IBM

World Trade Systems Centers

COMMUNICATION NETWORK MANAGEMENT
CENTRAL SITE OPERATION

GG24-1558-0

IBM
World Trade
Systems
Center

Technical
Bulletin

COMMUNICATION NETWORK MANAGEMENT

Central Site Operation

Author:
Michael Masslow, IBM Germany

Project advisors:
Jose de Alarcon and Harold Liberty, Raleigh Systems Center

GG24-1558-0
October 1982

First Edition (October 1982)

Publications are not stocked at the address below. Requests for copies of 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:

Raleigh Systems Center
IBM Corporation (986/B622-3)
P.O.Box 12195
Research Triangle Park, N.C. 27709, USA

CONTENTS

LIST OF ILLUSTRATIONS

With the Multisystem Network Facility (MSNF) of SNA products it is possible to interconnect single-domain networks to more complex multi-domain networks. This document is intended to show how a multi-domain (multi-host) SNA network can be operated from a single control position. Within this, emphasis has been placed on the description of controlling remote sub-hosts from a central host. This paper describes the specialities of central operation and how they are managed by means of Communication Network Management products. It further shows samples of command lists, procedures, routines etc. as a help to introduce the concept of centralized network and system operation in an installation. Nevertheless, many of the products and procedures described here as tools to manage centralized operation are applicable in every SNA environment.

This document is one of a series of reports on Communication Network Management (CNM). Management, as defined for these papers, is a set of tools, procedures and approaches used to control a network. A list of the other CNM documents can be found in "Appendix D. World Trade System Center Technical Papers" on page 75. The list shows the title and the order number together with a short description of the content of each of the publications.

The descriptions in this document are based on the following software:

- MVS/JES2 as the operating system for a central host and sub-host(s)
- ACF/VTAM Version 2
- ACF/NCP Release 3

The reader may adapt the descriptions to configurations containing MVS/JES3 systems if he considers that MVS/OCCF is not supported in MVS/JES3. DOS/VSE is not mentioned here because central control of MVS - DOS/VSE and DOS/VSE - DOS/VSE configurations is already described in the document 'Communication Network Management / Managing Interconnected Systems', GG24-1539.

This document is structured to first give an overview on central operation. It then covers

- System and network control
- System and network activation
- Failure and recovery

in three different chapters. The CNM products

- NCCF (Network Communication Control Facility)
- NCCF/TAF (Terminal Acces Facility)
- NPDA (Network Problem Determination Application)
- MVS/OCCF (Operator Communications Control Facility)
- SOF (Ssecondary Operator Facility)
- NPA (Network Performance Analizer)
- HCF(Host Control Facility)
- INFO/System (Information System V2) Which includes INFO/MVS and INFO/Management

are described in the last chapter. Readers who are familiar with these products can skip this chapter. Other readers should read it after the next chapter so as to understand the rest of the document.

It is expected that the reader has reasonable knowledge about SNA network operation. Certain areas will be reviewed in more or less detail although they do not solely refer to central control of multi-host networks. This is done to show a more complete picture of central network and system control rather then to provide an SNA operation education.

Note: A translation list for the acronyms and abbreviations used throughout the text can be found in "Appendix E. Acronyms and abbreviations" on page 77.

The ability to consolidate the operation of multiple processors at a single point of control has been a requirement for several years. For locally attached processors, this requirement was recognized e.g. by the operating subsystem JES3 which allows an installation to manage several processors as a unity and to divide operator control by processor functions rather than by processors.

For distributed processors attached to each other via data communication lines, the same requirements exist together with the requirement of central control on the network. Tools and techniques are available to accomplish central control of an SNA network and distributed hosts with today's hardware and software. This paper provides some information describing how all this works together and what constraints can be expected. Some topics described here may be already standard, as some installations whose host processors and communication controllers are locally attached to each other via channels have already realized centralized control of their network. Other facilities described, such as ROCF and MVS/OCCF, make it possible to bring remotely located MVS processors under central control.

The reasons for central control of a network and distributed host processors could be e.g.:

- Make operation, maintenance, and coordination more manageable
- Provide better service for the end users
- Reduce costs

All these may apply to many installations but central control only works in configurations up to a certain size. For size you may consider here the computer power of a single location as well as the extension of the network or the distance between the locations. It would be certainly ridiculous to control a data center with several CPUs, lots of tape drives, MSS, IBM 3800 printers, and so on from a remote data center similarly equipped. Central control of a network and host processors should be treated as an option rather than a compulsion for multi-host networks. If large data centers share a common SNA network, each data center can be responsible for a part of the network and may control sub-hosts, thus forming central control.

On the other hand, there are no restrictions which apply to a special environment. The design of SNA allows central network control and it depends on the application of hardware and software products as to how much central control can be achieved and how it is facilitated. It is mentioned throughout this paper where a special hardware unit or configuration has advantages or creates additional constraints but there are no hardware or configuration recommendations made here.

Before we have a look at the software products needed for central operation of a multiple host environment, we still should have a look at two general types of configurations. The first one is a multi-host configuration where all host processors are at a single location and somehow channel attached to each other; like the configuration shown in Figure 1 on page 4 **without** the two sub-hosts at the bottom. Such an environment can be centrally operated by the well known standard software and even without NCCF. The possibilities with the powerful system message routing facilities of MVS and e.g. JES3 are numerous. It is possible to separate network related messages from other messages and concentrate these messages from all hosts to a single console.

