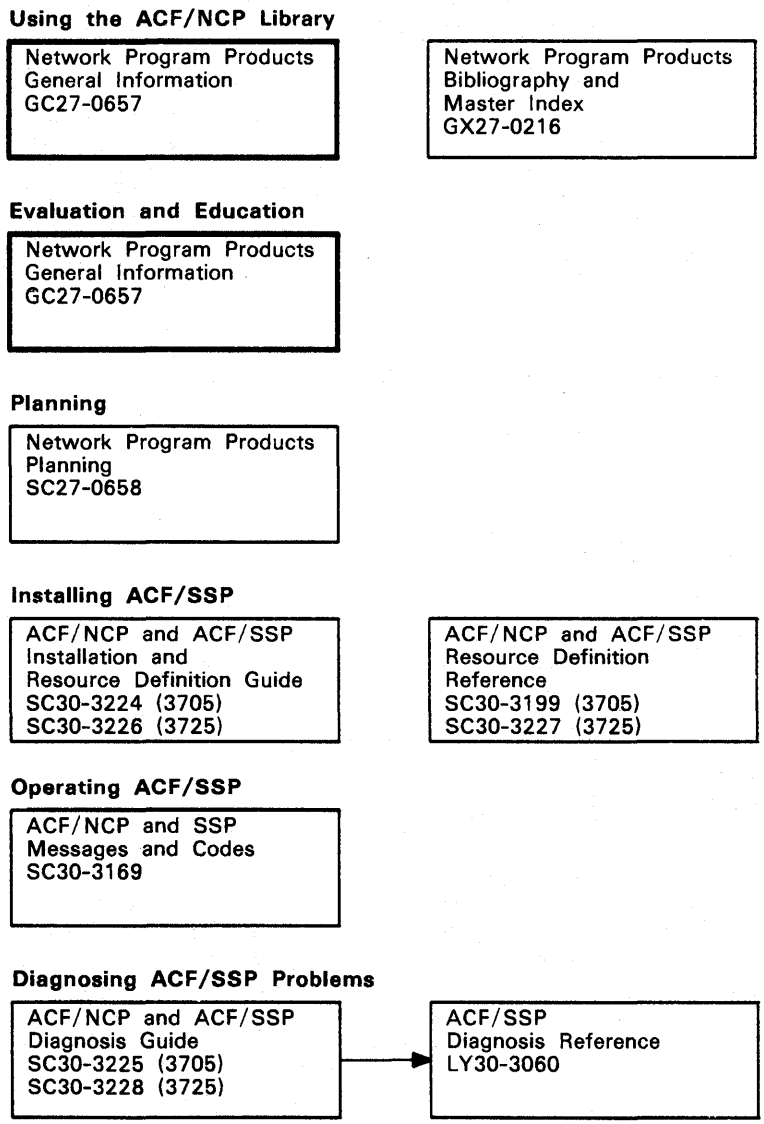


Figure B-5. The ACF/SSP Library

Network Program Products General Information (GC27-0657)

This book provides an overview of the facilities of ACF/SSP Version 2 Release 2 and of the major tasks involved in using it. It contains information on the hardware and software requirements for the use of ACF/SSP, and other information on the use of ACF/SSP with which you can determine whether or not you need this product.

Network Program Products Planning (SC27-0658)

The objective of this book is to help you plan a network containing ACF/VTAM, ACF/NCP, ACF/SSP, NCCF, and NLDM. After reading this book, system planners will be able to select the options that best suit the needs of your business.

This book provides information about planning an ACF/VTAM-based network for MVS systems. (It also has NCCF and ACF/NCP planning information for ACF/TCAM.) This book discusses planning for:

- Deciding what kind of network you want
- Installing ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM
  - Defining routes
- Operating an ACF/VTAM-based network
  - Starting ACF/VTAM and ACF/NCP
  - Using NCCF as a program operator
  - Operating in the same network with ACF/TCAM
- Testing an ACF/VTAM-based network
- Customizing an ACF/VTAM-based network
  - Establishing and terminating sessions
  - Tuning the network
  - Installation exit routines and replaceable modules
- ACF/VTAM application programs
- Using TSO/VTAM
- NCCF and CNM planning considerations for ACF/VTAM
- NCCF and CNM planning considerations for ACF/TCAM
- Planning considerations for using NCCF Version 2 with ACF/TCAM
- ACF/NCP planning considerations
- NLDM planning considerations
- Planning considerations for SNA network interconnection
- SSP planning considerations

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3705: Installation and Resource Definition Guide (SC30-3224-0)

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3725: Installation and Resource Definition Guide (SC30-3226-0)

These manuals contain information to help users produce an operating Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication

Controllers. The manuals cover the following four major areas:

- Installing the program
- Defining the program
- Generating the program
- Loading the program.

The primary purpose of the manuals is to help programmers determine which macros and operands they need to code to define their particular NCPs.

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3705: Resource Definition Reference (SC30-3199-0)

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3725: Resource Definition Reference (SC30-3227-0)

This manual contains detailed descriptions of the macro instruction statements used to define the Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communication Controllers. These manuals are directed to system analysts and system programmers. They will help them prepare an ACF/NCP to be used in communicating with an IBM System/370 in which one or more of the following access methods are being executed: ACF/TCAM, ACF/VTAM, TCAM, or VTAM.

Also, these manuals provide information on the partitioned emulation programming extension to ACF/NCP, which permits the 3705 or 3725 to emulate the operation of an IBM 2701 or 2703 Transmission Control Unit for specified communication lines. Stations on these lines communicate in emulation mode with application programs in the System/370 via BTAM, QTAM, TCAM, or equivalent access methods that can be used with the transmission control units mentioned.

Advanced Communications Function for Network Control Program and System Support Programs: Messages and Codes (SC30-3169-2)

This is a manual of messages issued by the Advanced Communications Function for System Support Programs (ACF/SSPs) Version 2 Release 2. These SSPs are associated with the Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 that operates in the IBM 3705 and 3725 Communication Controllers. The SSPs for which messages are issued are:

- The Advanced Communications Function/Trace Analysis Program (ACF/TAP)
- The independent loader utility provided as an NCP SSP under OS/VS
- The dynamic dump utility provided as an NCP SSP (for emulation mode only) under OS/VS
- The configuration report program provided as an NCP SSP under OS/VS.

This manual also includes messages issued by the communication controller assembler program during stage 1 of NCP generation.

Advanced Communication Function for Network Control Program and System Support Programs for the IBM 3705: Diagnosis Guide (SC30-3225-0)

Advanced Communications Function for Network Control Program and System Support Programs for the IBM 3725: Diagnosis Guide (SC30-3228-0)

These manuals contain information to help user diagnosticians and program support representatives isolate and define problems in the Advanced Communications Function for Network Control Program (ACF/NCP) Version 3 for the IBM 3705 and 3725 Communications Controllers. The primary purpose of the manuals is to help the user interact with the IBM Support Center to resolve a user's problem. Procedures in this manual describe how to:

- Determine whether the problem is with ACF/NCP
- Use relevant information to describe the problem
- Gather appropriate documentation about the problem
- Report the problem to the IBM Support Center

Advanced Communications Function for System Support Programs: Diagnosis Reference (LY30-3060-2)

This manual is directed to IBM program support representatives who are responsible for maintaining the Advanced Communications Function for System Support Programs (ACF/SSP) Version 2 Release 2. (The ACF/SSP Version 2 Release 2 is used with the ACF Network Control Program (ACF/NCP) Version 3.) The ACF/SSP includes an independent loader utility, dump utilities, and a configuration report program for the ACF/NCP operating in IBM 3705 and IBM 3725 Communication Controllers. The utilities and report program in the ACF/SSP can be used with OS/VS.

This manual describes the organization of the utilities and report program in the ACF/SSP and includes flow-of-control diagrams, module descriptions, and error-message-to-module cross-reference information. Also included is general information about the ACF/NCP generation process.

Figure B-6 shows the NCCF Version 2 library, arranged according to their related tasks. Following the figure are abstracts of the books.

Following the abstracts of the books is a diagram showing the evolution of the NCCF library to its current release.

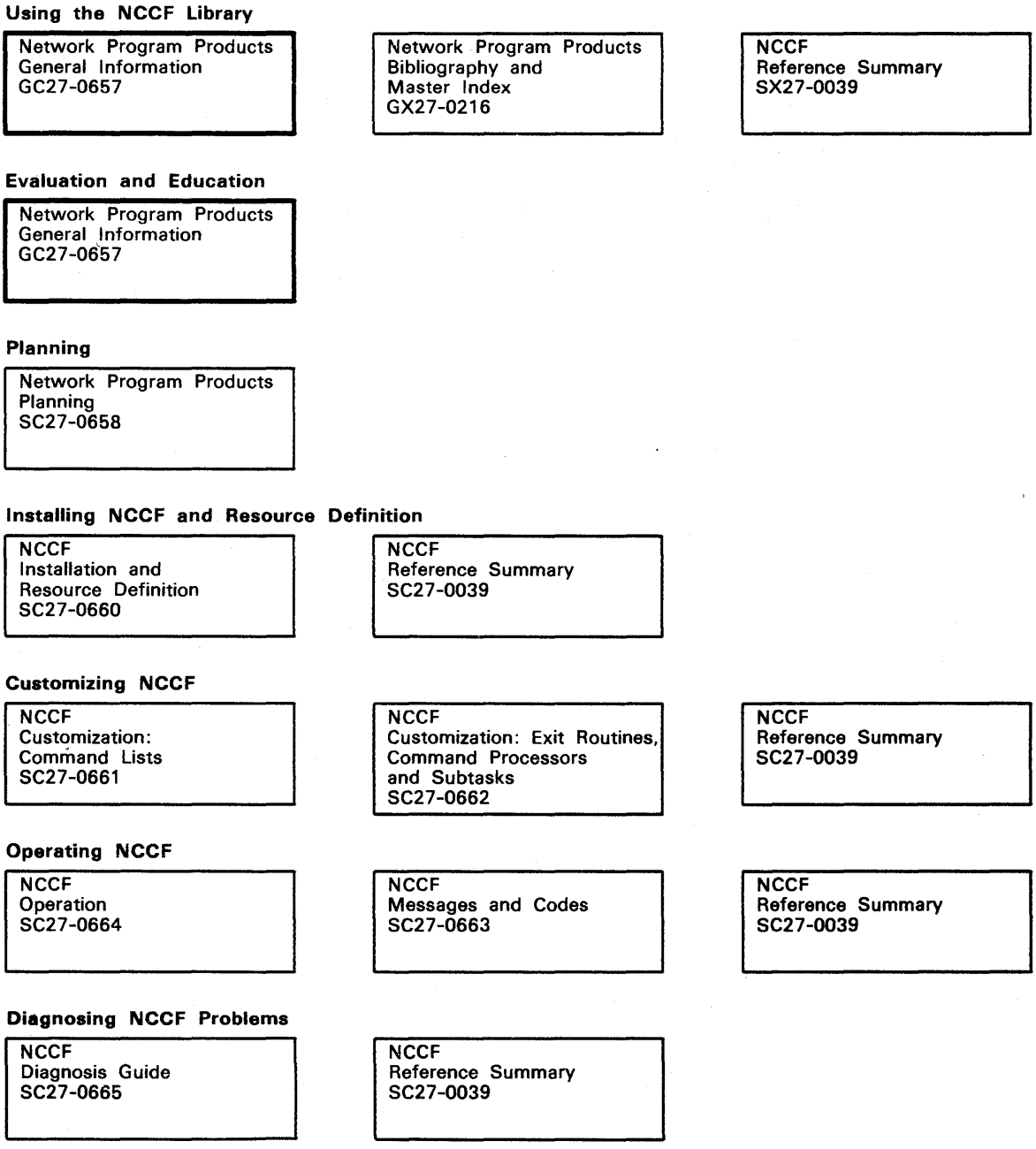


Figure B-6. The NCCF Version 2 Library

Network Program Products General Information (GC27-0657)

This book provides an overview of the facilities of NCCF Version 2 and of the major tasks involved in using it. It contains information on the hardware and software requirements for the use of NCCF, and other information on the use of NCCF with which you can determine whether or not you need this product.

Network Program Product Master Bibliography and Master Index (GX27-0216)

This book contains a list of other books that might be useful to someone planning, installing, or using a network that contains ACF/VTAM, ACF/NCP, SSP, NCCF, or NLDM. It also contains a listing of topics discussed in the ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM libraries. Each entry in the listing is followed by the titles of the books discussing that topic.

Network Program Products Planning (SC27-0658)

This book helps you plan for your NCCF network. You should read this manual before you install NCCF. The planning manual has additional information for users of ACF/VTAM Version 2 Release 2, but you should read this manual no matter what access method you are using.

Network Communication Control Facility Installation and Resource Definition (SC27-0660)

This book describes how to code the definition statements and JCL to define resources and get NCCF up and running.

Network Communication Control Reference Facility Summary (SX27-0039)

This book has information for quick look-up on messages, commands, and diagnostic hints and aids.

Network Communication Control Facility Customization: Command Lists (SC27-0661)

This book tells you how to write command lists to help control your network and make the operator's job easier.

Network Communication Control Facility Customization: Exit Routines, Command Processors, and Subtasks (SC27-0662)

This book tells you how to use and write your own exit routines, command processors, and subtasks. This makes control of the network easier.

Network Communication Control Facility Operation (SC27-0664)

This book tells you how to run NCCF. It describes the commands and how you can use them. There is a quick reference section for easy use.

Network Communication Control Facility Messages and Codes (SC27-0663)

This book has a listing of all the NCCF messages and codes. It tells you what each means and suggests actions you can take.

Network Communication Control Facility Diagnosis (SC27-0665)

This book tells you how to verify the source of a program problem, describe the problem in a standard way, search for similar problems previously found, and report new problems to an IBM support center.

Evolution of the NCCF Library

Figure B-7 shows the evolution of the NCCF library to the current release.

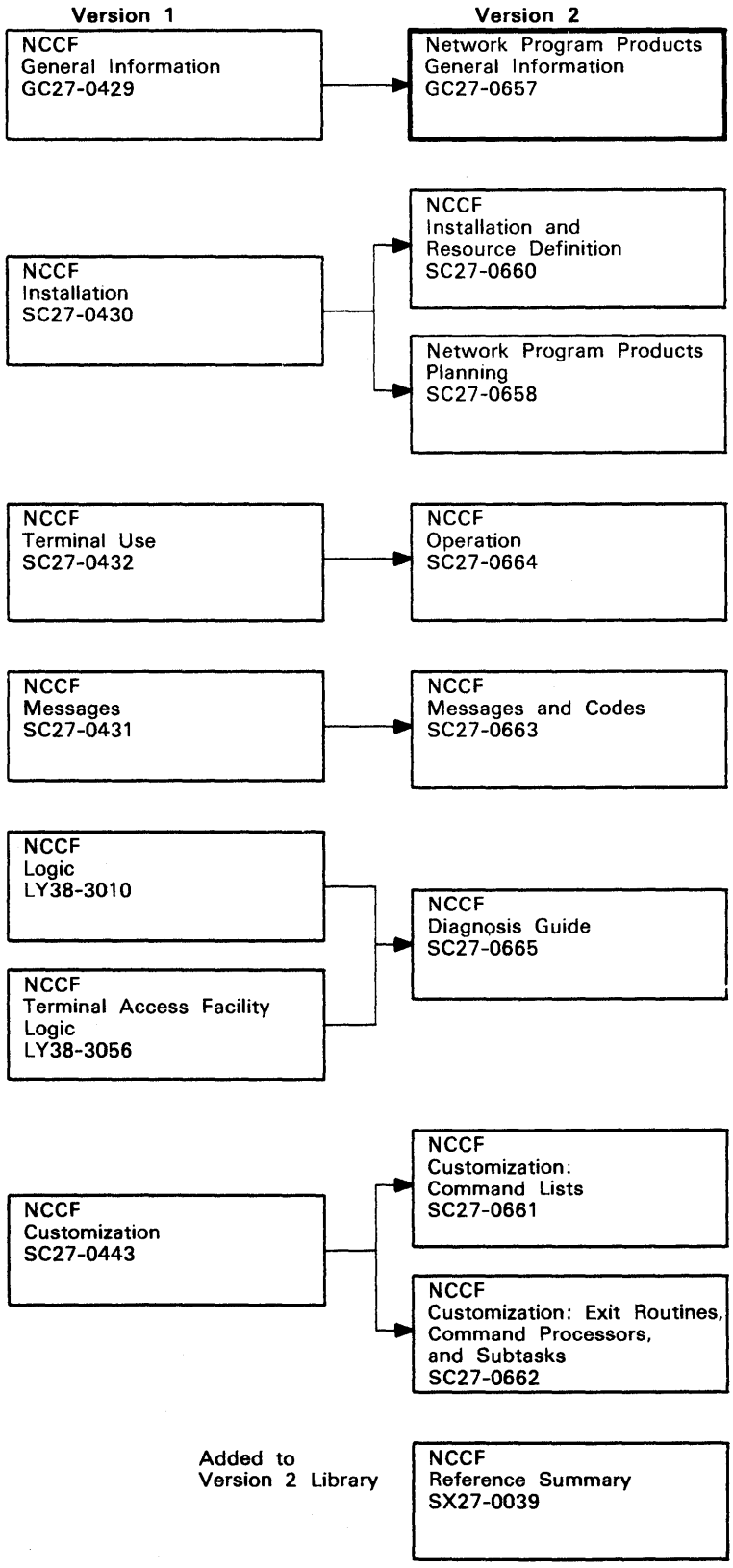


Figure B-7. Evolution of the NCCF Version 2 Library

NLDM Publications

Figure B-8 shows the books in the NLDM Release 2 library, arranged according to their related tasks. Following the figure are abstracts of the books.

Using the NLDM Library

Network Program Products
General Information
GC27-0657

Network Program Products
Bibliography and
Master Index
GX27-0216

Evaluation and Education

Network Program Products
General Information
GC27-0657

Planning

Network Program Products
Planning
SC27-0658

Installing NLDM

NLDM
Installation and
Operation
SC30-3165

Operating NLDM

NLDM
Installation and
Operation
SC27-3165

Diagnosing NLDM Problems

NLDM
Diagnosis Guide
SC30-3166

Figure B-8. The NLDM Release 2 Library

Network Program Products General Information (GC27-0657)

This book provides an overview of the facilities of NLDM Release 2 and of the major tasks involved in using it. It contains information on the hardware and software requirements for the use of NLDM, and other information on the use of NLDM with which you can determine whether or not you need this product.