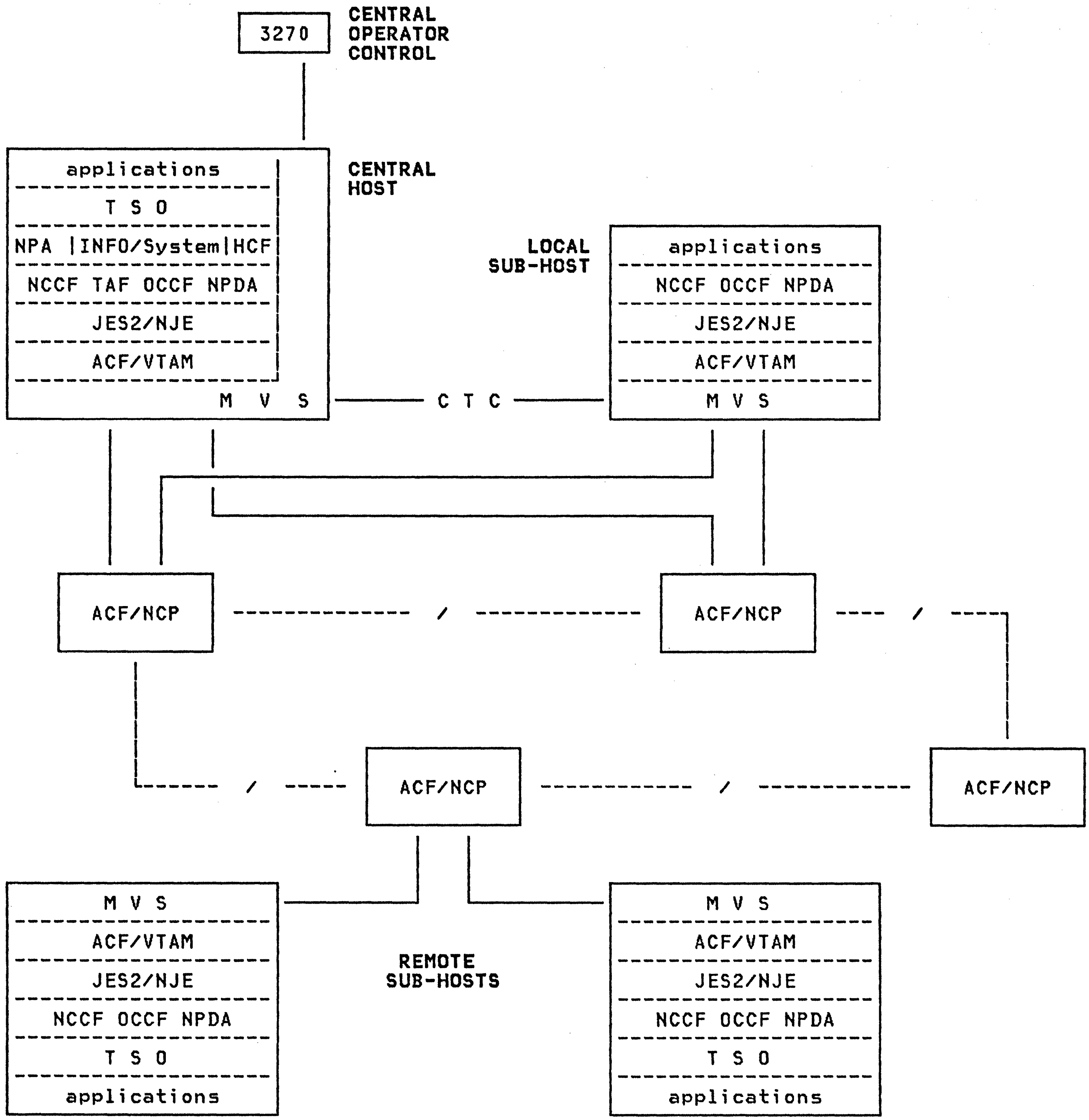


Figure 1. Sample of a centrally controlled configuration

The second type of configuration contains remote sub-hosts as in Figure 1 on page 4 (now the complete picture). Within this configuration it is still possible to centrally control the network to a certain degree with the basic software. For example, all terminals in the network which are attached to an IBM 3705 can be controlled from one host. But VTAM on the sub-hosts is also part of the network and these remote VTAMs control applications and locally attached terminals and have channel attached IBM 3705 controllers as ports to the network. VTAM on a remote sub-host has to be operated from the central site to fully achieve central network control and for that the standard operating systems are not sufficient. Additional tools, which are in general called Communication Network Management (CNM) products, have to be used to provide for the desired operability. These products are presented in the following list in an arbitrarily chosen classification. This is to show which products are mandatory to achieve a certain level of central control of a sub-host and which provide additional functions used to improve system and network management.

1. **Central network operation**

   NCCF — provides for remote console support for VTAM. Messages can be received from a remote VTAM. Commands can be issued for a remote VTAM.

2. **Central operation of remote sub-hosts after activation**

   MVS/OCCF — provides for remote MVS console support beyond VTAM. System messages can be received from a remote MVS. System commands can be issued for a remote MVS.