Network Program Product Master Bibliography and Master Index (GX27-0216)

This book contains a list of other books that might be useful to someone planning, installing, or using a network that contains ACF/VTAM, ACF/NCP, SSP, NCCF, or NLDM. It also contains a listing of topics discussed in the ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM libraries. Each entry in the listing is followed by the titles of the books discussing that topic.

Network Program Products Planning (SC27-0658)

The objective of this book is to help you plan a network containing ACF/VTAM, ACF/NCP, SSP, NCCF, or NLDM. After reading this book, system planners will be able to select the options that best suit the needs of your business.

This book provides information about planning an ACF/VTAM-based network for MVS systems. (It also has NCCF planning information for ACF/TCAM and ACF/VTAME, and ACF/NCP planning information for ACF/TCAM.) This book discusses planning for:

- Deciding what kind of network you want
- Installing ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM
- Defining the network to ACF/VTAM, ACF/NCP, SSP, NCCF, and NLDM
  - Defining routes
- Operating an ACF/VTAM-based network
  - Starting ACF/VTAM and ACF/NCP
  - Using NCCF as a program operator
  - Operating in the same network with ACF/TCAM
- Testing an ACF/VTAM-based network
- Customizing an ACF/VTAM-based network
  - Establishing and terminating sessions
  - Tuning the network
  - Installation exit routines and replaceable modules
- ACF/VTAM application programs
- Using TSO/VTAM
- NCCF and CNM planning considerations for ACF/VTAM
- NCCF and CNM planning considerations for ACF/TCAM
- Planning considerations for using NCCF Version 2 with ACF/TCAM
- SSP planning considerations
- ACF/NCP planning considerations
- NLDM planning considerations
- Planning considerations for SNA network interconnection.

Network Logical Data Manager Installation and Operation (SC30-3165)

This book allows:

- A systems programmer to install NLDM as a program running under the control of NCCF.
- The network operator or network diagnostician to use NLDM as a network problem determination aid. In addition to telling how to operate NLDM, this book presents a detailed NLDM problem-determination scenario and documents the NLDM commands, display panels, and messages.

This book applies to NLDM with ACF/VTAM or ACF/TCAM.

Network Logical Data Manager Diagnosis (SC30-3166)

This book enables the network diagnostician to isolate and describe problems that arise in the NLDM program product. It tells how to interact with an IBM field support center to get corrections to the programming errors. The book also includes a high-level description of the internal components of NLDM and of the program's operation.

Related Publications

This section provides the titles and form numbers of books containing information on products that work in conjunction with the network program products described in this book. Most of these books are listed as prerequisite or related reading in one or more of the books in the network program products libraries.

The titles and form numbers of the books listed were correct at the time this book was published. Before ordering any book listed, you should verify the accuracy of the title and form number with your IBM representative or the *IBM System/370 and 4300 Processors Bibliography,* GC20-0001.

Systems Network Architecture (SNA) Publications

Systems Network Architecture Concepts and Products, GC30-3072

Systems Network Architecture Technical Overview, GC30-3073

Systems Network Architecture Reference Summary, GA27-3136

Systems Network Architecture Logical Unit Types, GC20-1868

Systems Network Architecture Format and Protocol Reference Manual: Architectural Logic, SC30-3112

Cryptography Publications

Data Security Through Cryptography, GC22-9062

IBM Cryptographic Subsystem Concepts and Facilities, GC22-9063

OS/VS1 and OS/VS2 MVS Programmed Cryptographic Facility General Information, GC28-0942

OS/VS1 and OS/VS2 MVS Cryptographic Unit Support General Information, GC28-1015

Network Terminal Option (NTO) Publications

Network Terminal Option General Information, GC38-0297

Network Terminal Option Installation, SC38-0298

Network Problem Determination Application (NPDA) Publications

Network Problem Determination Application Version 2 General Information, GC34-2010

Threshold Analysis and Remote Access Feature General Information, GC34-2055

TSO and TSO/VTAM Publications

OS/VS2 System Programming Library: TSO, GC28-0629

OS/VS2 TSO Terminal User's Guide, GC28-0645

OS/VS2 TSO Command Language Reference, GC28-0646

OS/VS2 TSO Guide to Writing a Terminal Monitor Program or a Command Processor, GC28-0648

Operator's Library: OS/VS2 MVS System Commands, GC28-1031

MVS/Extended Architecture TSO Command Language Reference (Supplement to *OS/VS2 TSO Command Language Reference*, GC28-0646), SD23-0259

MVS/Extended Architecture TSO Guide to Writing a Terminal Monitor Program or a Command Processor (Supplement to *OS/VS2 TSO Guide: to Writing a Terminal Monitor Program or a Command Processor*, GC28-0648), GD23-0261

MVS/Extended Architecture TSO Extensions TSO Command Language Reference, SC28-1134

MVS/Extended Architecture TSO Extensions TSO Guide to Writing a Terminal Monitor Program or a Command Processor, SC28-1136

MVS/Extended Architecture System Programming Library: TSO, GC28-1173

MVS/Extended Architecture TSO Terminal Users Guide, GC28-1274

Publications on Other Access Methods

Advanced Communications Function for TCAM General Information: Introduction, GC30-3057

Advanced Communications Function for VTAM Entry General Information: Introduction, GC27-0438

Basic Telecommunications Access Method - Extended Support (BTAM-ES) General Information, GC38-0292

OS/VS Publications

OS/VS System Modification Program (SMP) System Programmer's Guide, GC28-0673

OS/VS System Modification Program (SMP) Messages and Codes, GC38-1047

OS/VS Linkage Editor and Loader, GC26-3813

MVS Publications

OS/VS2 MVS/System Product Version 1 General Information Manual, GC28-1025

OS/VS2 System Programming Library: System Generation Reference, GC26-3792

OS/VS2 System Programming Library: Initialization and Tuning Guide (MVS/SP), GC28-1029

OS/VS2 System Programming Library: Supervisor, GC28-1046

OS/VS2 System Programming Library: Service Aids, GC28-0674

Operator's Library: OS/VS2 MVS System Commands, GC28-1031

OS/VS2 Access Method Services, GC26-3841

OS/VS2 MVS Utilities, GC26-3902

OS/VS2 System Programming Library: OLTEP, GC28-0675

OS/VS2 System Programming Library: Data Management, GC26-3830

OS/VS2 Data Management Macro Instructions, GC26-3873

OS/VS2 MVS Data Management Macro Services Guide, GC26-3875

OS/VS2 MVS Checkpoint/Restart, GC26-3877

OS/VS2 MVS JCL, GC28-0692

Installing the IBM 3790 Communication System for Use with OS/VS2, GC22-9022

Operator's Library: OS/VS2 MVS JES2 Commands, GC23-0007

Operator's Library: Network Job Entry Facility for JES2 Commands, SC23-0011

OS/VS Message Library: VS2 System Messages, GC38-1002

OS/VS Message Library: VS2 System Codes, GC38-1008

MVS/Extended Architecture Publications

MVS/System Product Version 2 General Information, GC28-1118

MVS/Extended Architecture Overview, GC28-1146

Data Facility Product General Information, GC26-4007

MVS/Extended Architecture: System Generation Reference, GC26-4009

MVS/Extended Architecture System Programming Library: Initialization and Tuning, GC28-1149

MVS/Extended Architecture System Programming Library: System Macros and Facilities (Volume 1), GC28-1150

MVS/Extended Architecture System Programming Library: System Macros and Facilities (Volume 2), GC28-1151

MVS/Extended Architecture System Programming Library: System Modifications, GC28-1152

MVS/Extended Architecture System Programming Library: Service Aids, GC28-1159

MVS/Extended Architecture Access Method Services Reference, GC26-4019

MVS/Extended Architecture Utilities, GC26-4018

MVS/Extended Architecture OLTEP, GC28-1161

MVS/Extended Architecture System Programming Library: Data Management, GC26-4010

MVS/Extended Architecture Data Management Macro Instructions, GC26-4014

MVS/Extended Architecture Data Management Services, GC26-4013

MVS/Extended Architecture Checkpoint/Restart, GC26-4012

MVS/Extended Architecture JCL, GC28-1148

MVS/Extended Architecture Operations: JES2 Commands, SC23-0064

MVS/Extended Architecture Message Library: System Messages, SG28-1156

MVS/Extended Architecture Message Library: System Codes, SG28-1157

Appendix C. Advanced Communications Function for VTAM Version 2 Release 2: Summary

ACF/VTAM Version 2 Release 2 controls communication between application programs and terminals and other application programs. These terminals and application programs can be controlled by the same ACF/VTAM, by several ACF/VTAMs organized in a network, or by ACF/VTAMs in one or more networks.

ACF/VTAM Version 2 Release 2 operates under the OS/VS2 (MVS) and MVS/XA (compatibility mode) operating systems. Its program number is 5665-280.

The ACF/VTAM Encrypt/Decrypt Feature, program number 5665-280, provides data security by enciphering and deciphering messages sent across an ACF/VTAM session.

Testing Period

The testing period for both the base system and the Encrypt/Decrypt Feature is two months for ISG, 60 days for A/FE, and 30 days for E/ME/A.

No testing period is applicable to DSLO licenses.

License

A separate license is required for each designated machine on which the licensed program materials will be used, except as otherwise provided by IBM.

Program Services

Central service, including the IBM Support Center (or IBM Support Location for A/FE) for the basic license will be available until discontinued by IBM upon twelve months' written notice. For DSLO licenses, Central Service, including the IBM Support Center, will be provided only though the customer location designated in the basic license.

Local Licensed Program Support

Local Licensed Program Support will be available until discontinued by IBM upon twelve months' written notice.

Local Licensed Program Support will be provided under the terms and conditions of the Agreement for Local Licensed Program Support for IBM Licensed Programs at the Monthly Multiple Licensed Program Support Charge, or will be provided at the applicable hourly rate.

Local Licensed Program Support under this Agreement will only be furnished through the customer location designated by the Basic License. It will be provided by IBM Field Engineering for ISG and by IBM Customer Engineering for E/ME/A and A/FE.

Warranty

The ACF/VTAM Version 2 Release 2 Licensed Program is warranted to conform to its Licensed Program Specifications when shipped to the customer if properly used in the Specified Operating Environment.

The Licensed Program Specifications may be updated from time to time and such updates may constitute a change in specifications.

Following the discontinuance of all program service, this program will be distributed on an "As Is" basis without warranty of any kind either express or implied.

Availability of Licensed Program

The estimated availability date at PID (Program Information Department) for ACF/VTAM Version 2 Release 2 is the third quarter of 1984. Estimated availability at EPL (European Program Library) and other World Trade area Program Libraries is one month later than availability at PID.

Appendix D. Advanced Communications Function for NCP Version 3: Summary

ACF/NCP Version 3 controls the flow and routing of data among resources such as access methods, terminals, cluster controllers, telecommunication lines, and other ACF/NCPs. It can exist by itself or with other ACF/NCPs in a single-domain, multiple-domain, or interconnected network.

ACF/NCP Version 3 operates under the OS/VS2 (MVS) and MVS/XA (compatibility mode) operating systems. Its program number is 5667-124.

Testing Period

The testing period is two months for ISG, 60 days for A/FE, and 30 days for E/ME/A.

No testing period is applicable to DSLO licenses.

License

A separate license is required for each designated machine on which the licensed program material will be used, except as otherwise provided by IBM. The designated machine for this license will be the communication controller.

Program Services

Central service, including the IBM Support Center (or IBM Support Location for AFE) for the basic license will be available until discontinued by IBM upon twelve months' written notice. For DSLO licenses, Central Service, including the IBM Support Center, will be provided only through the customer location designated in the basic license.

Local Licensed Program Support

Local Licensed Program Support will be available until discontinued by IBM upon twelve months' written notice.

Local Licensed Program Support will be provided under the terms and conditions of the Agreement for Local Licensed Program Support for IBM Licensed Programs at the Monthly Multiple Licensed Program Support Charge, or will be provided at the applicable hourly rate.

Local Licensed Program Support under this Agreement will only be furnished through the customer location designated by the Basic License. It will be provided by IBM Field Engineering for ISG and by IBM Customer Engineering for E/ME/A and A/FE.

Warranty

The ACF/NCP Version 3 Licensed Program is warranted to conform to its Licensed Program Specifications when shipped to the customer if properly used in the Specified Operating Environment.

The Licensed Program Specifications may be updated from time to time and such updates may constitute a change in specifications.

Following the discontinuance of all program service, this program will be distributed on an "As Is" basis without warranty of any kind either express or implied.

Availability of Licensed Program

The estimated availability date at PID (Program Information Development) for ACF/NCP Version 3 March, 1984 for the 3705 and June, 1984 for the 3725. Estimated availability at EPL (European Program Library) and other World Trade area Program Libraries is one month later than availability at PID.

Appendix E. Advanced Communications Function for SSP Version 2 Release 2: Summary

ACF/SSP Version 2 Release 2 is a library of utility programs that provides functions to help create, install, use, and maintain an ACF/NCP. Some of the programs that make up ACF/SSP operate in the host processor and others operate in the communication controller in a single-domain, multiple-domain, or interconnected network.

ACF/SSP Version 2 Release 2 operates under the OS/VS2 (MVS) and MVS/XA (compatibility mode), operating systems. Its program number is 5735-XXA.

Testing Period

The testing period is two months for ISG, 60 days for A/FE, and 30 days for E/ME/A.

No testing period is applicable to DSLO licenses.

License

A separate license is required for each designated machine on which the licensed program materials will be used, except as otherwise provided by IBM. The designated machine for this license will be the IBM System/370, 30xx, and 43xx.

Program Services

Central Service, including the IBM Support Center (or IBM Support Location for AFE) for the basic license will be available until discontinued by IBM upon twelve months' written notice. For DSLO licenses, Central Service, including the IBM Support Center, will be provided only though the customer location designated in the basic license.

Local Licensed Program Support

Local Licensed Program Support will be available until discontinued by IBM upon twelve months' written notice.

Local Licensed Program Support will be provided under the terms and conditions of the Agreement for Local Licensed Program Support for IBM Licensed Programs at the Monthly Multiple Licensed Program Support Charge, or will be provided at the applicable hourly rate.

Local Licensed Program Support under this Agreement will only be furnished through the customer location designated by the Basic License. It will be provided by IBM Field Engineering for ISG and by IBM Customer Engineering for E/ME/A and A/FE.

Warranty

The ACF/SSP Version 2 Release 2 Licensed Program is warranted to conform to its Licensed Program Specifications when shipped to the customer if properly used in the Specified Operating Environment.

The Licensed Program Specifications may be updated from time to time and such updates may constitute a change in specifications.

Following the discontinuance of all program service, this program will be distributed on an "As Is" basis without warranty of any kind either express or implied.

Availability of Licensed Program

The estimated availability date at PID (Program Information Development) for ACF/SSP Version 2 Release 2 is March, 1984. Estimated availability at EPL (European Program Library) and other World Trade area Program Libraries is one month later than availability at PID.

Appendix F. Network Communications Control Facility Version 2: Summary

NCCF Version 2 provides the ACF/VTAM or ACF/TCAM network operator with facilities to control a data communication network in a single host or a multiple host environment. NCCF also provides access method services, data storage facilities, and an application program interface for IBM or user-written network management programs.

NCCF Version 2 contains significant usability and functional enhancements designed to improve the operation and management of data communication networks.

NCCF Version 2 extends the functions provided in NCCF Version 1 Release 2 by providing SNA network interconnect support, command list (CLIST) and operator automation enhancements, and usability improvements in message handling and screen management. NCCF Version 2 also provides improved storage management, improved command processor services, and support of ASCII-8 and Katakana.

The Terminal Access Facility, previously a separately ordered feature, is included in NCCF Version 2.

NCCF Version 2 operates under the OS/VS2 (MVS) and MVS/XA (compatibility mode) operating system. Its program number is 5668-947.

Testing Period

The testing period for the base system is one month for ISG, 30 days for A/FE and E/ME/A.

No testing period is applicable to DSLO licenses.

License

A separate license is required for each designated machine on which the licensed program materials will be used, except as otherwise provided by IBM.

Program Services

Central service, including the IBM Support Center (or IBM Support Location for AFE) for the basic license will be available until discontinued by IBM upon written notice effective on the date stated therein. For DSLO licenses, Central Service, including the IBM Support Center, will be provided only though the customer location designated in the basic license.

Local Licensed Program Support

Local Licensed Program Support will be available until discontinued by IBM upon written notice effective on the date stated therein.

Local Licensed Program Support will be provided under the terms and conditions of the Agreement for Local Licensed Program Support for IBM Licensed Programs at the Monthly Multiple Licensed Program Support Charge, at the Monthly Licensed Program Support Charge, or will be provided at the applicable hourly rate.

Local Licensed Program Support under this Agreement will only be furnished through the customer location designated by the Basic License. It will be provided by IBM Field Engineering for ISG and by IBM Customer Engineering for E/ME/A and A/FE.

Warranty

The NCCF Version 2 Licensed Program is warranted to conform to its Licensed Program Specifications when shipped to the customer if properly used in the Specified Operating Environment. This does not apply to DSLO.

The Licensed Program Specifications may be updated from time to time and such updates may constitute a change in specifications.

Following the discontinuance of all program service, this program will be distributed on an "As Is" basis without warranty of any kind either express or implied.

Availability of Licensed Program

The estimated availability date at PID (Program Information Development) for NCCF Version 2 is March, 1984. Estimated availability at EPL (European Program Library) and other World Trade area Program Libraries is one month later than availability at PID.

Appendix G. Network Logical Data Manager Release 2: Summary

NLDM Release 2, program number 5668-971, is an online interactive facility that provides the Network Communications Control Facility (NCCF) operator with session awareness data, including configuration data appropriate to the session being observed, and with a portion of the most recent PIUs (Path Information Units) and selected NCP control data for SNA local and remote sessions. Trace capability is also provided for non-SNA local 3270 resources and for NCP attached BSC and Start/Stop resources. This information is useful in performing problem determination at the session level. NLDM R2 also integrates the support for the Response Time Monitor (RTM) feature of the IBM SNA 3274 Display Controllers into the general logical problem determination capabilities of NLDM. This will provide an installation the ability to set up RTM parameters from a host, and to collect and display at an NCCF operator station actual end-user response time information measured and accumulated in the IBM 3274 Controllers. With NLDM R2, route data, including intermediate network nodes, virtual and explicit routes, and boundary nodes names and addresses, can be provided.