3. **Central operation of remote sub-hosts**

   ROCF — is a hardware feature in the IBM 4300 processor which is supported by MVS/OCCF. It facilitates a remote system console including remote IML/IPL.

4. **Supplementary products**

   NCCF/TAF — is a terminal simulator program. It allows a user to logon to and control subsystems like CICS/VS, IMS/VS, and IBM 8100 from an NCCF terminal.
   NPDA — assists in network and system problem determination for a local or remote domain.
   SOF — is used to simplify and automate MVS console operation. Most of the SOF functions are now included in MVS/OCCF.
   NPA — collects and displays network performance data from an NCP.
   HCF — allows access and control of IBM 8100 subsystems from an IBM /370 processor
   INFO — provides support for Problem/Change/Configuration Management.

You may now wish to review Figure 1 on page 4 to see the location of the software products which are dealt with in this book. Here, MVS/JES2, ACF/VTAM, and ACF/NCP are the base products for central network operation and NCCF and MVS/OCCF are the mandatory products to control remote sub-hosts. All of them must be available in every centrally operated processor in the network.

One of the prerequisites for introducing central network control in a real environment is the definition of a network wide convention for the naming of network nodes. Maintenance and operation of a network can be drastically simplified by a carefully chosen naming convention. Network names should be short, simple, and expressive to assist the network operator in his daily work.

The planning and preparation to centrally control an SNA network and the processors in the network is very much installation dependent and may include

- installation of the required software

- rearrangement of routes between subareas
- changes in the hardware area
- rearrangement of backup capabilities

The introduction of central control after the general planning should then be a step by step approach. One of these steps can be e.g. the activation of a sub-host from the central site or achieving control over a single 3705 or a single application. If the prerequisites for one step are provided, the central control should be practiced over a certain period before the responsibility for the subject of that step is fully handed over to the central site.

Moving data around the network becomes an important task in a centrally operated network. A decentralized multi-site environment, where each site controls its own network part, can be organized so that only information about cross-domain resources and VTAM and NCP PATH definitions have to be exchanged between locations. But in a centralized network with remote sub-hosts, the necessity for exchanging maintenance data grows. For example, when an IBM 3705 is loaded via VTAM through a sub-host's channel and the NCP is activated afterwards from a central host through a cross-subarea link, then the NCP definitions have to be available at both hosts. The maintenance of the network which consists of items like

- Keeping the members of the VTAMLST data set up to date
- Keeping the NCP load modules up to date
- Keeping VTAM exit routines, USSTABs, MODETABs, etc. up to date
- Sending VTAM and NCP dumps to the maintenance location
- Sending trace data to the maintenance location
- Applying fixes to the system components
- Keeping operator information up to date
- Collecting error records at the maintenance location
- Collecting performance records at the maintenance location

has to be carefully considered in planning for a centrally operated network. It is however not the purpose of this paper to address this area in further detail. The reader should refer to the documentation of data transfer products like

- JES2/NJE and
- Cross-Domain Network Data Transfer (CDNDT) FDP, Program Number 5798-DAE

for planning purposes.

NETWORK CONTROL

The tendency to concentrate communication network management to one point of control is stimulated by the fact that an active network does not need much operational effort as long as the network is working well. Most of network operations are related to recovery or problem determination. On the other hand, network monitoring becomes more important. To provide the required availability, it is important to quickly detect and respond to any abnormal situation in the network. VTAM or communication network management tools rather than the end user should tell the operator that there is something wrong in the network. NPA and NPDA Version 2 have standard facilities to alert operators of situations deviating from normal. These facilities are really useful because information of vital importance can be directed to the operator's attention.

SYSTEM CONTROL

Newly available products like MVS/OCCF make central control of remote hosts possible. Thus the central operator's responsibility in the scope of operation and monitoring can be expanded to comprise all components of the whole network as well as systems, subsystems, and applications. Controlling sub-hosts at remote locations require additional techniques and tools in comparison to those required for decentralized operation where the system components are within the operator's reach. Products like NCCF and OCCF which are valuable tools in all communication network environments become mandatory for centralized operation and monitoring.

By concentrating operational possibilities at the central site, many sub-hosts may not require a data processing skilled operator at the remote site. It is important in order to further reduce operational requirements at the remote site, to transfer monitoring of a sub-host to the central host. Monitoring is a permanent task to ensure that everything is alive and well. Care can be taken of the sub-host by people who are not dedicated to that job only if the sub-host is monitored by the central operator or automatically by itself. However, depending on the constraints of an installation, there are still more or less operator actions inevitably to be done at the remote site.

The following sections within this chapter are mainly organized by the tools which support the operator in his daily work:

N C C F

NCCF is a VTAM application program used to control an SNA network. At least VTAM itself, NCCF, and one NCCF display terminal have to be active and the network operator has to logon to NCCF as an NCCF user with the correct password, before the network can be operated through NCCF. An NCCF user can logon cross-domain to an NCCF in another host from a terminal which is already in session with NCCF. This establishes an NCCF to NCCF session and allows communication with multiple NCCFs simultaneously from one NCCF terminal (see Figure 18 on page 45 for a sample display).

At first sight network operation using NCCF is not very much different from using native MVS console support and routing all VTAM messages to a specific console. You can issue the same VTAM commands

```
D NET,....
V NET,....
F NET,....
```

and you will get the same VTAM messages on your NCCF terminal as on an MVS system console. But NCCF is more. It has a variety of functions (described in "Network Communications Control Facility (NCCF) Release 2" on page 45), which provide a program base for communication network management. Central operating of a multi-host environment can hardly be done without NCCF and products like OCCF, TAF, and INFO/System supplying capabilities beyond pure network operations. The central operator mainly uses NCCF and its related products to monitor and control the communication network and systems, subsystems, and applications at the remote site.

Although NCCF can be used right after installation, some additional effort is necessary to take full advantage of the capabilities offered by the product. This is primarily writing command lists for simplifying network operations and assigning PF keys to functions used most often. Further customization can be done by writing customized command processors or exit routines.

NCCF's PF key assignment is static for the duration of an NCCF run and you have to write an exit routine to make PF key assignment to CLISTs possible. The implementation of the CLIST capability is more flexible. It is possible to add new CLISTs or modify existing CLISTs and use those CLISTs without restarting NCCF. Here is an example of a very simple CLIST just to illustrate how easy operator input can be simplified. The one statement CLIST

```
V NET,ACT,ID=&1,SCOPE=ALL
```

is stored as a member called 'ACT' into the NCCF data set with DD-name DSICLD. The CLIST is invoked when the NCCF operator enters for instance

```
ACT L14025
```

and is then executed as the VTAM command

```
V NET,ACT,ID=L14025,SCOPE=ALL
```

Further CLISTs are discussed in section "CLISTs" on page 13. The reader may also refer to a paper called 'CNM Customizing NCCF, GG24-1554' as a supplement to the NCCF customization manual.

Controlling a multi-host environment can all be done from a single NCCF terminal. The central operator can

- control the network by issuing VTAM or NCCF commands, invoking NCCF CLISTs or user written command processors, receiving unsolicited messages
- access system consoles via NCCF to OCCF sessions
- access CICS/VS or IMS/VS as a master terminal operator via TAF
- access IBM 8100/DPPX or IBM 8100/DPCX subsystems via TAF and HCF
- do problem determination by NPDA
- do problem management by INFO/Management
- monitor system and network exceptions by the NPDA Alert Dynamic Display

It is clear that a central operator in a medium-sized or large environment is liable to be swamped by messages trying to handle all this on only one screen. Separating some of the functions described above to different NCCF terminals could be necessary. The next figure shows a sample of a possible multiple NCCF console configuration.