With NLDM R2 and VTAM V2R2, NLDM can be started or restarted on an active network. NLDM can become aware of existing sessions and can commence tracing those sessions as well as sessions starting after NLDM is active.

NLDM R2 consists of command processors that operate on NCCF Version 2. The data security facilities of NCCF Version 1 or 2 apply to NLDM R1 or R2 operation respectively.

Testing Period

The basic license testing period is one month for ISG, 30 days for A/FE and E/ME/A.

License

A separate license is required for each designated machine on which the licensed program materials will be used, except as otherwise provided by IBM.

Program Services

Central service, including the IBM Support Center (or IBM Support Location for AFE) for the basic license will be available until discontinued by IBM upon twelve months' written notice. For DSLO licenses, Central Service, including the IBM Support Center, will be provided only though the customer location designated in the basic license.

Local Licensed Program Support

Local Licensed Program Support will be available until discontinued by IBM upon twelve months' written notice.

Local Licensed Program Support will be provided under the terms and conditions of the Agreement for Local Licensed Program Support for IBM Licensed Programs at the Monthly Multiple Licensed Program Support Charge, or will be provided at the applicable hourly rate.

Local Licensed Program Support under this Agreement will only be furnished through the customer location designated by the Basic License. It will be provided by IBM Field Engineering for ISG and by IBM Customer Engineering for E/ME/A and A/FE.

Warranty

The NLDM Release 2 Licensed Program is warranted to conform to its Licensed Program Specifications when shipped to the customer if properly used in the Specified Operating Environment.

The Licensed Program Specifications may be updated from time to time and such updates may constitute a change in specifications.

Following the discontinuance of all program service, this program will be distributed on an "As Is" basis without warranty of any kind either express or implied.

Availability of Licensed Program

The estimated availability date at PID (Program Information Development) for NLDM Release 2 is March, 1984. Estimated availability at EPL (European Program Library) and other World Trade area Program Libraries is one month later than availability at PID.

Glossary

This glossary defines important ACF/VTAM, NCCF, SSP, NLDM, and ACF/NCP abbreviations and terms. It includes terms and definitions from the *IBM Vocabulary for Data Processing, Telecommunications, and Office Systems*, GC20-1699. Definitions from the *American National Dictionary for Information Processing* are identified by an asterisk (*). Definitions from draft proposals and working papers under development by the International Standards Organization, Technical Committee 97, Subcommittee 1 are identified by the symbol (TC97). Definitions from the *CCIT Sixth Plenary Assembly Orange Book, Terms and Definitions* and working documents published by the International Telecommunication Union, Geneva, 1978 are preceded by the symbol (CCITT/ITU). Definitions from published sections of the *ISO Vocabulary of Data Processing*, developed by the International Standards Organization, Technical Committee 97, Subcommittee 1 and from published sections of the *ISO Vocabulary of Office Machines*, developed by subcommittees of ISO Technical Committee 95, are preceded by the symbol (ISO).

Reference Words Used in the Entries

The following reference words are used in this glossary.

Contrast with. Refers to a term that has an opposed or substantively different meaning.

Deprecated term for. Indicates that the term should not be used. It refers to a preferred term, which is defined.

See. Refers to multiple-word terms that have the same last word.

See also. Refers to related terms that have similar (but not synonymous) meanings.

Synonym for. Appears in the commentary of a less desirable or less specific term and identifies the preferred term that has the same meaning.

Synonymous with. Appears in the commentary of a preferred term and identifies less desirable or less specific terms that have the same meaning.

ACB. Access method control block.

ACB address space. In ACF/VTAM, the address space in which the ACB is opened. See *associated address space* and *session address space.*

ACB name. (1) The name of an ACB macro instruction. (2) A name specified in the ACBNAME parameter of an APPL statement. Contrast with *network name.*

> **Note:** This name allows an ACF/VTAM application program that is used in more than one domain to specify the same application program identification (pointed to by the APPLID parameter of the program's ACB statement) in each copy. ACF/VTAM knows the program by both its ACB name and its network name (the name of the APPL statement). Program users within the domain can request a session using the ACB name or the network name; program users in other domains must use the network name (which must be unique in the network).

ACB-based macro instruction. In ACF/VTAM, a macro instruction whose parameters are specified by the user in an access method control block.

accept. In an ACF/VTAM application program, to accept a CINIT request from an SSCP to establish a session with a logical unit; the application program acts as the primary end of the session. Contrast with *acquire* (1).

> **Note:** The accept process causes a BIND request to be sent from the primary end of the session to the logical unit that will act as the secondary end of the session, requesting that the session be established and passing session parameters. For example, the session-initiation request that originally caused the SSCP to send the CINIT request may have resulted from a logon by the terminal operator, from a macro instruction issued by an ACF/VTAM application program, or from an ACF/VTAM operator command.

access method. 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 VSAM or ACF/VTAM.

accounting exit routine. In ACF/VTAM, an optional installation exit routine that collects statistics about session initiation and termination.

ACF. Advanced Communications Function.

ACF/NCP. Advanced Communications Function for the Network Control Program.

ACF/TCAM. Advanced Communications Function for the Telecommunications Access Method.

ACF/VTAM. Advanced Communications Function for the Virtual Telecommunications Access Method.

ACF/VTAM application program. A program that has opened an ACB to identify itself to ACF/VTAM and can now issue ACF/VTAM macro instructions.

ACF/VTAM definition. The process of defining the user application network to ACF/VTAM and modifying IBM-defined characteristics to suit the needs of the user.

ACF/VTAM definition library. The operating system files that contain the definition statements and start options filed during ACF/VTAM definition.

ACF/VTAM operator. A person or program authorized to issue ACF/VTAM operator commands. See *domain operator, program operator,* and *network operator* (2).

ACF/VTAM operator command. A command used to monitor or control an ACF/VTAM domain.

ACF/VTAME. Advanced Communications Function for the Virtual Telecommunications Access Method Entry.

acquire. (1) In ACF/VTAM, the operation in which an authorized ACF/VTAM application program initiates and establishes a session with another logical unit; the application program acts as the primary end of the session.

> **Note:** The acquire process causes an Initiate request to be sent to the SSCP which causes the SSCP to return a CINIT request to the application program (the PLU); this in turn causes the PLU to send a BIND request to the SLU.

Contrast with *accept.* (2) In relation to ACF/VTAM resource control, to take over resources (communication controllers or other physical units) that were formerly controlled by a data communication access method in another domain, or to assume control of resources that were controlled by this domain but released. Contrast with *release.* See also *resource takeover.*

active. In ACF/VTAM, pertaining to a major or minor node for which a VARY ACT command has been issued. Also, a major or minor node in a list of major nodes to be activated when ACF/VTAM is started. Contrast with *inactive.*

> **Note:** For a major node, this makes the node and its minor nodes known to ACF/VTAM. For a minor node, this generally results in the execution of an SNA protocol to make the minor node usable by the network. For an LU minor node, this indicates that the ACF/VTAM operator has given permission for the LU to participate in an LU-LU session.

address translation. See *network address translation.*

adjacent NCPs. Network control programs (NCPs) that are connected by subarea links with no intervening NCPs.

adjacent networks. Two SNA networks joined by a common gateway NCP.

adjacent nodes. Two nodes that are connected by one or more data links with no intervening nodes.

adjacent SSCP table. A list of SSCPs that can be used to determine the next SSCP on the session-initiation path to a same-network destination SSCP or to a destination network for an LU-to-LU session. The table is filed in the ACF/VTAM definition library.

adjacent subareas. Two subareas connected by one or more links with no intervening subareas. See also *subarea.*

Advanced Communications Function (ACF). A group of IBM program products (principally ACF/TCAM, ACF/VTAM, ACF/VTAME, and ACF/NCP) that use the concepts of Systems Network Architecture (SNA), including distribution of function and resource sharing.

Advanced Communications Function for the Network Control Program (ACF/NCP). A program product that provides communication controller support for single-domain and multiple-domain networks, and, optionally, multiple-network capability.

Advanced Communications Function for the Telecommunications Access Method (ACF/TCAM). A program product that provides single-domain network, and, optionally, multiple-domain capability. ACF/TCAM runs under MVS and OS/VS1 and provides message queuing.

Advanced Communications Function for the Virtual Telecommunications Access Method (ACF/VTAM). A program product that provides single-domain network and, optionally, multiple-domain and multiple-network capability. ACF/VTAM runs under MVS, and supports direct control application programs and subsystems such as VM/VCNA and VM/VSPC.

Advanced Communications Function for the Virtual Telecommunications Access Method Entry (ACF/VTAME). A program product that provides single-domain and multiple-domain network capability for 4300 systems using VSE.

alias name. A name defined in a host used to represent a logical unit name, logon mode table name, or class of service name in another network. This name is defined to a name translation program when the alias name does not match the real name. The name translation program is used to associate the real and alias names.

alias name translation facility. A function of the Network Communications Control Facility (NCCF) program product for converting logical unit names, logon mode table names, and class of service names used in one network into equivalent names to be used in another network.

alias network address. An address used by a gateway NCP and a gateway SSCP in one network to represent an LU or SSCP in another network.

any-mode. In ACF/VTAM: (1) The form of a RECEIVE request that obtains input from any one (unspecified) session. (2) The form of an accept request that completes the establishment of a session by accepting any one (unspecified) queued CINIT request. Contrast with *specific-mode.* See *continue-any mode.* See also *accept.*

API. Application program interface.

application program. (1) A program written for or by a user that applies to the user's work. (2) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities.

application program exit routine. In ACF/VTAM, a user-written exit routine that performs functions for a particular application program and is run as part of the application program. Examples are the RPL exit routine, the EXLST exit routine, and the TESTCB exit routine. Contrast with *installation exit routine.*

application program identification. The symbolic name by which an application program is identified to ACF/VTAM.

> **Note:** It is specified in the APPLID parameter of the ACB macro instruction. It corresponds to the ACBNAME parameter in the APPL statement or, if ACBNAME is defaulted, to the name of the APPL statement.

application program interface (API). The formally-defined programming language interface between an IBM system control program or program product and its user.

application program major node. In ACF/VTAM, a member of the ACF/VTAM definition library that contains one or more APPL statements, each representing an application program.

associated address space. In ACF/VTAM, the address space in which RPL-based requests are issued that specify an ACB opened in another address space.

asynchronous exit routine. In ACF/VTAM, an RPL exit routine or an EXLST exit routine other than LERAD or SYNAD. Contrast with *inline exit routine.*

asynchronous operation. In ACF/VTAM, an operation, such as a request for session establishment or data transfer, in which the application program is allowed to continue execution while ACF/VTAM performs the operation. ACF/VTAM informs the program after the operation is completed. Contrast with *synchronous operation.*

asynchronous request. In ACF/VTAM, a request for an asynchronous operation. Contrast with *synchronous request.*

authorization exit routine. In ACF/VTAM, an optional installation exit routine that approves or disapproves requests for session initiation.

authorized path. In ACF/VTAM a facility that enables an application program to specify that a data transfer or related operation be carried out in a privileged and more efficient manner.

automatic activation. In ACF/VTAM, the activation of links and link stations in adjacent subarea nodes as a result of channel device name or RNAME specifications related to an activation command naming a subarea node.

automatic deactivation. In ACF/VTAM, the deactivation of links and link stations in adjacent subarea nodes as a result of a deactivation request naming a subarea node.

> **Note:** Automatic deactivation occurs only for automatically activated links and link stations that have not also been directly or indirectly activated.

automatic logon. A process by which ACF/VTAM creates a session-initiation request (logon) for a session between a secondary logical unit (other than a secondary application program) and a designated primary logical unit whenever the secondary logical unit is not in session with, or queued for a session with, another primary logical unit. See also *controlling application program* and *controlling logical unit.*

> **Note:** Specifications for the automatic logon can be made when the secondary logical unit is defined or can be made using the VARY NET,LOGON command.

auxiliary network address. In ACF/VTAM, any network address, except the main network address, assigned to an LU capable of having parallel sessions. Contrast with *main network address.*

available. In ACF/VTAM, pertaining to a logical unit that is active, connected, enabled, and not at its session limit.

back-level host. In SNA network interconnection, a host processor containing ACF/TCAM, ACF/VTAME, or a release of ACF/VTAM prior to the current release.

back-to-back gateways. Two gateways separated by one intervening network that contains no gateway SSCP function involved with either of the two gateway NCPs.

basic information unit (BIU). In SNA, the unit of data and control information that is passed between half-sessions. It consists of a request/response header (RH) followed by a request/response unit (RU).

basic mode. In ACF/VTAM Version 1 Release 1 and in VTAM, a mode of data transfer in which the application program can communicate with non-SNA terminals without using SNA protocols. Contrast with *record mode.*

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.*

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.*

bidder. In SNA, the LU-LU half-session defined at session activation as having to request and receive permission from the other LU-LU half-session to begin a bracket. Contrast with *first speaker.* See also *bracket protocol.*

binary synchronous communication (BSC). (1) Communication using binary synchronous line discipline. (2) A uniform procedure, using a standardized set of control characters and control character sequences, for synchronous transmission of binary-coded data between stations.

binary synchronous transmission. Data transmission in which synchronization of characters is controlled by timing signals generated at the sending and receiving stations. See also *start-stop transmission* and *Synchronous Data Link Control.*

BIND. In SNA, a request to activate a session between two logical units. See also *session activation request.*

BIU. Basic information unit.

BIU segment. In SNA, the portion of a basic information unit (BIU) that is contained within a path information unit (PIU). It consists of either a request/response header (RH) followed by all or a portion of a request/response unit (RU), or only a portion of an RU.

blocking of PIUs. In SNA, an optional function of path control that combines multiple path information units (PIUs) into a single basic transmission unit (BTU).

> **Note:** When blocking is not done, a BTU consists of one PIU.

BNN. Boundary network node.

boundary function. In SNA, (1) A capability of a subarea node to provide protocol support for adjacent peripheral nodes, such as: (a) transforming network addresses to local addresses, and vice versa; (b) performing session sequence numbering for low-function peripheral nodes; and (c) providing session-level

pacing support. See also *path control network* and *network addressable unit.* (2) The component that provides these capabilities.

boundary network node (BNN). In ACF/TCAM, the programming component that performs FID2 conversion, channel data link control, pacing, and channel/device error recovery procedures for a locally attached station. These functions are similar to those performed by a network control program for an NCP-attached station.

boundary node. A subarea node that performs boundary functions. See also *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.

bracket. In SNA, one or more chains of request units (RUs) and their responses that are exchanged between the two LU-LU half-sessions and that represent a transaction between them. A bracket must be completed before another bracket can be started. Examples of brackets are data base inquiries/replies, update transactions, and remote job entry output sequences to work stations. See also *begin bracket* and *end bracket.*

bracket protocol. In SNA, a data flow control protocol in which exchanges between the two LU-LU half-sessions are achieved through the use of brackets, with one LU designated at session activation as the first speaker and the other as the bidder. The bracket protocol involves bracket initiation and termination rules. See also *bidder* and *first speaker.*

BSC. Binary synchronous communication.

BTU. Basic transmission unit.

buffer. A portion of storage for temporarily holding input or output data.

buffer group. In ACF/VTAM, a group of buffers associated with one or more contiguous, related entries in a buffer list. The buffers may be located in discontiguous areas of storage and may be combined into one or more request units.

buffer list. In ACF/VTAM, a contiguous set of control blocks (buffer list entries) that allow an application program to send function management (FM) data from a number of discontiguous buffers with a single SEND macro instruction.

buffer list entry. A control block within a buffer list that points to a buffer containing function management (FM) data to be sent.

cancel closedown. A closedown in which ACF/VTAM is abnormally terminated either because of an unexpected situation or as the result of an operator command. See also *orderly closedown* and *quick closedown.*

CDRM. Cross-domain resource manager.

CEB. Conditional end bracket.

chain. See *RU chain.*

change-direction protocol. In SNA, a data flow control protocol in which the sending logical unit (LU) stops sending normal-flow requests, signals this fact to the receiving LU using the change-direction indicator (in the request header of the last request of the last chain), and prepares to receive requests.

channel adapter. A communication controller hardware unit used to attach the controller to a System/360 or a System/370 channel.

channel-attached. (1) Pertaining to the attachment of devices directly by data channels (I/O channels) to a computer. Contrast with *link-attached.* (2) Pertaining to devices that are attached to a controlling unit by cables, rather than by telecommunication lines.

channel-attached 3705. An IBM 3705 Communications Controller that is attached to a host processor by means of a data channel. Contrast with *link-attached 3705.*

channel-attached cross-domain NCP. An NCP that is channel-attached to a data host, but resides in the domain of another host. It has been contacted over the channel by the host, but it has not been activated. (That is, no SSCP-to-PU session exists for it.)

channel-attachment major node. In ACF/VTAM: (1) a major node whose minor node is 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.

character-coded. In ACF/VTAM, pertaining to commands (such as LOGON or LOGOFF) entered by an end user and sent by a logical unit in character form. The character-coded command must be in the syntax defined in the user's unformatted system services definition table. Synonym for *unformatted.* Contrast with *field-formatted.*

CID. Communication identifier.

CINIT. A network services request sent from an SSCP to an LU requesting that LU to establish a session with another LU and to act as the primary end of the session.

ciphertext. Synonym for *enciphered data.*

class of service (COS). In SNA, a designation of the path control network characteristics, such as path security, transmission priority, and bandwidth, that apply to a particular session. The end user designates class of service at session initiation by using a symbolic name that is mapped into a list of virtual routes, any one of which can be selected for the session to provide the requested level of service.

Cleanup. A network services request, sent by an SSCP to an 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.

clear data. Data that is not enciphered. Synonymous with *plaintext.*

clear session. A session in which only clear data is transmitted or received. Contrast with *cryptographic session.*

closedown. The deactivation of a device, program, or system. See *cancel closedown, orderly closedown,* and *quick closedown.*

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 controlled entirely by hardware; for example, the IBM 3272 Control Unit.