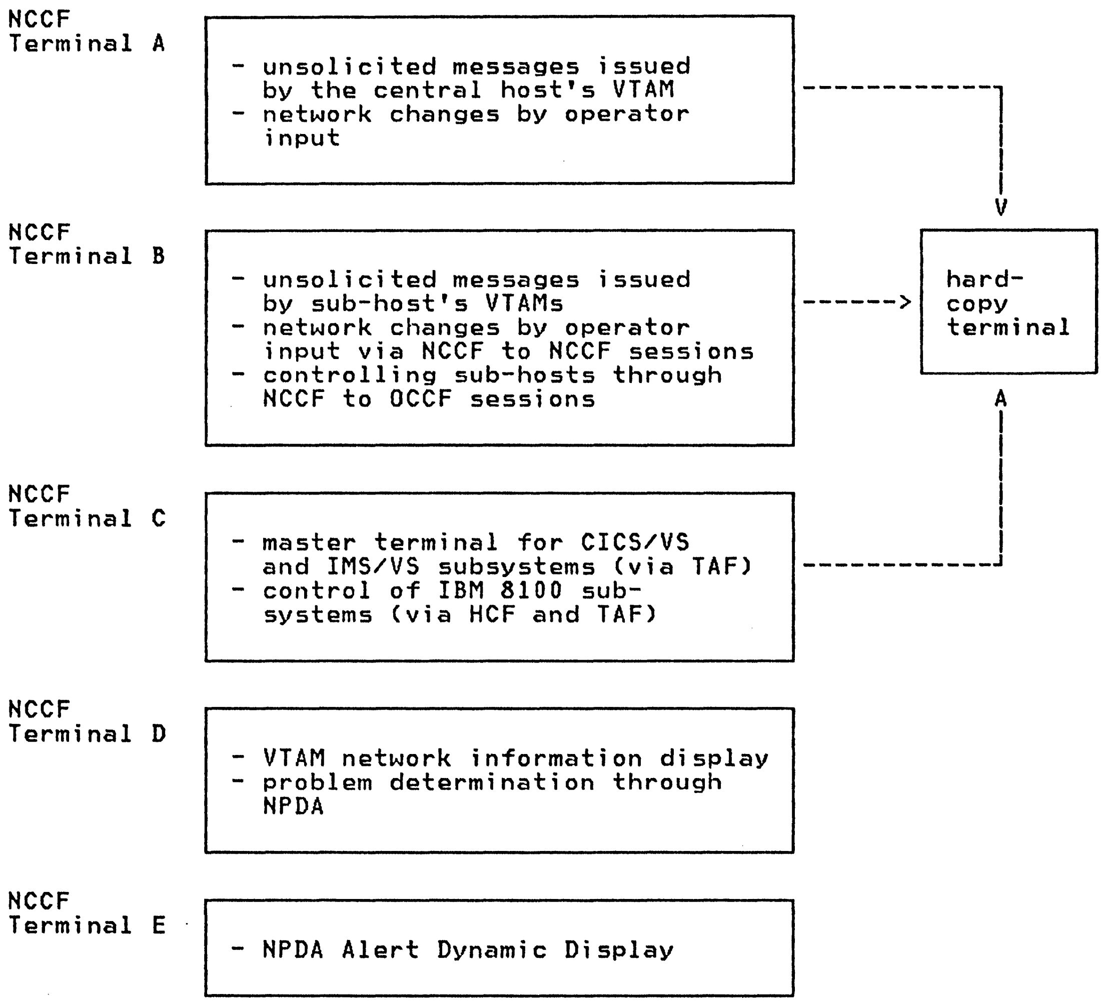


Figure 2. Multiple NCCF consoles

To plan for a multiple NCCF console configuration for central network and system control you need to understand NCCF's message routing capabilities. You also have to take into consideration that some functions need an application to application session setup before you can use them and that products like NPDA and OCCF make use of NCCF to NCCF sessions. The following hints give you some information in this area:

- Any kind of messages which respond to a terminal input are routed back to the terminal where the input was entered.

- Messages generated by VTAM as a result of an unrequested change in the network are called unsolicited messages. VTAM deliverers them to NCCF as they would go to the system console when NCCF is not active. In a multi-domain network they comprise messages relating to same-subarea and cross-subarea components depending on VTAM's ownership. NCCF delivers unsolicited messages to only one NCCF terminal and when they are scrolled off the screen they cannot be recalled. It is a problem to make NCCF route these messages to the terminal of your choice. You can find a rather complex diagram in the 'NCCF Terminal Use' manual about unsolicited message routing but it does not tell you all you have to know. Unsolicited messages routing in NCCF is dependant on things like: operator authorization, sequence of terminal definition in NCCF, sequence of logon to NCCF, etc. In some cases for instance, the first operator who logs on to NCCF gets all the unsolicited messages. It is fairly important especially for the NCCF to NCCF sessions (logon cross-domain to NCCF) that organizational arrangements are made for the logon sequence to make sure that unsolicited messages appear at the terminal you want.

- A network can be divided in a way that an NCCF operator can control a subset of the network resources. So, distribution of unsolicited messages to different NCCF terminals can be achieved depending on network resource names. For that you have to add the SPAN parameter to all major and minor node definitions in VTAM and the NCP deck(s) which belong to such a subset.

- A NCCF operator can logon cross-domain to an NCCF on another host. He can do this either from a dedicated terminal or from a terminal which is already in session with an NCCF (this is probably the more common way). If the operator is in session with more than one NCCF, the messages from different hosts are intermixed but they can be related to a particular host by their message prefix. For NCCF cross-domain message routing, the rules described earlier apply.

- Errors recorded by NPDA relate to components which are owned by the host where NPDA is running on. This means that in a centrally controlled multi-domain environment most errors are recorded in the data base of the central host and can be viewed from a terminal logged on same-domain to NCCF. NPDA viewing filters can provide a means of message routing. For instance, NPDA Alert Dynamic Displays can be set up for subsets of the network by specifying different sets of viewing filters for every NPDA Alert Dynamic Display screen (see "NPDA Version 2" on page 16 for more information about NPDA).

- If NPDA is also available on a sub-host, errors of local hardware or shared ownership resources, such as NCPs, are recorded at the sub-hosts NPDA data base. To view such data, an NPDA to NPDA cross-domain session can be established from the central host. For NCCF multiple console configuration considerations it is noted that such a session uses an existing NCCF to NCCF session.

- NCCF to OCCF cross-domain sessions can be established in two ways:

  - Logon cross-domain to NCCF from a dedicated terminal and then establish a same-domain NCCF to OCCF session.

  - Use an existing NCCF to NCCF cross domain session which is probably the more sensible way.

- TAF does not require any special multiple console considerations. TAF uses its own sessions to supply access to other applications. Provided the NCCF user has the proper authorization, TAF can be used from any NCCF terminal.

MVS/OCCF

MVS/OCCF has basically three functions which are nearly independent from each other:

1. **Simplify system operation** by CLISTs and automatic message replies. These facilities are independent of any communication access methods and can be used in any MVS/JES2 system.

2. Allow **remote operations** of an MVS/JES2 system through an NCCF to NCCF session. This function can be used in conjunction with the facilities described above and allows the monitoring and control of remote systems.

3. **Support ROCF**, a feature of IBM 4300 processors. ROCF allows an IBM 4300 processor to be remote operated and IPLed by an IBM BSC 3275 terminal through a switched line. OCCF can be used to simulate the IBM 3275 and thus make it unnecessary to install a IBM 3275 and a BSC line that requires Emulation Program (see section " Activation of a remote IBM 4300 by ROCF and MVS/OCCF" on page 26 for more information).

The first two facilities provide essential functions required for remote MVS/JES2 system operation while the third is an indispensable capability in running unattended remote sub-hosts.

Remote operations of an MVS/JES2 system are achieved in OCCF by logically transferring the system console from one host to another. This is the key facility to monitor and control remote sub-hosts and its usage is simple. The central operator logs on through an existing NCCF to NCCF session to an active OCCF in a sub-host. He is than able to communicate with the MVS system as an MVS operator (see Figure 3, Figure 4 on page 12, and Figure 5 on page 12).

```
 NETWORK COMMUNICATIONS CONTROL FACILITY                          09/27/82 12:37:34 A
 * NCF10    SDOM NCF11
 - NCF10    DSI033I NCF11    SESSION STARTING FOR NETOP
 C NCF10    PLEASE PRECEED REPLY TO PASSWORD WITH ?.
 - NCF11    DSI809A PLEASE ROUTE OPID,PASSWORD,PROFILE,HARDCOPY,INITIALCMD
 - NCF11    DSI810I NCCF ACF/VTAM READY
 - NCF11    DSI020I OPERATOR NETOP    LOGGED ON FROM TERMINAL NCF10001 USING
            PROFILE(PROFGLOB),HCL(        )
 * NCF11    LOGONX
 - NCF11    DSI810I NCCF ACF/VTAM READY
 | NCF11    DSI082I AUTOWRAP STARTED
 C NCF11    You have CTL=GLOBAL and MSGRECVR=YES for your session.
 C NCF11    Enter LOG/LOGOFF to terminate session.
 C NCF11    Enter HELP, PFK1 OR PFK13 FOR HELP.
 C NCF11    Enter  NOTES  for system messages.
 * NCF10    OCF11 %QLOGON    <=== invokation of user provided CLIST which issues
  C NCF10    ROUTE NCF11,OCCF %QLOGON                              <===  this command
 - NCF11    DSI810I NCCF ACF/VTAM READY
  E NCF11 STC 480 CBF029I QLOGON ACCEPTED FOR NCCF OPERATOR NETOP
  E NCF11 STC 480 CBF038I MVS/OCCF HAS BEEN QSTARTED FOR REPLY

???

cf11 d r,1
_
```

Figure 3. MVS/OCCF output on an NCCF screen: The operator logs on to an OCCF by routing the command 'OCCF %QLOGON' to one host's NCCF (Note that % and the character sequence OCCF are user chosen). He can then monitor and control the host from his NCCF terminal by receiving system messages, issuing commands or invoking OCCF CLISTs. System messages are intermixed with other NCCF output and can be related to a specific host by the NCCF provided prefix (NCF11 and NCF21).

```
 NETWORK COMMUNICATIONS CONTROL FACILITY                     09/27/82 12:38:17 A
          IEE112I 12.37.27 PENDING REQUESTS 769                          (NCF11    )
 RM=3   IM=2     EM=1      RU=0     IR=0     AMRF
 ID:R/K T MESSAGE TEXT
     03 R r03 ADM2000 I TO TERMINATE ADMOPUT REPLY 'STOP'
     02 R r02 DSI802A NCF11    REPLY WITH VALID NCCF SYSTEM OPERATOR
          COMMAND
     01 R r01 CHF0011A ENTER HCF/LCV CONTROL COMMAND
    638 I *IEA000A 410,CC=3/NO PATHS AVAILABLE,,,
     75 I *ICH505A RACF INITIALIZATION ABEND S 013.
     74 E *IEA911E COMPLETE DUMP ON SYS1.DUMP00
           FOR ASID (0001)
            ERROR ID = SEQ00001 CPU00 ASID0001 TIME12.06.20.6


 ??? ***
ocf11 d a,l
```

Figure 4. MVS/OCCF output in response to an operator issued 'D R,L': NCCF clears the screen before it presents these messages

```
 NETWORK COMMUNICATIONS CONTROL FACILITY                     09/27/82 12:38:38 A
          IEE104I 12.38.00 82.270 ACTIVITY 773                           (NCF11    )
  JOBS       M/S        TS USERS      SYSAS        INITS       ACTIVE/MAX VTAM
 00000      00008        00002        00006        00003        00002/00040
  JES2      JES2       IEFPROC  NSW  S   SOF       SOF      SOF      OWT  S
  OCCFN     OCCFN      ST1      IN   S   NET       NET      NET      NSW  S
  TSO       TSO        TCAS     OWT  S   VMDISC    VMDISC   DISC     OWT  S
  HCF       HCF        ST1      OWT  S   ADMPRINT ADMPRINT ADMPRINT OWT  S
 TSOUSR1 OWT   TSOUSR2 OWT




 ??? ***
```

Figure 5. MVS/OCCF output in response to an operator issued 'D A,L': NCCF clears the screen before it presents these messages

The central operator may do this from the same or another NCCF terminal for all sub-hosts in the network as it is shown in Figure 6 on page 13. A logon to OCCF in the same domain is also possible and may be sensible. This allows e.g. a central operator to invoke OCCF CLISTs for the central host from his NCCF terminal.