CMC. Communication management configuration

CNM. Communication network management.

command. (1) A request from a terminal for the performance of an operation or the execution of a particular program. (2) In SNA, any field set in the transmission header (TH), request header (RH), and sometimes portions of a request unit, that initiates an action or that begins a protocol; for example: (a) Bind Session (session-control request unit), a command that activates an LU-LU session, (b) the change-direction indicator in the RH of the last RU of a chain, (c) the virtual route reset window indicator in a FID4 transmission header. See also *ACF/VTAM operator command.*

communication common carrier. In the USA and Canada, a public data transmission service that provides the general public with transmission service facilities; for example, a telephone or telegraph company.

communication control character. Synonym for *transmission control character.*

communication control unit. A communication device that controls the transmission of data over lines in a network. Communication control units include transmission control units (such as the 2702 Transmission Control Unit) and communication controllers (such as the 3705 Communications Controller).

communication controller. A type of communication control unit whose operations are controlled by one or more programs stored and executed in the unit. For example, the IBM 3705 Communications Controller. It manages the details of line control and the routing of data through a network.

communication identifier (CID). In ACF/VTAM, a key for locating the control blocks that represent a session. The key is created during the session-establishment procedure and deleted when the session ends.

communication line. Deprecated term for *telecommunication line* and *transmission line.*

communication macro instructions. In ACF/VTAM, the set of RPL-based macro instructions used to communicate during a session.

communication management configuration. (1) In ACF/VTAM, a technique for configuring a network that allows for the consolidation of many network management functions for the entire network in a single host processor. (2) A multiple-domain network configuration in which one of the hosts, called the communication management host, performs most of the controlling functions for the network, thus allowing the other hosts, called data hosts, to process applications. This is accomplished by configuring the network so that the communication management host owns most of the resources in the network that are not application programs. The resources that are not owned by the communication management host are the resources that are channel-attached stations of data hosts.

communication management host. The host processor in a communication management configuration that does all network-control functions in the network except for the control of devices channel-attached to data hosts. Contrast with *data host.*

communication network management (CNM) application program. An ACF/VTAM application program that is authorized to issue formatted management services request units containing physical-unit-related requests and to receive formatted management services request units containing information from physical units.

communication network management (CNM) interface. The interface that allows an application program to send Forward request units (RUs) to an access method (and to receive responses to these RUs) and to receive Deliver request units (RUs) from an access method (and to send responses to these RUs). These request/response units contain network services request/response units (data and commands).

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.

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 restart. In ACF/VTAM, the recovery facility that can be used after a failure or deactivation of a major node, ACF/VTAM, or the host processor to restore the domain to its status at the time of the failure or deactivation.

configuration services. In SNA, one of the types of network services in the system services control point (SSCP) and in the physical unit (PU); configuration services activate, deactivate, and maintain the status of physical units, links, and link stations. Configuration services also shut down and restart network elements and modify path control routing tables and address-translation tables. See also *maintenance services, management services, network services, session services,* and *system services control point.*

connected. In ACF/VTAM, pertaining to a PU or LU that has an active physical path to the host processor containing the SSCP that controls the PU or LU.

connection. Synonym for *physical connection.*

connection point manager. In SNA, a component of the transmission control layer that: (1) performs session-level pacing of normal-flow requests, (2) checks sequence numbers of received request units, (3) verifies that request units do not exceed the maximum permissible size, (4) routes incoming request units to their destinations within the half-session, and (5) enciphers and deciphers FMD request units when cryptography is selected. The connection point manager coordinates the normal and expedited flows for one half-session.

> **Note:** The sending connection point manager within a half-session builds the request/response header (RH) for outgoing request/response units (RUs), and the receiving connection point manager interprets the request/response headers that precede incoming request/response units.

continue-any mode. In ACF/VTAM, a state into which a session is placed that allows its input to satisfy a RECEIVE request issued in any-mode. While this state exists, input on the session can also satisfy RECEIVE requests issued in specific-mode. Contrast with *continue-specific mode.*

continue-specific mode. In ACF/VTAM, a state into which a session is placed that allows its input to satisfy only RECEIVE requests issued in specific-mode. Contrast with *continue-any mode.*

controlling application program. In ACF/VTAM, an application program with which a secondary logical unit (other than an application program) is automatically put in session whenever the secondary logical unit is available. See also *automatic logon* and *controlling logical unit.*

controlling logical unit. In ACF/VTAM, a logical unit with which a secondary logical unit (other than an application program) is automatically put in session whenever the secondary logical unit is available. A controlling logical unit can be either an application program or a device-type logical unit. See also *automatic logon* and *controlling application program.*

converted command. An intermediate form of a character-coded command produced by ACF/VTAM through use of an unformatted system services definition table. The format of a converted command is fixed; the unformatted system services definition table must be constructed in such a manner that the character-coded command (as entered by a logical unit) is converted into the predefined, converted command format. See also *unformatted.*

COS. Class of service.

cross keys. Synonym for *cross-domain keys.*

cross-domain. In SNA, pertaining to control of resources involving more than one domain.

cross-domain keys. In SNA, a pair of cryptographic keys used by a system services control point (SSCP) to encipher the session cryptography key that is sent to another SSCP and to decipher the session cryptography key that is received from the other SSCP during initiation of cross-domain LU-LU sessions that use session-level cryptography. Synonymous with *cross keys.*

cross-domain link. (1) A subarea link connecting two subareas that are in different domains. (2) A link physically connecting two domains.

cross-domain LU-LU session. In SNA, a session between logical units (LUs) in different domains. Contrast with *same-domain LU-LU session.*

cross-domain resource. A resource owned by a CDRM in another domain but known by the CDRM in this domain by network name and associated cross-domain resource manager.

cross-domain resource manager (CDRM). In ACF/VTAM, the function in the system services control point (SSCP) that controls initiation and termination of cross-domain sessions.

cross-network. In SNA, pertaining to control or resources involving more than one SNA network.

cross-network LU-LU session. In SNA, a session between logical units (LUs) in different networks.

cross-network session. An LU-to-LU or SSCP-to-SSCP session whose path traverses more than one SNA network.

cross-subarea. In SNA, pertaining to control or resources involving more than one subarea node.

cross-subarea link. A link between two adjacent subarea nodes.

CRV. Cryptography Verification.

cryptographic. Pertaining to the transformation of data to conceal its meaning. See also *encipher* and *decipher.*

cryptographic algorithm. A set of rules that specify the, mathematical steps required to encipher and decipher data.

cryptographic key. In systems using the Data Encryption Standard (DES), a 64-bit value (containing 56 independent bits and 8 parity bits) provided as input to the algorithm in determining the output of the algorithm. See *cross-domain keys, session cryptography key, host master key,* and *secondary logical unit key.*

cryptographic session. In SNA products, an LU-LU session in which a function management data (FMD) request may be enciphered before it is transmitted and deciphered after it is received. Contrast with *clear session.* See *required cryptographic session* and *selective cryptographic session.*

cryptographic session key. In SNA, deprecated term for *session cryptography key.*

Cryptography Verification (CRV) request. A request unit sent by the primary logical unit (PLU) to the secondary logical unit (SLU) as part of cryptographic session establishment, to allow the SLU to verify that the PLU is using the correct cryptographic session key.

CSP. Communication scanner processor.

data channel. A device that connects a processor and main storage with I/O storage units. Synonymous with input/output channel and I/O channel.

data communication. The transmission and reception of data.

data encrypting key. A key used to encipher and decipher data transmitted in a cryptographic session. Contrast with *key encrypting key.* See *session cryptography key.*

Data Encryption Standard (DES) algorithm. A cryptographic algorithm designed to encipher and decipher data using a 64-bit cryptographic key, as specified in the *Federal Information Processing Standard Publication 46,* January 15, 1977.

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 (1) controls whether the half-session can send, receive, or concurrently send and receive request units (RUs); (2) groups related RUs into RU chains; (3) delimits transactions via the bracket protocol; (4) controls the interlocking of requests and responses in accordance with control modes specified at session activation; (5) generates sequence numbers; and (6) correlates requests and responses.

data flow control protocol. In SNA, the sequencing rules for requests and responses by which network addressable units in a session coordinate and control data transfer and other operations. For example, see *bracket protocol.*

data host. In a communication management configuration, a host that is dedicated to processing applications and does not control network resources, except for its channel-attached devices. Contrast with *communication management host.*

data link. In SNA, synonym for *link.*

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.

data link control protocol. In SNA, a set of rules used by two nodes on a data link to accomplish an orderly exchange of information. Synonymous with *line control.*

data terminal equipment (DTE). (TC97) That part of a data station that serves as a data source, data sink, or both, and provides for the data communication control function according to protocols.

data traffic reset state. The state usually entered after Bind Session, if Cryptography Verification is used, and after Clear, but prior to Start Data Traffic. While a session is in this state, requests and responses for data and data flow control cannot be sent. Only certain session control requests can be sent.

decipher. To convert enciphered data into clear data. Contrast with *encipher.*

default SSCP list. A list of SSCPs, either in ACF/VTAM's network or another network, that can be used when no predefined CDRSC or name translation function is provided specifying an LU's owning CDRM. This list is filed as a part of an adjacent SSCP table in the ACF/VTAM definition library.

default SSCP selection. An ACF/VTAM function that selects a set of one or more SSCPs to which a session request can be routed when there is no predefined CDRSC or name translation function provided that specifies an LU's owning CDRM. See also *default SSCP list.*

definite response. In SNA, a value in the form-of-response-requested field of the request header. The value directs the receiver of the request to return a response unconditionally, whether positive or negative, to that request. Contrast with *exception response* and *no response.*

definition statement. In ACF/VTAM, the means of describing an element of the network.

delayed-request mode. In SNA, an operational mode in which the sender may continue sending request units on the normal flow after sending a definite-response request chain on that flow, without waiting to receive the response to that chain. Contrast with *immediate-request mode.*

delayed-response mode. In SNA, an operational mode in which the receiver of normal-flow request units can return responses to the sender in a sequence different from that in which the corresponding request units were sent. Contrast with *immediate-response mode.*

Note: An exception is the response to the DFC request CHASE: all responses to normal-flow request units received before CHASE must be sent before the response to CHASE is sent.

DES. Data Encryption Standard.

designated gateway SSCP. A gateway SSCP designated to perform all the gateway control functions during LU-to-LU session setup.

device control character. A control character used for the control of ancillary devices associated with a data processing system or data communication system, for example, for switching such devices on or off.

device-type logical unit. In ACF/VTAM, a logical unit that has a session limit of one and usually acts as the secondary end of a session. It is typically an SNA terminal (such as a logical unit for a 3270 terminal or a logical unit for a 3790 application program). It could be the primary end of a session, for example, the logical unit representing the Network Routing Facility logical unit. See also *peripheral node.*

DFC. Data flow control.

DFSYN response. In ACF/VTAM, a normal-flow response that is treated as a normal-flow request so that it may be received in order with normal-flow requests.

direct activation. In ACF/VTAM, the activation of a resource as a result of an activation command specifically naming the resource. Contrast with *indirect activation.*

direct deactivation. In ACF/VTAM, the deactivation of a resource as a result of a deactivation command specifically naming the resource. Contrast with *indirect deactivation.*

disabled. In ACF/VTAM, pertaining to an LU that has indicated to its SSCP that it is temporarily not ready to establish LU-LU sessions. An Initiate request for a session with a disabled LU can specify that the session be queued by the SSCP until the LU becomes enabled. The LU can separately indicate whether this applies to its ability to act as a primary logical unit (PLU) or a secondary logical unit (SLU). See also *enabled* and *inhibited.*

disconnection. The termination of a physical connection.

DLC. Data link control.

domain. In SNA, a system services control point (SSCP) and the physical units (PUs), logical units (LUs), links, link stations, and all the associated resources that the SSCP has the ability to control by means of activation requests and deactivation requests. Synonymous with *single-domain network.*

domain operator. In a multiple-domain network, the person or program that controls the operation of the resources controlled by one system services control point. Contrast with *network operator* (2).

Downstream Load Utility (DSLU). A program product that uses the communication network management (CNM) interface to support the load requirements of certain type 2 physical units, such as the IBM 3644 Automatic Data Unit and the IBM 8775 Display Terminal.

DRDS. Dynamic reconfiguration data set.

DTE. Data terminal equipment.

duplex. * In data communication, pertaining to a simultaneous two-way independent transmission in both directions. Synonymous with *full duplex.* Contrast with *half duplex.*

dynamic reconfiguration. In ACF/VTAM, the process of changing the network configuration (peripheral PUs and LUs) associated with a boundary node, without regenerating the boundary node's complete configuration tables.

dynamic reconfiguration data set (DRDS). In ACF/VTAM, a data set used for storing definition data that can be applied to a generated communication controller configuration at the operator's request. See also *dynamic reconfiguration.*

ECB. Event control block.

echo check. A check to determine the correctness of the transmission of data in which the received data are returned to the source for comparison with the originally transmitted data.

element. (1) A field in the network address. (2) The particular resource within a subarea identified by the element address. See also *subarea.*

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.*

enabled. In ACF/VTAM, pertaining to an LU that has indicated to its SSCP that it is now ready to establish LU-LU sessions. The LU can separately indicate whether this prevents it from acting as a primary logical unit (PLU) or as a secondary logical unit (SLU). See also *disabled* and *inhibited.*

encipher. (1) To scramble data or convert it, prior to transmission, to a secret code that masks the meaning of the data to any unauthorized recipient. (2) In ACF/VTAM, to convert clear data into enciphered data. Contrast with *decipher.*

enciphered data. Data whose meaning is concealed from unauthorized users. Synonymous with *ciphertext.*

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 user. In SNA, the ultimate source or destination of application data flowing through an SNA network. An end user may be an application program or a terminal operator.

ER. Explicit route.

event control block (ECB). A control block used to represent the status of an event.

exception request (EXR). In SNA, a request that replaces another message unit in which an error has been detected.

> **Note:** The exception request contains a 4-byte sense field that identifies the error in the original message unit and, except for some path errors, is sent to the destination of the original message unit; if possible, the sense data is returned in a negative response to the originator of the replaced message unit.

exception response. In SNA, a value in the form-of-response-requested field of a request header: the receiver is requested 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 one, may be returned. Contrast with *definite response* and *no response.* See also *negative response.*

exit list (EXLST). In VSAM and ACF/VTAM, a control block that contains the addresses of routines that receive control when specified events occur during execution; for example, routines that handle session-establishment request processing or I/O errors.

exit routine. Any of several types of special-purpose user-written routines. See *accounting exit routine, authorization exit routine, logon-interpret routine, virtual route selection exit routine, EXLST exit routine,* and *RPL exit routine.*

EXLST exit routine. In ACF/VTAM, a routine whose address has been placed in an exit list (EXLST) control block. The addresses are placed there with the EXLST macro instruction, and the routines are named according to their corresponding operand; hence DFASY exit routine, TPEND exit routine, RELREQ exit routine, and so forth. All exit list routines are coded by the ACF/VTAM application programmer. Contrast with *RPL exit routine.*

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 (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, the path control network components, including a specific set 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).* See also *path* and *route extension.*

explicit route length. In SNA, the number of transmission groups in an explicit route.

EXR. Exception request.

external domain. The part of the network that is controlled by an SSCP other than the SSCP that controls this part.

FD. Full duplex.

FDX. Full duplex.

feedback information. In ACF/VTAM, information that is placed in certain RPL fields when an RPL-based macro instruction is completed.

FIC. First-in-chain.

FID. Format identification.

field-formatted. Pertaining to a request or response that is encoded into fields, each having a specified format such as binary codes, bit-significant flags, and symbolic names. Contrast with *character-coded.*

field-formatted request. In SNA, a request that is encoded into fields, each having a specified format such as binary codes, binary counts, bit-significant flags, and symbolic names; a format indicator in the request/response header (RH) for the request is set to zero. Contrast with *character-coded.*

first speaker. In SNA, the LU-LU half-session defined at session activation as: (1) able to begin a bracket without requesting permission from the other LU-LU half-session to do so, and (2) winning contention if both half-sessions attempt to begin a bracket simultaneously. Contrast with *bidder.* See also *bracket protocol.*

first-in-chain (FIC). An request unit whose request header (RH) begin chain indicator is on and whose RH end chain indicator is off. See also *RU chain.*

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. See also *pacing, session-level pacing,* and *virtual route pacing.*

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. Transmission header formats differ in accordance with the types of nodes between which they pass.

Note: There are 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 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 PU type 2 peripheral node.

FID3, used for traffic between a subarea node and an adjacent PU 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.

formatted system services. A portion of ACF/VTAM that provides certain system services as a result of receiving a field-formatted command, such as an Initiate or Terminate command. Contrast with *unformatted system services (USS).* See also *field-formatted.*

full duplex (FD, FDX). Synonym for *duplex.*

function management data (FMD). In SNA, 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 SSCPs.

function management (FM) header. In SNA, one or more headers, optionally present in the leading request units (RUs) of an RU chain, that allow one half-session in an LU-LU session to: (1) select a destination at the session partner and control the way in which the end-user data it sends is handled at the destination, (2) change the destination or the characteristics of the data during the session, and (3) transmit between session partners status or user information about the destination (for example, a program or device).

Note: FM headers can be used on LU-LU session types 0, 1, 4, and 6.

function management (FM) profile. In SNA, a specification of various data flow control protocols (such as RU chains and data flow control requests) and FMD options (such as use of FM headers, compression, and alternate codes) supported for a particular session. Each function management profile is identified by a number.

gateway. The combination of machines and programs that provide address translation, name translation, and SSCP rerouting between independent SNA networks to allow those networks to communicate. A gateway consists of one gateway NCP and at least one gateway SSCP.

gateway control functions. Functions performed by a gateway SSCP in conjunction with the gateway NCP to assign alias network address pairs for Lu-to-Lu sessions, assign virtual routes for the Lu-to-Lu sessions in adjacent networks, and translate network names within BIND RUs.

gateway host. A host node that contains a gateway SSCP.

gateway NCP. An NCP that performs address translation and through which cross-network session traffic passes. The gateway NCP connects two or more independent SNA networks.

gateway node. See *gateway NCP.*

gateway SSCP. An SSCP that is capable of cross-network session initiation, termination, takedown, and session outage notification. A gateway SSCP is in session with the gateway NCP; it provides network name translation and assists the gateway NCP in setting up alias network addresses for cross-network sessions.