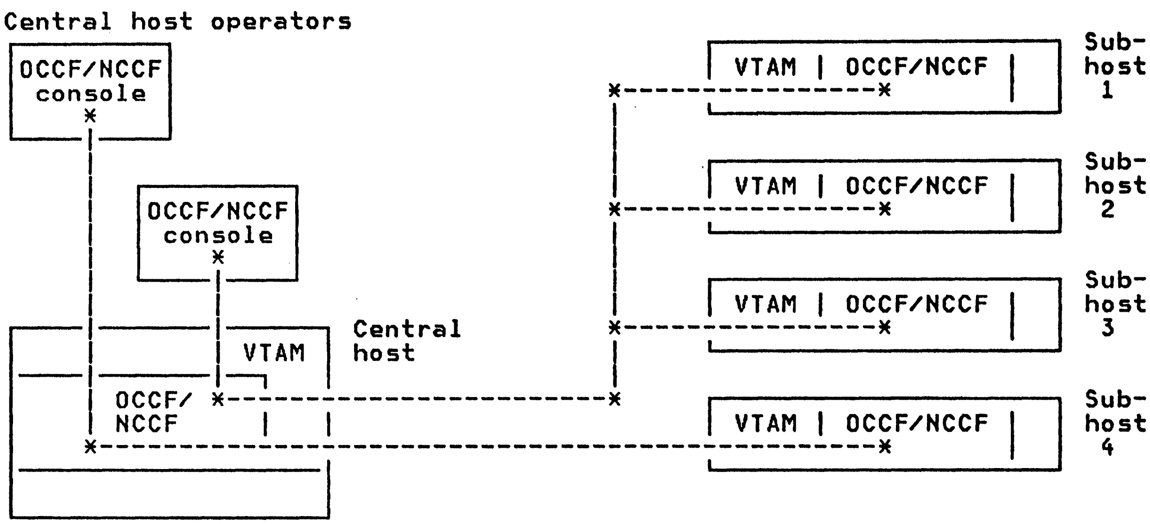


Figure 6. Multiple sub-hosts controlled through OCCF

The user can define the messages to be routed to the OCCF/NCCF terminal. Messages can be selected by their MVS routing code and by the message id. E.g. by specifying

IEA* ROUTE

in the OCCF definition deck of a sub-host, all messages starting with the characters IEA are routed to a logged on OCCF/NCCF terminal. Message routing in OCCF has no influence on the message routing in MVS. All messages which go to an OCCF/NCCF terminal are also processed by the console support of MVS. However, multiple consoles are not supported by OCCF. One host can only have one OCCF console.

CLISTS

NCCF, OCCF, and SOF command lists can be used to speed up and simplify network and system operation. A CLIST allows a list of commands to be invoked for execution by one command. NCCF supports CLISTs consisting of VTAM commands, NCCF commands, NCCF control statements and statements to invoke other NCCF CLISTs. NCCF has the most powerful CLIST control language of the three products. The CLIST support of OCCF and SOF are fairly similar to each other. OCCF/SOF CLISTs can contain OCCF/SOF control statements and everything that can be entered through a MVS system console, e.g. MVS and JES2 commands.

The following chart gives an overview to see which type console must be used to invoke a specific type of CLIST or to issue a specific type of command (MVS, JES2, or VTAM):

	MVS console	NCCF terminal	NCCF terminal logged on to OCCF
MVS and JES2 commands	+	*	+
VTAM commands	+	+	+
NCCF CLISTs	-	+	+
OCCF CLISTs	+	*	+
SOF CLISTs	+	*	+

\+ possible

\- not possible

* possible by an installation coded NCCF command processor. The source statements for such a command processor called 'MVS' are contained in this book and can be found in "Appendix C. NCCF command processor: MVS" on page 69. 'MVS' allows a user to issue MVS commands, JES2 commands, invoke OCCF CLISTs etc. from an NCCF terminal or an NCCF CLIST. Although no messages are returned to an NCCF terminal (e.g. when a 'D A,L' is issued) this program is still useful as it is shown in several samples later in this book.

Note: VTAM commands include replies to some VTAM messages.

A central operator can be easily over run if he has to operate multiple systems by the standard capabilities of the operating systems. To make central operation efficient he has to be relieved as far as possible. For centralized network and system operation, CLISTs are therefore nearly indispensable. Sample CLISTs for specific problems are documented throughout this paper. Within this section CLISTs are treated more generally and with the intention to show some more samples:

Online information

NCCF, OCCF, and SOF do not have any online 'Help' function which provides information for the users about usage and function of the operating facilities. This can be overcome by using the CLIST capability of each product to tailor its own 'Help' facility. Such a 'Help' facility should be provided at least for the installation supplied CLISTs. Most of the CLIST samples described in this paper contain within them a little description of their function and how to use them. By convention, a user gets the 'Help' information if a CLIST is invoked with a ? as the first parameter or if no parameter is specified for a CLIST which requires one. An overview on operator commands, CLISTs, etc. should be also provided to give the inexperienced user an introduction (see "NCCF CLIST: HELP" on page 57).

However, providing for descriptive information causes additional exertion in defining a CLIST and for CLISTs with just a few statements it is often enough information to have a look at these statements. For OCCF and SOF CLISTs the display facility of these products can be used to incorporate a 'Help' tool in a CLIST with just a few standard statements. If you have a look at "CLISTs for system monitoring" on page 60 you can see the statement '%QSHOW SYSMON' near the bottom of the CLIST SYSMON. %QSHOW is an OCCF command. Within this sample, it is executed when the user enters 'SYSMON ? ' and it will display the statements of the CLIST SYSMON at the users console.