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, request/response header, and request/response unit data.

generic BIND. A synonym for a session activation request.

generic UNBIND. A synonym for a session deactivation request.

GPT. Generalized path information unit trace.

half-duplex. * In data communication, pertaining to an alternate, one way at a time, independent transmission. Contrast with *duplex.*

half-session. In SNA, a component that provides FMD services, data flow control, and transmission control for one of the sessions of a network addressable unit (NAU). See also *primary half-session* and *secondary half-session.*

host LU. An SNA logical unit located in a host processor, for example, an ACF/VTAM application program. Contrast with *peripheral LU.*

host master key. In SNA, deprecated term for *master cryptography key.*

host processor. (1) (TC97) A processor that controls all or part of a user application network. (2) In a network, the processing unit in which the data communication access method resides. (3) In an SNA network, the processing unit that contains a system services control point (SSCP).

ICV. Initial chaining value.

immediate-request mode. In SNA, an operational mode in which the sender stops sending request units (RUs) on a given flow (normal or expedited) after sending a definite-response request chain on that flow until that chain has been responded to. Contrast with *delayed-request mode.* See also *immediate-response mode.*

immediate-response mode. In SNA, an operational mode in which the receiver responds to request units (RUs) on a given normal flow in the order it receives them; that is, in a first-in, first-out sequence. Contrast with *delayed-response mode.* See also *immediate-request mode.*

inactive. In ACF/VTAM, pertaining to a major or minor node that has not been activated or for which the VARY INACT command has been issued. Contrast with *active.*

indirect activation. In ACF/VTAM, the activation of a lower-level resource of the resource hierarchy as a result of SCOPE or ISTATUS specifications related to an activation command naming a higher-level resource. Contrast with *direct activation.*

indirect deactivation. In ACF/VTAM, the deactivation of a lower-level resource of the resource hierarchy as a result of a deactivation command naming a higher-level resource. Contrast with *direct deactivation.*

inhibited. In ACF/VTAM, pertaining to an LU that has indicated to its SSCP that it is not ready to establish LU-LU sessions. An Initiate request for a session with an inhibited LU will be rejected by the SSCP. The LU can separately indicate whether this applies to its ability to act as a primary logical unit (PLU) or as a secondary logical unit (SLU). See also *enabled* and *disabled.*

initial chaining value (ICV). An eight-byte pseudo-random number used to verify that both ends of a session with cryptography have the same session cryptography key. The initial chaining value is also used as input to the Data Encryption Standard (DES) algorithm to encipher or decipher data in a session with cryptography. Synonymous with *session seed.*

Initiate. A network services request, sent from an LU to an SSCP, requesting that an LU-LU session be established.

inline exit routine. In ACF/VTAM, a SYNAD or LERAD exit routine. Contrast with *asynchronous exit routine.*

INN. Deprecated term for *intermediate routing node (IRN).*

installation exit routine. In ACF/VTAM, a user-written exit routine that can perform functions related to initiation and termination of sessions and is run as part of ACF/VTAM rather than as part of an application program. Examples are the accounting, authorization, logon-interpret, and virtual route selection exit routines. Contrast with *application program exit routine.*

interconnected networks. SNA networks connected by gateways.

interconnection. See *SNA network interconnection.*

intermediate routing function. In SNA, a path control capability in a subarea node that receives and routes path information units (PIUs) that neither originate in nor are destined for network addressable units (NAUs) in the subarea node. Contrast with *boundary function.*

intermediate routing node (IRN). In SNA, a subarea node with intermediate routing function. A subarea node may be a boundary node, an intermediate routing node, both, or neither, depending on how it is used in the network.

intermediate SSCP. An SSCP along a session initiation path that owns neither of the LUs involved in a cross-network LU-to-LU session.

interpret table. In ACF/VTAM, an installation-defined correlation list that translates an argument into a string of eight characters. Interpret tables can be used to translate logon data into the name of an application program for which the logon is intended.

IRN. Intermediate routing node.

key-encrypting key. A key used in sessions with cryptography to encipher and decipher other keys. Contrast with *data encrypting key.*

large message performance enhancement outbound (LMPEO). In ACF/VTAM, a facility in which ACF/VTAM reformats function management (FM) data that exceeds the maximum request unit (RU) size (as specified in the BIND) into a chain or partial chain of RUs.

last-in-chain (LIC). A request unit whose request header (RH) end chain indicator is on and whose RH begin chain indicator is off. See also *RU chain.*

LERAD exit routine. A synchronous EXLST exit routine that is entered automatically when a logic error is detected.

LIC. Last-in-chain.

line. See *communication line.*

line control. Synonym for *data link control protocol.*

line group. One or more telecommunication lines of the same type that can be activated and deactivated as a unit.

link. In SNA, the combination of the link connection and the link stations joining network nodes; for example: (1) a System/370 channel and its associated protocols, (2) a serial-by-bit connection under the control of Synchronous Data Link Control (SDLC). Synonymous with *data link.*

> **Note:** A link connection is the physical medium of transmission; for example, a telephone wire or a microwave beam. A link includes the physical medium of transmission, the protocol, and associated communication devices and programming; it is both logical and physical.

link connection. In SNA, 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).

link level 2 test. See *link test.*

Link Problem Determination Aids. A set of test commands executed by a 3863, 3864, or 3865 modem or a 3867 Link Diagnostic Unit to determine which of various network components may be causing an error in the network.

link station. (1) In SNA, the combination of hardware and software that allows a node to attach to and provide control for a link. (2) In ACF/VTAM, a named resource within a subarea node representing another subarea node directly attached by a cross-subarea link. In the resource hierarchy, the link station is subordinate to the cross-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.

> **Note:** Three tests can be made; they differ in the resources that are dedicated during the test. A link test, level 0 requires a dedicated subarea node, link, and secondary link station. A link test, level 1 requires a dedicated link and secondary link station. A link test, level 2 requires only the dedicated link station.

link-attached. In ACF/VTAM, pertaining to devices that are physically connected by a telecommunication line. Synonymous with *remote.* Contrast with *channel-attached.*

link-attached communication controller. An IBM communication Controller that is attached to another communication controller by means of a link.

LMPEO. Large message performance enhancement outbound.

load module. (ISO) A program unit that is suitable for loading into main storage for execution; it is usually the output of a linkage editor.

local. Synonymous with *channel-attached.* Pertaining to a device that is attached to a controlling unit by cables, rather than by a telecommunication line.

local address. In SNA, an address used in a peripheral node in place of an SNA network address and transformed to or from an SNA network address by the boundary function in a subarea node.

local non-SNA major node. In ACF/VTAM, a major node whose minor nodes are channel-attached non-SNA terminals.

local session identification (LSID). In SNA, a field in a FID3 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).

local SNA major node. In ACF/VTAM, a major node whose minor nodes are channel-attached peripheral nodes.

log off. To request that a session be terminated.

log on. (1) To initiate a session. (2) In SNA products, to initiate a session between an application program and a logical unit.

logic error. In ACF/VTAM, an error condition that results from an invalid request; a program logic error.

logical unit (LU). In SNA, a port through which an end user accesses the SNA network in order to communicate with another end user and through which the end user accesses the functions provided by system services control points (SSCPs). An LU can support at least two sessions – one with an SSCP and one with another LU – and may be capable of supporting many sessions with other logical units. See also *network addressable unit (NAU), peripheral LU, physical unit, system services control point, primary logical unit,* and *secondary logical unit.* Contrast with *physical unit (PU).*

logical unit (LU) services. In SNA, capabilities in a logical unit to: (1) receive requests from an end user and, in turn, issue requests to the system services control point (SSCP) in order to perform the requested functions, typically for session initiation; (2) receive requests from the SSCP, for example to activate LU-LU sessions via Bind Session requests; and (3) provide session presentation and other services for LU-LU sessions. See also *physical unit (PU) services.*

logoff. In ACF/VTAM, an unformatted session-termination request.

logon. In ACF/VTAM, an unformatted session-initiation request for a session between two logical units. See *automatic logon* and *simulated logon.* See also *session-initiation request.*

logon data. In ACF/VTAM: (1) The user data portion of a field-formatted or unformatted session-initiation request. (2) The entire logon sequence or message from an LU. Synonymous with *logon message.*

logon message. Synonym for *logon data.*

logon mode. In ACF/VTAM, a subset of session parameters specified in a logon mode table for communication with a logical unit. See also *session parameters.*

logon mode table. In ACF/VTAM, a set of entries for one or more logon modes. Each logon mode is identified by a logon mode name.

logon-interpret routine. In ACF/VTAM, an installation exit routine, associated with an interpret table entry, that translates logon information. It may also verify the logon.

LPDA. Link Problem Determination Aids.

LSID. Local session identification.

LU. Logical unit.

LU connection test. In SNA products, a diagnostic aid that permits a terminal operator to check whether the path between a system services control point (SSCP) and a logical unit (LU) is operational.

LU type. In SNA, a deprecated term for *LU-LU session type.*

LU-LU session. In SNA, a session between two logical units in an SNA network. It provides communication between two end users, or between an end user and an LU services component.

LU-LU session type. In SNA, the classification of an LU-LU session in terms of the specific subset of SNA protocols and options supported by the logical units (LUs) for that session, namely:

> The mandatory and optional values allowed in the session activation request.
> The usage of data stream controls, FM headers, RU parameters, and sense codes.
> Presentation services protocols such as those associated with FM header usage.

LU-LU session types 0, 1, 2, 3, 4, 6, and 7 are defined.

> **Note:** At session activation, one LU-LU half-session selects the session type and includes or excludes optional protocols of the session type by sending the session activation request, and the other half-session concurs with the selection by sending a positive response or rejects the selection by sending a negative response. In LU-LU session types 4 and 6, the half-sessions may negotiate the optional parameters to be used. For the other session types, the primary half-session selects the optional protocols without negotiating with the secondary half-session.

main network address. In ACF/VTAM, the LU network address used for the SSCP-LU session and certain LU-LU sessions with the LU. Contrast with *auxiliary network address.*

mainline program. In ACF/VTAM, that part of the application program that issues OPEN and CLOSE macro instructions.

maintenance and operator subsystem (MOSS). A subsystem of the 3725 Communication Controller that contains a processor and operates independently of the rest of the controller. It loads and supervises the 3725, runs problem determination procedures, and assists in maintaining both hardware and software.

maintenance services. In SNA, one of the types of network services in system services control points (SSCPs) and physical units (PUs). Maintenance services provide facilities for testing links and nodes and for collecting and recording error information. See also *configuration services, management services, network services,* and *session services.*

major node. In ACF/VTAM, a set of minor nodes that can be activated and deactivated as a group. See *node* and *minor node.*

management services. In SNA, one of the types of network services in system services control points (SSCPs) and logical units (LUs). Management services forward requests for network data, such as error statistics, and deliver the data in reply. See also *configuration services, maintenance services, network services,* and *session services.*

mandatory cryptographic session. Synonym for *required cryptographic session.*

master cryptography key. In SNA, a cryptographic key used to encipher operational keys that will be used at a node.

maximum SSCP rerouting count. The maximum number of times a session initiation request will be rerouted to intermediate SSCPs before the request reaches the destination SSCP. This count is used to prevent endless rerouting of session initiation requests.

message. In ACF/VTAM, the amount of FM data transferred to ACF/VTAM by the application program with one SEND request.

message unit. In SNA, the unit of data processed by any layer; for example, a basic information unit (BIU), a path information unit (PIU), or a request/response unit (RU).

MIC. Middle-in-chain.

middle-in-chain (MIC). A request unit whose request header (RH) begin chain indicator and RH end chain indicator are both off. See also *RU chain.*

minor node. In ACF/VTAM, a uniquely-defined resource within a major node. See *node* and *major node.*

modem. (modulator-demodulator) A device that modulates and demodulates signals transmitted over data communication facilities.

MOSS. Maintenance and operator subsystem.

multiple-domain network. In SNA, a network with more than one system services control point (SSCP). Contrast with *single-domain network.*

multiple gateways. More than one gateway serving to connect the same two SNA networks for cross-network sessions.

multipoint link. A link or circuit interconnecting several link stations. Synonymous with multidrop line. Contrast with *point-to-point link.*

Multisystem Networking Facility. An optional feature of ACF/TCAM and ACF/VTAM Version 1 that permits these access methods, together with ACF/NCP, to control a multiple-domain network.

multithread application program. An ACF/VTAM application program that processes requests for more than one session concurrently. Contrast with *single-thread application program.*

name translation. In SNA network interconnection, converting logical unit names, logon mode table names, and class of service names used in one network into equivalent names to be used in another network. This function can be provided through NCCF and invoked by a gateway SSCP when necessary. See also *alias name.*

native network. The network attached to a gateway NCP and in which that NCP's resources reside.

NAU. Network addressable unit.

NC. Network control.

NCCF. Network Communications Control Facility.

NCP. Network control program.

NCP major node. In ACF/VTAM, a set of minor nodes representing resources, such as lines and peripheral nodes, controlled by a network control program. See *major node.*

negative polling limit. For a start-stop or BSC terminal, the maximum number of consecutive negative responses to polling that the communication controller accepts before suspending polling operations.

negative response. In SNA, a response indicating that a request did not arrive successfully or was not processed successfully by the receiver. Contrast with *positive response.* See *exception response.*

negotiable BIND. In SNA, a capability that allows two LU-LU half-sessions to negotiate the parameters of a session when the session is being activated.

network. (1) (TC97) An interconnected group of nodes. (2) In data processing, a user application network. See *path control network, public network, SNA network,* and *user application network.*

network address. In SNA, an address, consisting of subarea and element fields, that identifies a link, a link station, or a network addressable unit. Subarea nodes use network addresses; peripheral nodes use local addresses. The boundary function in the subarea node to which a peripheral node is attached transforms local addresses to network addresses and vice versa. See *local address.* See also *network name.*

network address translation. In SNA network interconnection, conversion of the network address assigned to a logical unit in one network into an address in an adjacent network. This function is provided by the gateway NCP that joins the two networks. See also *alias network address* and *real network address.*

network addressable unit (NAU). In SNA, a logical unit, a physical unit, or a system services control point. It is the origin or the destination of information transmitted by the path control network. See also *network name, network address,* and *path control network.*

> **Note:** Each NAU has a network address that represents it to the path control network. (LUs may have multiple addresses for parallel LU-LU sessions.) The path control network and the NAUs collectively constitute the SNA network.

Network Communications Control Facility (NCCF). An IBM program product consisting of a base for command processors that can monitor, control, and improve the operation of a network.

network configuration tables. The tables through which the system services control point (SSCP) interprets the network configuration.

network control (NC). In SNA, an RU category used for requests and responses exchanged between physical units (PUs) for such purposes as activating and deactivating explicit and virtual routes and sending load modules to adjacent peripheral nodes. See also *data flow control layer* and *session control.*

network control mode. The functions of a network control program that enable it to direct a communication controller to perform activities such as polling, device addressing, dialing, and answering. Contrast with *emulation mode.*

network control program (NCP). A program, generated by the user from a library of IBM-supplied modules, that controls the operation of a communication controller.

network control program generation. The process, performed in a host system, of assembling and link-editing a macro instruction program to produce a network control program.

network identifier (network ID). The network name defined to NCPs and hosts to indicate the name of the network in which they reside. It is unique across all communicating SNA networks.

Network Logical Data Manager (NLDM). An IBM program product that collects and correlates LU-to-LU session-related data and provides the user with online access to this information. It runs as an NCCF communication network management (CNM) application program.

network name. (1) In SNA, the symbolic identifier by which end users refer to a network addressable unit (NAU), a link, or a link station. See also *network address.* (2) In a multiple-domain network, the name of the APPL statement defining an ACF/VTAM application program is its network name and it must be unique across domains. Contrast with *ACB name.* See *uninterpreted name.*

network node. Synonym for *node.*

network operator. (1) A person or program responsible for controlling the operation of all or part of a network. (2) The person or program that controls all the domains in a multiple-domain network. Contrast with *domain operator.*

network operator console. A system console or terminal in the network from which an operator controls the network.

Network Problem Determination Application (NPDA). A program product that assists the user in identifying network problems from a central control point using interactive display techniques.

Network Routing Facility (NRF). An IBM program product that resides in the ACF/NCP, which provides a path for messages between terminals, and routes messages over this path without going through the host processor.

network services (NS). In SNA, the services within network addressable units (NAUs) that control network operation through SSCP-SSCP, SSCP-PU, and SSCP-LU sessions. See *configuration services, maintenance services, management services,* and *session services.*

network services (NS) header. In SNA, a 3-byte field in an 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 RU (for example, configuration services, session services) and the particular request code within a category.

Network Services Procedure Error (NSPE). A request unit that is sent by an SSCP to an LU when a procedure requested by that LU has failed.

Network Terminal Option (NTO). An IBM program product that extends the capabilities of the ACF/NCP to support a select group of non-SNA devices.

networking. In a multiple-domain network, communication among domains.

NIB. Node initialization block.

NIB list. A series of contiguous node initialization blocks.

NLDM. Network Logical Data Manager.

no response. In SNA, a value in the form-of-response-requested field of the request header (RH) indicating that no response is to be returned to the request, whether or not the request is received and processed successfully. Contrast with *definite response* and *exception response.*

node. (1) In SNA, an endpoint of a link or junction common to two or more links in a network. Nodes can be distributed to host processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities. (2) In ACF/VTAM, a point in a network defined by a symbolic name. Synonymous with *network node.* See *major node* and *minor node.*

node initialization block (NIB). In ACF/VTAM, a control block associated with a particular node or session that contains information used by the application program to identify the node or session and to indicate how communication requests on a session are to be handled by ACF/VTAM.

node name. In ACF/VTAM, the symbolic name assigned to a specific major or minor node during network definition.

node type. In SNA, a designation of a node according to the protocols it supports and the network addressable units (NAUs) that it can contain. Four types are defined: 1, 2, 4, and 5. Type 1 and type 2 nodes are also referred to as peripheral nodes and type 4 and type 5 nodes are also referred to as subarea nodes. See also *physical unit type.*

non-native network. Any network attached to a gateway NCP that does not contain that NCP's resources.

non-SNA terminal. A terminal that does not use SNA protocols.

nonswitched data link. A connection between a link-attached device and a communication controller that does not have to be established by dialing. Contrast with *switched data link.* See also *point-to-point data link* and *multipoint data link.*

nonswitched line. A telecommunication line on which connections do not have to be established by dialing. Contrast with *switched line.*

normal flow. In SNA, a data flow designated in the transmission header (TH) that is used primarily to carry end-user data. The rate at which requests flow on the normal flow can be regulated by session-level pacing. Contrast with *expedited 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 (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 the boundary functions.

Notify. A network services request unit that is sent by an SSCP to an LU to inform the LU of the status of a procedure requested by the LU.

NPDA. Network Problem Determination Application.

NRF. Network Routing Facility.

NS. Network services.

NSPE. Network Services Procedure Error.

NTO. Network Terminal Option.

OIC. Only-in-chain.

only-in-chain (OIC). A request unit who request header (RH) begin chain indicator and RH end chain indicator are both on. See also *RU chain.*

operator. * A person who operates a machine. See *network operator.*

orderly closedown. The orderly deactivation of ACF/VTAM and its domain. An orderly closedown does not complete until all application programs have closed their ACBs. Until then, RPL-based operations continue; however, no new sessions can be established and no new ACBs can be opened. Contrast with *cancel closedown* and *quick closedown.*

pacing. In SNA, a technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion. See *session-level pacing, send pacing,* and *virtual route (VR) pacing.* See also *flow control.*

pacing group. In SNA, (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. Synonymous with *window.* (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.

pacing group size. In SNA, (1) The number of path information units (PIUs) in a virtual route pacing group. The pacing group size varies according to traffic congestion along the virtual route. Synonymous with *window size.* (2) The number of requests in a session-level pacing group.

pacing response. In SNA, an indicator that signifies a receiving component's readiness 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.

page. The portion of a panel that is shown on a display surface at one time.

panel. In computer graphics, a predefined display image that defines the locations and characteristics of display fields on a display surface.

parallel links. In SNA, two or more links between adjacent subarea nodes.

parallel sessions. In SNA, two or more concurrently active sessions between the same two logical units (LUs) using different pairs of network addresses. Each session can have independent session parameters.

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. (1) In SNA, the series of path control network components (path control and data link control) that are traversed by the information exchanged between two network addressable units (NAUs). A path consists of a virtual route and its route extension, if any. See also *explicit route.* (2) In defining a switched major node, a potential dial-out port that can be used to reach a physical unit.

path control (PC) layer. In SNA, the layer that manages the sharing of link resources of the SNA network and routes basic information units (BIUs) through it. Path control routes message units between network addressable units (NAUs) in the network and provides the paths between them. It converts the BIUs from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units (BTUs) and one or more PIUs with data link control. See also *BIU segment, blocking of PIUs, data link control layer,* and *transmission control layer.*

> **Note:** The unit of control information built by the sending path control component is the transmission header (TH), attached to the BTU; the TH is interpreted by the receiving path control component. The path control layer in subarea nodes consists of explicit route control, transmission group control, virtual route control, and boundary function path control.

path control (PC) network. In SNA, the part of the SNA network that includes the data link control and path control layers. See *SNA network* and *user application network.* See also *boundary function.*

path information unit (PIU). In SNA, a message unit consisting of a transmission header (TH) alone, or of a TH followed by a basic information unit (BIU) or a BIU segment. See also *transmission header.*

path test. A test provided by NLDM Release 2 that enables a network operator to determine whether a path between two LUs that are currently in session is available.

PC. Path control.

pending active session. In ACF/VTAM, the state of an LU-LU session recorded by the SSCP when it finds both LUs available and has sent a CINIT request to the primary logical unit (PLU) of the requested session.

PEP. Partitioned emulation programming.

peripheral LU. In SNA, a logical unit representing a peripheral node.

peripheral node. In SNA, 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 is a type 1 or type 2 node connected to a subarea node.

peripheral PU. In SNA, a physical unit representing a peripheral node.

physical connection. In ACF/VTAM, a point-to-point connection or multipoint connection.

physical unit (PU). In SNA, one of three types of network addressable units (NAUs); each node of an SNA network contains a physical unit (PU) that manages and monitors the resources (such as attached links) of a node, as requested by an SSCP via an SSCP-PU session. See also *peripheral PU, physical unit type,* and *subarea PU.*

> **Note:** 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.

physical unit (PU) services. In SNA, the components within a physical unit (PU) that provide configuration services and maintenance services for SSCP-PU sessions. See also *logical unit (LU) services.*

physical unit type. In SNA, the classification of a physical unit (PU) according to the type of node in which it resides. The PU type is the same as its node type; that is, a type 1 PU resides in a type 1 node, and so forth.

PIU. Path information unit.

plaintext. Data that is not enciphered. Synonym for *clear data.*

PLU. Primary logical unit.

point-to-point link. A link that connects a single remote link station to a node; it may be either switched or nonswitched. Contrast with *multipoint link.*

polling. (1) * Interrogation of devices for purposes such as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (2) (TC97) The process whereby stations are invited, one at a time, to transmit.

positive response. A response indicating that a request was received and processed. Contrast with *negative response.*

primary application program. In ACF/VTAM, an application program acting as the primary end of an LU-LU session.

primary end of a session. The end of a session that uses primary protocols. The primary end establishes the session. For an LU-LU session, the primary end of the session is the primary logical unit. Contrast with *secondary end of a session.* See *half-session.*

primary half-session. In SNA, the half-session that sends the session activation request. See also *primary logical unit.* Contrast with *secondary half-session.*

primary logical unit (PLU). In SNA, the logical unit (LU) that contains the primary half-session for a particular LU-LU session. Contrast with *secondary logical unit.*

> **Note:** A particular logical unit may contain both primary and secondary half-sessions for different active LU-LU sessions.

problem determination. The process of identifying the source of a problem; for example, a program component, a machine failure, telecommunication facilities, user or contractor-installed programs or equipment, an environment failure such as a power loss, or a user error.

program operator. An ACF/VTAM application program that is authorized to issue ACF/VTAM operator commands and receive ACF/VTAM operator awareness messages. See also *solicited messages* and *unsolicited messages.*

protocol. (1) (CCITT/ITU) A specification for the format and relative timing of information exchanged between communicating parties. (2) (TC97) The set of rules governing the operation of functional units of a communication system that must be followed if communication is to be achieved. (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. See also *bracket protocol.* Synonymous with *line control discipline* and *line discipline.* See also *link protocol.*

PU. Physical unit.

PU type. Physical unit type.

public network. A network established and operated by communication common carriers or telecommunication Administrations for the specific purpose of providing circuit-switched, packet-switched, and leased-circuit services to the public. Contrast with *user-application network.*

PU-PU flow. In SNA, the exchange between physical units (PUs) of network control requests and responses.

queued BIND. In ACF/VTAM, a BIND request, sent from the primary logical unit (PLU) to the secondary logical unit (SLU), that has not yet been responded to by the SLU. This creates a pending active session at the SLU. When the SLU is an ACF/VTAM application program, it responds to a BIND by issuing an OPNSEC or SESSIONC macro instruction.

queued CINIT. In ACF/VTAM, a CINIT request, sent from an SSCP to an LU, that has not yet been responded to by the LU. This creates a pending active session at the LU. An ACF/VTAM application program responds to a CINIT by issuing an OPNDST ACCEPT or a CLSDST macro instruction.

queued session. In ACF/VTAM, pertaining to a requested LU-LU session that cannot be started because one of the LUs is not available. If the session-initiation request specified queuing, the SSCP(s) will record the request and later continue with the session-establishment procedure when both LUs become available.

quick closedown. In ACF/VTAM, a closedown in which any RPL-based communication macro instruction is terminated (posted complete with an error code) and no new sessions can be established and no new ACBs can be opened. See also *cancel closedown* and *orderly closedown.*

quiesce protocol. In ACF/VTAM, a method of communicating in one direction at a time. Either the primary logical unit (PLU) or the secondary logical unit (SLU) assumes the exclusive right to send normal-flow requests, and the other node refrains from sending such requests. When the sender wants to receive, it releases the other node from its quiesced state.

RDT. Resource definition table.

real network address. The address by which a logical unit is known within the SNA network in which it resides.

real name. The name by which a logical unit, logon mode table, or class of service table is known within the SNA network in which it resides.

receive pacing. In SNA, the pacing of message units that the component is receiving. See also *send pacing.*

record mode. In ACF/VTAM, the mode of data transfer in which the application program can communicate with logical units. Contrast with *basic mode.*

release. In ACF/VTAM resource control, to relinquish control of resources (communication controllers or physical units). See also *resource takeover.* Contrast with *acquire* (2).

remote. Synonym for *link-attached.*

request header. In SNA, a request unit (RU) header preceding a request unit.

request parameter list (RPL). In ACF/VTAM, a control block that contains the parameters necessary for processing a request for data transfer, for establishing or terminating a session, or for some other operation.

request unit (RU). In SNA, a message unit that contains control information such as a request code or FM headers, end-user data, or both.

request/response header (RH). In SNA, control information, preceding a request/response unit (RU), that specifies the type of RU (request unit or response unit) and contains control information associated with that RU.

request/response unit (RU). In SNA, a generic term for a request unit or a response unit.

required cryptographic session. A cryptographic session in which all outbound data is enciphered and all inbound data is deciphered. Synonymous with *mandatory cryptographic session.* Contrast with *selective cryptographic session* and *clear session.*

resource. Any facility of the computing system or operating system required by a job or task, and including main storage, input/output devices, the processing unit, data sets, and control or processing programs.

resource definition table (RDT). In ACF/VTAM, a table that describes the characteristics of each node available to ACF/VTAM and associates each node with a network address. This is the main ACF/VTAM network configuration table.

resource hierarchy. In ACF/VTAM, the relationship among network resources in which some resources are subordinate to others as a result of their position in the network structure and

architecture; for example, the LUs of a peripheral PU are subordinate to that PU, which, in turn, is subordinate to the link attaching it to its subarea node.

resource takeover. In ACF/VTAM, action initiated by a network operator to transfer control of resources from one domain to another. See also *acquire* (2) and *release.*

responded output. In ACF/VTAM, a type of output request that is completed when a response is returned. Contrast with *scheduled output.*

response header (RH). In SNA, 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. See also *negative response, pacing response,* and *positive response.*

response time. The amount of time that lapses between when a user presses the enter key at the terminal and when the reply to that request appears at the terminal.

response time monitor. A feature available with the 3274 control unit, for measuring response times.

response unit (RU). In SNA, 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), or if negative, contains sense data defining the exception condition.

REX. Route extension.

RH. Request/response header.

route. See *explicit route* and *virtual route.*

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 *path, explicit route (ER), virtual route (VR).*

Route Table Generator (RTG). An IBM-supplied field developed program that assists the user in generating path tables for SNA networks.

RPL. Request parameter list.

RPL exit routine. In ACF/VTAM, an application program exit routine whose address has been placed in the EXIT field of a request parameter list. ACF/VTAM invokes the routine to indicate that an asynchronous request has been completed. See *EXLST exit routine.*

RPL-based macro instruction. In ACF/VTAM, a macro instruction whose parameters are specified by the user in a request parameter list.

RTM. See response time monitor.

RU. Request/response unit.

RU chain. In SNA, a set of related request/response units (RUs) that are consecutively transmitted on a particular normal or expedited data flow. The request RU chain is the unit of recovery: if one of the RUs in the chain cannot be processed, the entire chain is discarded.

> **Note:** Each RU belongs to only one chain, which has a beginning and an end indicated via control bits in request/response headers within the RU chain. Each RU can be designated as first-in-chain (FIC), last-in-chain (LIC), middle-in-chain (MIC), or only-in-chain (OIC). Response units and expedited-flow request units are always sent as only-in-chain.

same-domain LU-LU session. In SNA, an LU-LU session between logical units (LUs) in the same domain. Contrast with *cross-domain LU-LU session.*

SC. Session control.

scanner interface trace (SIT). A record of the activity within the communication scanner processor (CSP) for a specified data link between a 3725 Communication Controller and a resource.

scheduled output. In ACF/VTAM, a type of output request that is completed, as far as the application program is concerned, when the program's output data area is free. Contrast with *responded output.*

SCS. SNA character string.

SDLC. Synchronous Data Link Control.

secondary application program. An application program acting as the secondary end of an LU-LU session.

secondary end of a session. That end of a session that uses secondary protocols. For an LU-LU session, the secondary end of the session is the secondary logical unit. Contrast with *primary end of a session.* See also *secondary logical unit* and *half-session.*

secondary half-session. In SNA, the half-session that receives the session-activation request. See also *secondary logical unit.* Contrast with *primary half-session.*

secondary logical unit (SLU). In SNA, the logical unit (LU) that contains the secondary half-session for a particular LU-LU session. Contrast with *primary logical unit.*

> **Note:** A logical unit may contain secondary and primary half-sessions for different active LU-LU sessions.

secondary logical unit (SLU) key. A key-encrypting key used to protect a session cryptography key during its transmission to the secondary half-session.

segmenting of BIUs. In SNA, an optional function of path control that divides a basic information unit (BIU) received from transmission control into two or more path information units (PIUs). The first PIU contains the request header (RH) of the BIU and usually part of the RU; the remaining PIU or PIUs contain the remaining parts of the RU.

> **Note:** When segmenting is not done, a PIU contains a complete BIU.

selective cryptographic session. A cryptographic session in which an application program is allowed to specify the request units to be enciphered. Contrast with *required cryptographic session* and *clear session.*

send pacing. In SNA, pacing of message units that a component is sending. See also *receive pacing.*

serial networks. A group of SNA networks connected in series by gateways.

session. In SNA, a logical connection between two network addressable units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. The session activation request and response can determine options relating to such things as the rate and concurrency of data exchange, the control of contention and error recovery, and the characteristics of the data stream. Sessions compete for network resources such as the links within the path control network. For routing purposes, each session is identified by the network or local addresses of the session partners. See *half-session, LU-LU session, SSCP-LU session, SSCP-PU session,* and *SSCP-SSCP session.* See also *LU-LU session type* and *PU-PU flow.*

> **Note:** Each session is uniquely identified in a transmission header (TH) by a pair of network addresses, identifying the origin and destination NAUs of any transmissions exchanged during the session.

session activation request. In SNA, a request that activates a session between two network addressable units (NAUs) and specifies session parameters that control various protocols during session activity; for example, BIND and ACTPU. Synonymous with *generic BIND.* Contrast with *session deactivation request.*

session address space. In ACF/VTAM, an ACB address space or an associated address space in which an OPNDST or OPNSEC macro instruction is issued to establish a session. See also *ACB address space* and *associated address space.*

session awareness data. Data relating to sessions that is collected by NLDM and that includes the session type, the names of session partners, and information about the session activation status. It is collected for LU-LU, SSCP-LU, SSCP-PU, and SSCP-SSCP sessions and for non-SNA terminals not supported by NTO.

session control (SC). In SNA, (1) 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. (2) An RU category used for requests and responses exchanged between the session control components of a session and for session activation/deactivation requests and responses.

session cryptography key. In SNA, a data encrypting key used to encipher and decipher function management data (FMD) requests transmitted in an LU-LU session that uses cryptography.

session data. Data relating to sessions that is collected by NLDM and that consists of session awareness data and session trace data.

session deactivation request. In SNA, a request that deactivates a session between two network addressable units (NAUs); for example, UNBIND and DACTPU. Synonymous with *generic UNBIND.* Contrast with *session activation request.*

session limit. (1) In SNA, the maximum number of concurrently active LU-LU sessions a particular logical unit can support.

> **Note:** ACF/VTAM application programs acting as logical units have no session limit. Device-type logical units have a session limit of one.

(2) In the network control program, the maximum number of concurrent line-scheduling sessions on a non-SDLC, multipoint line.

session management exit routine. An installation-supplied ACF/VTAM exit routine that performs authorization, accounting, and gateway path selection functions.

session parameters. In SNA, the parameters that specify or constrain the protocols (such as bracket protocol and pacing) for a session between two network addressable units. See also *logon mode.*

session partner. In SNA, one of the two network addressable units (NAUs) having an active session.

session seed. Synonym for *initial chaining value.*

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.*

session services. In SNA, one of the types of network services in the system services control point (SSCP) and in the logical unit (LU). These services provide facilities for an LU or a network operator to request that the SSCP initiate or terminate sessions between logical units. See *configuration services* and *maintenance services.*

session trace. In NLDM, the function that collects session trace data for sessions involving specified resource types or involving a specific resource.

session trace data. Data relating to sessions that is collected by NLDM whenever a session trace is started and that consists of session activation parameters, access method PIU data, and ACF/NCP data.

session-establishment macro instructions. In ACF/VTAM, the set of RPL-based macro instructions used to initiate, establish, or terminate LU-LU sessions.

session-establishment request. In ACF/VTAM, a request to an LU to establish a session. For the primary logical unit (PLU) of the requested session, the session-establishment request is the CINIT sent from the SSCP to the PLU. For the secondary logical unit (SLU) of the requested session, the session-establishment request is the BIND sent from the PLU to the SLU.

session-initiation request. In SNA, an Initiate or logon request from a logical unit (LU) to a system services control point (SSCP) that an LU-LU session be activated.

session-level pacing. In SNA, a flow control technique that permits a receiving connection point manager to control the data transfer rate (the rate at which it receives request units)

on the normal flow. It is used to prevent overloading a receiver with unprocessed requests when the sender can generate requests faster than the receiver can process them. See also *pacing* and *virtual route pacing.*

session-termination request. In ACF/VTAM, a request that an LU-LU session be terminated.

shadow resource. In ACF/VTAM, an alternate representation of a network resource that is retained as a definition for possible future use.

share limit. In SNA, the maximum number of control points that can concurrently control a network resource.

shared. Pertaining to the availability of a resource to more than one use at the same time.

shared-control gateway. A gateway consisting of one gateway NCP that is controlled by more than one gateway SSCP.

simple gateway. A gateway consisting of one gateway NCP and one gateway SSCP.

simulated logon. A session-initiation request generated when an ACF/VTAM application program issues a SIMLOGON macro instruction. The request specifies an LU with which the application program wants a session in which the requesting application program will act as the PLU.

single-domain network. In SNA, a network with one system services control point (SSCP). Contrast with *multiple-domain network.*

single-thread application program. An ACF/VTAM application program that processes requests for multiple sessions one at a time. Such a program usually requests synchronous operations from ACF/VTAM, waiting until each operation is completed before proceeding. Contrast with *multithread application program.*

SIT. Scanner interface trace.

SLU. Secondary logical unit.

SMF. System Management Facilities.

SNA. Systems Network Architecture.

SNA character string (SCS). A character string composed of EBCDIC controls, optionally intermixed with end-user data, that is carried within a request/response unit.

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 addressable units (NAUs), boundary function components, and the path control network.

SNA network interconnection. 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 terminal. A terminal that supports Systems Network Architecture protocols.

SNBU. Switched network backup.

solicited message. A response from ACF/VTAM to a command entered by a program operator. Contrast with *unsolicited message.*

specific-mode. In ACF/VTAM: (1) The form of a RECEIVE request that obtains input from one specific session. (2) The form of an accept request that completes the establishment of a session by accepting a specific queued CINIT request. Contrast with *any-mode.* See *continue-specific mode.*

SSCP. System services control point.

SSCP ID. In SNA, a number that uniquely identifies a system services control point (SSCP). The SSCP ID is used in session activation requests sent to physical units (PUs) and other SSCPs.

SSCP rerouting. In SNA network interconnection, the technique used by the gateway SSCP to send session-initiation RUs, by way of a series of SSCP-to-SSCP sessions, from one SSCP to another, until the owning SSCP is reached.

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-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.

SSCP-SSCP session. In SNA, a session between the system services control point (SSCP) in one domain and the SSCP in another domain. An SSCP-SSCP session is used to initiate and terminate cross-domain LU-LU sessions.

start option. In ACF/VTAM, a user-specified or IBM-supplied option that determines certain conditions that are to exist during the time an ACF/VTAM system is operating. Start options can be predefined or specified when ACF/VTAM is started.

start-stop transmission. (1) (TC97) Asynchronous transmission such that a group of signals representing a character is preceded by a start element and is followed by a stop element. (2) Asynchronous transmission in which a group of bits is preceded by a start bit that prepares the receiving mechanism for the reception and registration of a character and is followed by at least one stop bit that enables the receiving mechanism to come to an idle condition pending the 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, any attached peripheral nodes, and their associated resources. Within a subarea node, all network addressable units, 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. In SNA, 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.

subarea LU. In SNA, a logical unit in a subarea node. Contrast with *peripheral LU.*

subarea node. In SNA, a node that uses network addresses for routing and whose routing tables are therefore affected by changes in the configuration of the network. Subarea nodes can provide boundary function support for peripheral nodes. Type 4 and type 5 nodes are subarea nodes. See also *intermediate routing node, peripheral node,* and *node type.*

subarea PU. In SNA, a physical unit in a subarea node.

subarea/element address split. The division of a 16-bit network address into a subarea address and an element address.

switched line. A communication line in which the connection between the communication controller and a remote link station is established by dialing.

switched major node. In ACF/VTAM, a major node whose minor nodes are physical units and logical units attached by switched SDLC links.

switched network backup (SNBU). In ACF/VTAM, an optional facility that allows a user to specify, for certain types of PUs, a switched line to be used as an alternate path if the primary line becomes unavailable or unusable.

SYNAD exit routine. A synchronous EXLST exit routine that is entered when a physical error is detected.

Synchronous Data Link Control (SDLC). A discipline 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 or multipoint. SDLC conforms to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute and High-Level Data Link Control (HDLC) of the International Standards Organization.

synchronous operation. In ACF/VTAM, a communication, or other operation in which ACF/VTAM, after receiving the request for the operation, does not return control to the program until the operation is completed. Contrast with *asynchronous operation.*

synchronous request. In ACF/VTAM, a request for a synchronous operation. Contrast with *asynchronous request.*

System Management Facilities (SMF). A standard feature of OS/VS2 MVS that collects and records a variety of system and job-related information.

system services control point (SSCP). In SNA, a focal point within an SNA network for managing the configuration, coordinating network operator and problem determination requests, and providing directory support and other session services for end users of the network. Multiple SSCPs, cooperating as peers, 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 domain.

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.

> **Note:** The purpose of the layered structure of SNA is to allow the ultimate origins and destinations of information – that is, the end users – to be independent of, and unaffected by, the way in which the specific SNA network services and facilities used for information exchange are provided.

TC. Transmission control.

TCAS. Terminal Control Address Space.

telecommunication line. Any physical medium such as a wire or microwave beam, that is used to transmit data. Synonymous with *transmission line.*

terminal. A device, usually equipped with a keyboard and some kind of display, capable of sending and receiving information over a link.

terminal component. A separately-addressable part of a terminal that performs an input or output function, such as the display component of a keyboard-display device or a printer component of a keyboard-printer device.

Terminal Control Address Space (TCAS). The part of TSO/VTAM that provides logon services for TSO/VTAM users.

Terminate. In SNA, a request unit that is sent by an LU to its SSCP to cause the SSCP to start a procedure to end one or more designated LU-LU sessions.

TG. Transmission group.

TGID. Transmission group identifier.

TH. Transmission header.

transmission control character. Any control character used to control or facilitate transmission of data between data terminal equipment. Synonymous with *communication control character.*

transmission control (TC) layer. In SNA, the layer within a half-session that synchronizes and paces session-level data traffic, checks session sequence numbers of requests, and enciphers and deciphers end-user data. Transmission control has two components: the connection point manager and session control. See also *half-session.*

transmission group (TG). In SNA, a group of links between adjacent subarea nodes, appearing as a single logical link for routing of messages.

> **Note:** A transmission group may consist of one or more SDLC links (parallel links) or of a single System/370 channel.

transmission group identifier (TGID). In SNA, a set of three values, unique for each transmission group, consisting of the subarea addresses of the two adjacent nodes connected by the transmission group, and the transmission group number (1-255).

transmission header (TH). In SNA, 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 line. Synonym for telecommunication line.

transmission priority. In SNA, a rank assigned to a path information unit (PIU) that determines its precedence for being selected by the transmission group control component of path control for forwarding to the next subarea node of the route used by the PIU.

transmission services (TS) profile. In SNA, a specification in a session activation request (and optionally, in the responses) of transmission control (TC) protocols (such as session-level pacing and the usage of session-level requests) to be supported by a particular session. Each defined transmission services profile is identified by a number.

transmission subsystem component (TSC). The component of ACF/VTAM that comprises the transmission control, path control, and data link control layers of SNA.

TSC. Transmission subsystem component.

TSO/VTAM. Time Sharing Option for the Virtual Telecommunications Access Method.

TWX. Teletypewriter exchange service.

unformatted. In ACF/VTAM, pertaining to commands (such as LOGON or LOGOFF) entered by an end user and sent by a logical unit in character form. The character-coded command must be in the syntax defined in the user's unformatted system services definition table. Synonymous with *character-coded.* Contrast with *field-formatted.*

unformatted system services (USS). In SNA products, a system services control point (SSCP) facility that translates a character-coded request, such as a logon or logoff request into a field-formatted request for processing by formatted system services and translates field-formatted replies and responses into character-coded requests for processing by a logical unit. Contrast with *formatted system services.* See also *converted command.*

uninterpreted name. In SNA, a character string that an SSCP is able to convert into the network name of an LU.

> **Note:** Typically, an uninterpreted name is used in a logon or Initiate request from an SLU to identify the PLU with which the session is requested. The SSCP interprets the name into the network name of the PLU in order to set up the session. When the PLU eventually sends a BIND to the SLU, the BIND contains the original uninterpreted name.

unsolicited message. A message, from ACF/VTAM to a program operator, that is unrelated to any command entered by the program operator. Contrast with *solicited message.*

user. Anyone who requires the services of a computing system.

user correlator. A 4-byte value supplied to ACF/VTAM by an application program when certain macro instructions (such as REQSESS) are issued. It is returned to the application program when subsequent events occur (such as entry to a SCIP exit routine upon receipt of BIND) that result from the procedure started by the original macro instruction.

user exit queue. A structure built by ACF/VTAM that is used to serialize the execution of application program exit routines. Only one exit routine on each user exit queue can run at a time.

user-application network. A configuration of data processing products, such as processors, controllers, and terminals, established and operated by users for the purpose of data processing or information exchange, which may use services offered by communication common carriers or telecommunication Administrations. Contrast with *public network.*

USS. Unformatted system services.

virtual route (VR). In SNA, a logical connection (1) between two subarea nodes that is physically realized as a particular explicit route, or (2) that is contained wholly within a subarea node for intra-node 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.*

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 (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* and *session-level pacing.*

virtual route selection exit routine. In ACF/VTAM, an optional installation exit routine that modifies the list of virtual routes associated with a particular class of service before a route is selected for a requested LU-LU session.

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.

VR. Virtual route.

VRID. Virtual route identifier.

VSAM. Virtual storage access method.

VTAM Terminal I/O Coordinator (VTIOC). The part of TSO/VTAM that converts TSO TGET, TPUT, TPG, and terminal control macro instructions into SNA request units.

VTIOC. VTAM Terminal I/O Coordinator.

window. In SNA, synonym for *pacing group*.

window size. In SNA, synonym for *pacing group size*.

XID. A data link control command and response passed between adjacent nodes that allows the two nodes to exchange identification and other information necessary for operation over the data link.

Index

A

abstracts of publications
  ACF/NCP B-13
  ACF/SSP B-20
  ACF/VTAM B-2
  NCCF B-24
  NLDM B-28
access method publications B-31
ACF/NCP
  ACF/NCP
    BSC devices A-7
    start-stop devices A-8
  channel-attachment 2-8
  device support A-7
  dumps
    CSP 1-11, 2-21
    MOSS 1-11, 2-21
    NCP 1-11, 2-21
  dynamic storage display 2-22
  functions
    network maintenance 2-5, 2-19
    network operation 2-4, 2-13
    network performance 2-4, 2-16
    network recovery 2-5, 2-24
    network security 2-5, 2-26
    network structure 2-4, 2-6
    problem determination 2-5, 2-19
    session flow 2-4, 2-11
    summary of 2-3
  gateway 1-32, 2-10
  generation 2-4, 2-28
  monitor mode 2-10
  multiple, generating 2-29
  NCCF
    devices A-9
  Network Routing Facility supported 2-10
  non-SNA device support 2-10
  parallel SDLC links between 2-10
  PLU (Primary Logical Unit) in 2-10
  program summary D-1
  publications B-13
  requirements
    hardware 3-7
    programming 3-7
    storage 3-8
  storage display 2-22
  supported products
    BSC devices A-7
    SDLC devices A-7
    start-stop devices A-8
  takeover 2-25
  use of, summarized 1-2
ACF/SSP
  functions
    ACF/NCP generation 2-28
    communication controller assembler 2-29
    conditional assembly removal 2-29
    configuration report program 2-31
    dump utility 2-30
    dynamic dump utility 2-30
    loader utility 2-29
    summary of 2-28
    trace analysis program (ACF/TAP) 2-30
  program summary E-1
  publications B-20
  use of, summarized 1-3
ACF/TAP (trace analysis program) 1-12, 2-30
ACF/TCAM
  NCCF operator control extension 2-36
  publications B-31
ACF/VTAM
  ACF/VTAM
    program products A-6
  address control block address extension (ACF/NCP) 2-8
  adjacent networks 1-38
  adjacent SSCP sessions 2-11
  alias name translation facility (NCCF) 1-22, 1-33
  application programs
    enhancements 2-27
  application programs, converting 3-6
  ASCII-8 support under NCCF 2-35
  compatibility
    ACF/NCP 3-3
    ACF/VTAM application programs 3-3
    BTAM application programs 3-4
    cross-domain communication 3-5
    cross-network communication 3-6
    IBM programs 3-4
  conversion
    ACF/VTAM application programs 3-6
    BTAM application programs 3-6
  default selection 1-22
  displays 1-10, 2-15
  dynamic storage display 2-15
  functions
    application programs 2-3, 2-27
    network maintenance 2-2, 2-19
    network operation 2-2, 2-13
    network performance 2-2, 2-16
    network recovery 2-2, 2-24
    network security 2-3, 2-26
    network structure 2-2, 2-6
    problem determination 2-2, 2-19
    session flow 2-2, 2-11
    summary of 2-1
  NCP 2-2
  NLDM support
    session awareness data 2-15
    session trace data 2-24
  performance considerations 2-16
  processing time 2-18
  program summary C-1
  publications B-2
  requirements
    hardware 3-1
    programming 3-1
    storage 3-1
  storage use 2-18
  supported products
    communication controllers A-5
    devices A-1
    Network Terminal Option A-1
    program products A-6
  traces 1-12, 2-2, 2-5, 2-23
    ACF/VTAM and ACF/NCP 1-12
  tuning statistics 2-19
  use of, summarized 1-2
ACF/VTAM Version 2 Release 2
  functional enhancements over your current release
    application programming 2-27

configuration design 2-6
introduced 2-1
network flow control 2-11
network operations 2-13
network performance 2-16
network recovery 2-24
network security 2-26
problem determination 2-19
ACF/VTAME publications B-31
activating resources 1-6
adjacent networks 1-38
adjacent SSCP sessions 2-11
Advanced Communication Function for NCP 2-8
alias name translation 1-22, 1-33
alias name translation facility (NCCF) 2-35
alternate routes, example of 1-14
application programs 2-27
automatic logon 2-3
in general 2-3
migration considerations 3-3
application programs, converting 3-6
ASCII-8 support under NCCF 2-35
assembly removal, conditional 2-29
auditability under ACF/VTAM 3-7
automatic logon 2-3
availability, relationship to configuration

B

backup for failing hardware 1-12
block-handling routines 2-29
BTAM
application programs
compatibility 3-4
publications B-31
BTP, ACF/VTAM support for A-6

C

CDRM
function 2-11
introduced 1-22
CDRSC 1-22, 2-8
channel monitor mode 2-10
channel-attachment NCPs 2-8
channel-to-channel adapters 2-8
channel-to-channel attached hosts 2-8
CICS/MVS
NCCF control 1-9
CICS/VS
ACF/VTAM support for A-6
BTAM, use of 3-4
NCCF control through 2-36
CLIST 2-45
CLISTs (command lists) for NCCF 1-9, 1-12, 1-15, 2-32
CMC 1-22, 1-26, 1-34
CNM (Communication Network Management)
downstream load 2-8
functions 2-31
interface 2-21
CNM (Communications Network Management)
products supported by NCCF A-11
collect command 2-45
command list 2-45
command lists 1-9, 1-12, 1-15, 2-32
command processor (NCCF) 2-33
command processors (NCCF) 1-9
communication controller assembler 2-29
conditional assembly removal 2-29
communication management configuration 1-22, 1-26, 1-34
communication processor scanner 1-12
communication scanner processor 1-11
compatibility
ACF/NCP 3-8
ACF/TCAM 3-8
ACF/VTAM 3-4, 3-8
NCCF 3-10
NLDM 3-11
conditional assembly removal 2-29
configuration design 1-25
availability of resources 1-12
communication management configuration 1-26
ease of operation affected 1-15
intermediate routing nodes 1-26
multiple domain networks 1-25
performance affected by 1-13
configuration isolation 1-38
configuration report program 2-31
connecting ACF/NCPs, example 1-6
connectivity test
logical unit 2-22
NLDM 2-22
contact without ACTPU (channel-attachment ACF/NCP) 2-8
conversion
ACF/VTAM application programs 3-6
BTAM application programs 3-6
cross-domain
communicaion using NCCF 2-32
links 2-9
resource manager 1-22
sessions 2-11
cross-network sessions 2-11
cryptographic feature 2-26
cryptography publications B-30
CSP (communication scanner processor)
dump 1-11, 2-21
trace 1-12, 2-24
customizing NCCF 1-9, 2-33

D

data collection 2-40, 2-43
data display 2-46
data flow, factors that affect 1-7
data host enhancement (channel-attachment NCP) 2-8
data link
data rates 2-8
ownership, extended 2-8
data rates 2-8
data security
under ACF/VTAM 3-7
under NCCF 2-32
data services under NCCF 2-32
default ACF/VTAM selection 1-22, 1-33
default SSCP selection 1-34, 2-11
delayed configuration restart 3-2
device support
ACF/NCP A-7
SDLC devices A-7
ACF/VTAM A-1
NCCF A-9
access methods A-10
CNM program products A-11
NLDM A-11

TSO/VTAM A-1
disk log 2-38
DISOSS/370, ACF/VTAM support for A-6
display response time 1-10, 1-23
displays
ACF/VTAM 1-10, 2-15
NLDM help 2-46
NLDM lists 2-47
traces
NLDM 2-48
downstream load 2-8
downstream load utility (DSLU) 2-21, A-6
DSILGMOD requirement in NCCF 2-37
DSX (distributed system executive)
ACF/VTAM support for A-6
NCCF 2-37
dumps
ACF/NCP 1-11, 2-2, 2-5
CSP 1-11, 2-21
data set selection
ACF/NCP 2-21
dynamic 2-30
formatted 2-30
MOSS 1-11, 2-21
snapshot 2-23
unformatted 2-30
utility 2-30
3725 1-11, 2-21
dynamic ACF/NCP storage display 2-22
dynamic CDRSC 1-22, 2-8
dynamic CDRSC definition 2-17
Dynamic Cross-Domain Resource 2-8
dynamic dump utility 2-30
dynamic reconfiguration 2-15

E

emulation mode 2-30
Encrypt/Decrypt feature 2-3, 2-18, 2-26, 3-2
encryption 1-13, 1-35, 2-3, 2-18, 2-26, 3-2, B-30
error notification for inoperative routes 2-16, 2-23
evolution of libraries
ACF/NCP B-17
ACF/SSP B-17
ACF/VTAM B-8
NCCF B-26
exit routines
ACF/VTAM application programs 1-13
NCCF 1-9, 2-33
explicit route 2-13, 2-45
extended ACF/NCP connection 2-8
extended authorized receiver control 2-37
extended data link ownership 2-8

F

forced deactivation of links 2-15, 2-25
forced session termination 2-15, 2-25
FTP, ACF/VTAM support for A-6
functions
ACF/VTAM Version 2 Release 2
application programming 2-27
configuration design 2-6
introduced 2-1
network flow control 2-11
network operations 2-13
network performance 2-16
network recovery 2-24
network security 2-26
problem determination 2-19

G

gateway 1-32, 1-38
ACF/NCP 1-32, 2-10
ACF/VTAM 2-10
GDDM, ACF/VTAM support for A-6
generalized trace facility 2-30
GTF 2-30

H

hardware requirements
ACF/NCP 3-7
ACF/SSP 3-7
ACF/VTAM 3-1
NCCF 3-8
NLDM 3-10
requirements
hardware 3-10
programming 3-10
storage 3-10
high-speed link transmission 2-10
Host Command Facility
ACF/VTAM support for A-6
NCCF control of 2-37
host intermediate routing node 2-10
Host prep (8100/DPCX support) A-6

I

IDWS, ACF/VTAM support for A-6
IIPS/IIAS, ACF/VTAM support for A-6
IIS, ACF/VTAM support for A-6
IMR (intensive mode error recording) 2-22
IMS/VS
ACF/VTAM support for A-6
NCCF control 1-9, 2-36
Information Management, NCCF support for A-11
Information/System, ACF/VTAM support for A-6
initialization of NLDM 2-45
Intensive Mode Error Recording (IMR): 2-22
interconnected networks 1-31
example of 1-41
multiple-gateway configurations 1-36
network maintenance 1-34
network operation 1-33
network performance 1-34
network recovery 1-35
network security 1-35
network structure 1-32
problem determination 1-34
rationale for 1-31
session flow 1-32
single-gateway configuration 1-36
tandem configuration 1-38
intermediate routing nodes 1-25, 1-26
IRN 1-25, 1-26, 2-10
isolation, configuration 1-38

J

Japanese language 2-36
JES, ACF/VTAM support for A-6

K

Katakana translate table 2-36

L

lines
  ACF/NCP attached 2-4
  choosing 1-5
  port mapping to 2-22
link
  problem determination aid 2-22
link level 2 test 2-23
link problem determination aid 2-22
loader utility of ACF/SSP 2-29
log 2-38
logical unit connectivity test 2-22
logmode table requirement (NCCF) 2-37
logon
  authorization extension (NCCF) 2-36
  automatic 2-3
long-running command support (NCCF) 2-36
LU connectivity test 2-22

M

maintenance and operator subsystem dump 1-11, 2-21
maximum RU size 2-17
migration
  ACF/NCP 2-6
  ACF/VTAM 2-6
  NCCF 2-33
  NLDM 2-41
migration to new releases
  functional enhancements over your release
    application programming 2-27
    configuration design 2-6
    introduced 2-1
    network flow control 2-11
    network operations 2-13
    network performance 2-16
    network recovery 2-24
    network security 2-26
    problem determination 2-19
modulo 128 2-10
monitor mode
  channel 2-10
  SDLC 2-10
MOSS dump 1-11, 2-21
MSNF 2-10
MSNF (Multisystem Networking Facility)
  repackaging 2-10
  with Terminal Access Facility 2-37
multiple ACF/NCPs
  gateways, example 1-37
  generating 2-29
multiple data services tasks (NCCF) 2-36
multiple domain network 1-19
  configuration design 1-25
multiple routes 2-13
multiple-domain network
  example of 1-29
  network maintenance 1-24
  network operation 1-22
  network performance 1-23
  network recovery 1-24
  problem determination 1-24
multiple-domain networks
  network structure 1-19
multiple-gateway configurations 1-36
multiple-line input (NCCF) 2-37
Multisystem Networking Facility 2-10
  See also MSNF
mutiple-domain network
  session flow 1-21
MVS publications B-32
MVS/IDWS, ACF/VTAM support for A-6
MVS/OCCF
  ACF/VTAM support for A-6
  NCCF support for A-11
MVS/XA publications B-33

N

name translation facility of NCCF 1-22, 1-33, 2-35
NCCF (Network Communications Control Facility)
  functions
    available under specific access methods 3-9
    basic 2-32
    enhancements 2-33
    overview 2-39
    summary of 2-32
  requirements
    hardware requirements 3-8
    programming requirements 3-8
    storage requirements 3-8
NCCF command list 2-45
NCCF(Network Communications Control Facility)
  ACF/VTAM support for A-6
  alias name translation capability 1-22, 1-33, 2-35
  CLISTs 1-9, 1-15, 2-32, 2-33, 2-35
  CNM interface support 2-32
  command processors 1-9, 2-33
  commands 2-35
  compatibility 3-10
  customizing 1-9, 2-33
  data security and auditing 2-32
  data services 2-32
  exit routines 1-9, 2-33
  logmode requirement 2-37
  multiple-domain use of 1-22, 1-24, 2-32
  network operation, use of in 1-9, 1-22
  operation 2-38
  operator control 2-32, 2-36
  predefined definitions and JCL 2-38
  presentation services 2-36
  problem determination use of in 1-24
  problem determination, use of in 1-11
  program summary F-1
  publications B-24
  scope of commands 2-35
  screen modes 2-33
  single-domain use of 1-9
  span of control 1-23, 2-32
  subtasks 2-33
  supported products
    devices A-9
    program products 1-10
  Terminal Access Facility 1-9, 2-36, 2-37
  usability enhancements 2-37

use of summarized 1-3
Network Communications Control Facility 1-3
Network Control Program 1-2
network gateway 1-38
network maintenance
ACF/NCP functions for 2-5, 2-19
ACF/VTAM functions for 2-2, 2-19
interconnected networks 1-34
multiple-domain networks 1-24
single-domain networks 1-11
network operation
ACF/NCP functions for 2-4, 2-13
ACF/VTAM functions for 2-2, 2-13
configuration design related to 1-15
interconnected networks 1-33
multiple-domain network 1-22
single-domain networks 1-8
use of NCCF 1-9, 1-22
network performance
ACF/NCP functions for 2-4, 2-16
ACF/VTAM functions for 2-2, 2-16
configuration design relation to 1-13
dynamic CDRSC retention 2-17
interconnected networks 1-34
maximum RU size 2-17
multiple-domain networks 1-23
Network Performance Analyzer (NPA) 1-23, 2-17
Network Performance Analyzer(NPA) 1-10
processing time 2-18
single-domain networks 1-10
storage use 2-18
transmission group thresholds 2-19
tuning statistics (ACF/VTAM) 2-19
Network Performance Analyzer 1-10
Network Performance Analyzer (NPA) 1-23, 2-17
Network Problem Determination Application
See NPDA
network recovery
ACF/NCP functions for 2-5
ACF/NCP takeover 2-25
ACF/VTAM functions for 2-2
forced deactivation of links 2-25
forced session termination 2-25
interconnection networks 1-35
multiple-domain networks 1-24
session outage notification (SON) 2-19, 2-25
single-domain networks 1-12
SSCP restart 2-25
SSCP-to-SSCP resynchronization 2-25
Network Routing Facility (NRF) 2-10, A-6
network sectioning 1-38
network security
ACF/NCP activation 2-26
ACF/NCP functions for 2-5, 2-26
ACF/VTAM functions for 2-3, 2-26
Encrypt/Decrypt Feature (ACF/VTAM) 2-26
interconnected networks 1-35
NCCF functions for 2-32
session management exit routine 2-26
single-domain network 1-13
network structure 1-4
ACF/NCP functions for 2-4, 2-6
ACF/VTAM functions for 2-2, 2-6
interconnected networks 1-32
multiple-domain networks 1-19
single-domain networks 1-4
Network Terminal Option
See NTO
networks, adjacent 1-38
NLDM
session awareness data
ACF/VTAM support for 2-15
domain lists 2-47
line port address 2-47
most recent sessions list 2-47
NAU lists 2-47
route configuration 2-47
session configuration 2-47
transmission group information 2-48
session trace data
access method PIU data 2-48
ACF/VTAM support for 2-24
NCP data 2-48
session activation parameters 2-48
NLDM(Network Logical Data Manager)
ACF/NCP functions for 2-24
ACF/NCP support for 2-15, 2-24
ACF/VTAM functions for 2-24
ACF/VTAM support for 2-15, 2-24, A-6
compatibility 3-11
connectivity test 2-46
displays 2-45, 2-46
functions 2-40
interconnected networks 1-33, 1-34
migration 2-41
NCCF support for A-11
network operation 1-33
network security 1-35
problem determination 1-34
program products supported 2-40
program summary G-1
publications B-28
requirements
route test 2-16, 2-46
session awareness data 2-43, 2-46
session trace data 2-43, 2-48
session traces 2-48
supported products A-11
use of summarized 1-3, 2-40
VSAM data base 2-40, 2-43
non-SNA device support 3-3
non-SNA device support (ACF/NCP) 2-10, A-1
nonadjacent networks 1-38, 1-41
nondisruptive ACF/NCP takeover 2-25
nondisruptive SSCP restart 2-25
NPA (Network Performance Analyzer) 1-23, 2-17
NPA(Network Performance Analyzer) 1-10
NPDA
ACF/VTAM support for A-6
IMR (intensive mode error recording) records 2-22
LPDA used with 2-22
NCCF support for 2-32, A-11
performance monitoring 1-10
problem determination 1-11
publications B-31
NRF (Network Routing Facility) 2-10, A-6
NTO (Network Terminal Option)
ACF/VTAM support for A-6
NLDM session data for 2-40
non-SNA devices 2-10, 3-3, A-1
publications B-31

O

operation
  See network operation
operator commands
  ACF/VTAM 2-2
  modifying 2-16
  NCCF control of 1-9, 2-32
operator control (NCCF) 2-32, 2-36
operator messages
  modifying 2-16
  module names in 2-23
OS/VS publications B-32
ownership 1-19
  ACF/NCPs 1-19, 1-32, 2-9
  devices 1-19
  extended for data links 2-8
  gateway ACF/NCP resources 1-32

P

pacing
  route 1-8, 2-19
  session 1-8, 2-2, 2-4, 2-11, 2-28
parallel SCDLC links between ACF/NCPs 2-10
Partitioned Emulation Program
  See PEP (Partitioned Emulation Program) modules
path selection exit routines 2-13
PEP (Partitioned Emulation Program) modules
  loading 2-16
  NPA used with 2-18
performance
  See network performance
PF (program function) key
  NCCF support of 2-38
  NLDM display of settings 2-46
PLU support in an ACF/NCP 2-10
POI (programmed operator interface)
  application programs 3-4
  role in network operation 2-2
port
  address of station, NLDM display of 2-47
  mapped to line 2-22
  swapping 2-10
predefined definitions and JCL, NCCF 2-38
presentation services (NCCF) 2-36
primary logical unit support in an ACF/NCP 2-10
problem determination and network maintenance
  ACF/NCP functions for 2-5, 2-19
  ACF/VTAM functions for 2-2, 2-19
  CNM interface 2-21
  dumps 1-11, 2-21
  intensive mode error recording 2-22
  interconnected networks 1-34
  line-to-port mapping (ACF/NCP) 2-22
  link level 2 test 2-23
  logical unit connectivity test 2-22
  LPDA (link problem determination aid) 2-22
  multiple-domain networks 1-24
  NLDM connectivity test 2-22
  PTF numbers with module names 2-23
  route verification 2-23
  single-domain networks 1-11
  storage display (ACF/NCP) 2-22
  traces
program function key
  See PF (program function) key
program summary
  ACF/NCP D-1
  ACF/SSP E-1
  ACF/VTAM C-1
  NCCF F-1
  NLDM G-1
Programmable Store System Host Support,
  ACF/VTAM support for A-6
Programmed Cryptographic Facility 2-26, 3-2
programmed operation interface
  See POI (programmed operator interface)
programming requirements
  ACF/NCP 3-7
  ACF/SSP 3-7
  ACF/VTAM 3-1
  Encrypt/Decrypt Feature of ACF/VTAM 3-2
  NCCF 3-8
  NLDM 3-10
  TSO/VTAM 3-1
PTF numbers including module names 2-23
publications
  access methods B-31
  ACF/NCP B-13
  ACF/SSP B-20
  ACF/VTAM B-2
  cryptography B-30
  MVS B-32
  MVS/XA B-33
  NCCF B-24
  NLDM B-28
  NPDA B-31
  NTO B-31
  OS/VS B-32
  SNA B-30
  TSO and TSO/VTAM B-31

R

reconfiguration, dynamic 2-15
recovery (see also network recovery)
  ACF/NCP failures 2-3, 2-25
  ACF/VTAM capability 2-3
  host failures 2-3, 2-25
request size, maximum 2-17
response time activation 2-45
response time data 1-10, 1-33, 2-40, 2-43, 2-46
response time definition 2-45
response time measurement 2-45
Response Time Monitor 1-10, 2-40, 2-43
response time objectives 2-45
response time ranges 2-40, 2-45
response time summaries 2-46
response time trends 2-46
restart, SSCP 2-25
route pacing 1-8, 2-19
route verification 2-16, 2-23
routing node 1-8, 1-26, 1-27, 1-34
RU size, maximum 2-17

S

scope of commands (NCCF) 2-35
screen modes (NCCF) 2-33
SDLC link level 2 test 2-23
  traces
    ACF/VTAM and ACF/NCP 2-23
SDLC monitor mode 2-10
sectioned networks 1-38

security
See network security
session
concept of explained 1-7
cross-domain 2-11
cross-network 2-11
session awareness data (NLDM)
domain lists 2-47
most recent sessions list 2-47
NAU lists 2-47
route configuration 2-47
session configuration 2-47
transmission group information 2-48
session data (NLDM) 2-45
session flow
ACF/NCP functions for 2-4
ACF/VTAM functions for 2-2, 2-11
interconnected networks 1-32
multiple-domain networks 1-21
single-domain networks 1-7
session management exit routine
multiple gateway configurations 1-36
network security 1-35, 2-26
path selection 2-13
Session mapping 2-45
session outage notification (SON) 2-25
session pacing 1-8, 2-2, 2-4, 2-11, 2-28
session partners 1-33
session response time 2-46
session trace data (NLDM) 2-43
access method PIU data 2-48
ACF/NCP data 2-48
session activation parameters 2-48
sessions
cross-domain 2-11
cross-network 2-11
shared ownership 1-19, 1-20, 1-32, 2-9
single-domain networks
application programming 1-13
configuration design 1-13
example of 1-17
network maintenance 1-11
network operation 1-8
network performance 1-10
network recovery 1-12
network security 1-13
network structure
device types 1-5
owning network resources explained 1-6
subareas explained 1-6
problem determination 1-11
session flow 1-7
single-gateway configurations 1-36
SNA network interconnection (see also interconnected networks) 2-10
SNA transaction 2-43
SON (session outage notification) 2-25
span of NCCF operator control 1-9, 1-23, 2-32
SSCP restart 2-25
SSCP-to-SSCP resynchronization 2-25
SSP
See ACF/SSP
start procedures 1-8
start-stop link transmission enhancement 2-11
statistics, tuning 1-23
storage display (ACF/NCP) 2-22
storage requirements
ACF/NCP 3-7
ACF/VTAM 3-1
NCCF 3-8
NLDM 3-10
SSP/NCP 3-7
storage savings (NCCF) 2-36
subareas, concept of explained 1-6
subsystem sessions supported by the Terminal Access Facility 3-9
subtasks
NCCF 1-10
performance considerations 2-18
summary of functions
ACF/VTAM Version 2 Release 2
supported products
ACF/NCP
ACF/VTAM A-1
devices A-1
NCCF
NLDM A-11
TSO/VTAM, devices A-4
System Support Program
See ACF/SSP

T

TAF
See Terminal Access Facility (NCCF)
takeover of resources 1-24, 2-3
tandem configurations 1-38
tandem interconnected networks
adjacent 1-38
nonadjacent 1-38, 1-39
Terminal Access Facility (NCCF)
full-screen sessions 2-37
operator-control sessions 2-37
subsystem sessions supported by 1-9, 2-36
terminals
ACF/NCP support for A-7
ACF/VTAM support for A-1
NCCF support for A-9
TSO/VTAM support for A-4
Threshold Analysis and Remote Access Feature of NPDA
NCCF support for A-11
performance uses for 1-10
Time Sharing Option of ACF/VTAM
See TSO/VTAM
timed autowrap (NCCF) 2-38
timer-initiated commands (NCCF) 2-35
trace analysis program (ACF/TAP) 1-12, 2-30
traces 1-12, 2-2, 2-5, 2-23, 2-45
translating network names 1-22, 1-33, 2-35
transmission groups 2-11, 2-19, 2-24
transmission priorities 2-13
TSO
ACF/VTAM
communication controllers A-5
ACF/VTAM support for A-6
devices supported by A-4
NCCF control of 2-37
publications B-31
TSO/VTAM
programming requirements 3-1
publications B-31
tuning statistics 1-10, 1-23, 2-19

U

unformatted system services 3-4
usability enhancements 2-37

V

virtual route
  pacing 2-13, 2-19
  window size 2-13, 2-19
VS/APL, ACF/VTAM support for A-6
VSAM
  disk log 2-38
  encryption requirements 3-2
  NLDM data base 2-40, 2-43
VSPC, ACF/VTAM support for A-6

W

window size 2-13

3

3036 console allocation as a terminal 2-16
3600 Finance Communication System
  performance 1-10
3725
  CSP dump 1-11, 2-21
  high-speed link transmission 2-10
  modulo 128 2-10
  MOSS 1-11
  MOSS dump 2-21
  port swapping 2-10
  scanner interface trace 2-24
  start-stop link transmission 2-11

4

4700 Finance Communication System
  performance 1-10

Network Program Products

General Information

Order No. GC27-0657-1

READER'S COMMENT FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

What is your occupation? _____

Number of latest Newsletter associated with this publication. _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice.)

GC27-0657-1

Cut Along This Line

Reader's Comment Form

Please Do Not Staple

Fold and Tape

Fold and Tape

No Postage Necessary If Mailed In The United States

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N. Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Dept. E03
P. O. Box 12195
Research Triangle Park
North Carolina 27709

Fold and Tape

Fold and Tape

Please Do Not Staple

IBM®

Cut Along This Line

GC27-0657-1

Printed in U.S.A.

IBM