Note: Throughout this paper % is used to designate an OCCF command or CLIST. The OCCF default designator character is /

Installation provided consistency between NCCF, OCCF, and SOF CLISTs

The samples in "CLISTs to activate network nodes" on page 57 should show how one and the same function, is defined in NCCF, OCCF, and SOF. In an operation environment where two or all three products are installed there is an advantage to define e.g. an NCCF CLIST and an OCCF CLIST with the same external syntax for the same function. The activation of network nodes is just a sample for that and it provides similar capabilities for the operator at an MVS console and an NCCF terminal.

Simplification of operation

If you have a look at the CLIST shown under headline "MVS/OCCF CLIST: OS MOUNT command" on page 59 you can see how the OS MOUNT command can be simplified. An operator just has to enter e.g.

```
%M 197 DLIB82          instead of

V 197,ONLINE
M 197,VOL=(SL,DLIB82),USE=PRIVATE
```

Other samples for simplification of system operation using a OCCF CLIST are included in Appendix A. Two of the clists are used to allow GFT to be executed from any source that can submit OS commands. Here OCCF's automatic message reply facility is used. GTF can be started and stopped without further operator action (GTF normally requires a reply from the operator at the MVS console). This allows invoking GTF from an NCCF terminal by using the NCCF command processor 'MVS' (see the description of the 'MVS' command processor earlier in this chapter). All the NCCF user has to enter is:

```
MVS /STARTGTF        or
MVS /STOPGTF         respectively
```

Gathering of line trace or VTAM buffer trace data is a common task for problem determination. VTAM buffers regarding cross-domain traffic between a terminal and an application can only be traced in the host of the primary session partner. In a centrally controlled configuration that is normally a sub-host where the application runs. The STARTGTF/STOPGTF CLISTs in conjunction with the 'MVS' command processor allow traces to start and stop in a remote sub-host from any NCCF terminal. (Note that MVS commands for a remote sub-host can be issued from **one** NCCF/OCCF terminal only).

Reduction of operator intervention

Here are two samples how operator intervention is substituted by automatically invoked CLISTs. The first one is a sample for reactivation of an IBM 8100/DPCX subsystem. When a DISABLE HOST command is executed in a DPCX subsystem, DPCX sends an SNA request for a discontact which makes VTAM issue the message

```
IST169I DISCONNECTION CAUSED VARY INACT FOR PU = .....
```

and deactivate the PU. This is a normal procedure when IBM 8100/DPCX is brought down e.g. in the evening. But the PU representing the IBM 8100/DPCX subsystem has to be reactivated by an VARY ACT command in order to allow reactivation of the IBM 8100 the next morning. To relieve the network operator of issuing VARY ACT commands in such cases, the NCCF facility to intercept a VTAM message and execute a specific CLIST instead is used in the sample under headline "NCCF CLIST to reactivate selected PUs after msg IST169I" on page 60. The CLIST called IST169I is executed every time VTAM issues message IST169I ... . The message together with a VARY ACT command for the disconnected PU is then issued by the CLIST.

The next sample shows how the NCCF command EVERY can be used for automatic revival of failed system functions. If you have a look at the NCCF initial CLIST shown under headline "NCCF initial CLISTs" on page 64 you can see an EVERY command which is coded to schedule execution of a CLIST called MONITOR every 30 minutes after NCCF initialization. The CLIST MONITOR in turn invokes the OCCF CLIST SYSMON through the 'MVS' command processor (see CLISTs under headline "CLISTs for system monitoring" on page 60). In an OCCF CLIST you can code nearly any type of MVS or JES2 command. The commands in the sample CLIST SYSMON are defined to care about restart of NJE, NJE lines, and NJE to NJE sessions. NJE lines may temporarily go down or NJE to NJE session can be disrupted e.g. by a route failure but JES2 does not try to restart them. By applying the described technique NJE can be automatically restarted after a temporary failure without operator intervention. This is important particularly for NJE in an unattended sub-host.

It should however be noted that all facilities to automatically restart components have to be developed in a way that they are not triggered if the component is deactivated deliberately. It is also recommended for other types of automated procedures that the possibility to overwrite automatic operations should be retained.

Tailoring of VTAM messages

Care should be exercised when tailoring VTAM messages. In no case should any VTAM message that is part of a full-screen message be modified. When a full screen message is processed by NCCF, the VTAM messages that are not modified are presented first and then the user modified messages. If the first message or the last message is modified by a clist, NCCF may not present any data.

NPDA VERSION 2

NPDA is a tool to automatically collect statistical data and information about unusual events within a network and store it into a data base for later display at an NCCF terminal. Beyond this, NPDA Version 2 now provides alert handling capabilities. Alerts, which are indications of high priority events, can be presented to the network operator, as soon as the alert triggering event occurs. In many cases, the network operator is now able to react to failures of network components much sooner than with NPDA Version 1.

Compared to NPDA Version 1, the new alert handling capability is more a new approach to present the data rather than a collection of new data about unusual events. Alerts are stored in the NPDA data base and displayed to the user in a reverse-chronological order and are not organized by components. They may be presented on an NCCF screen in:

- A dynamic display -- a single display that is updated each time NPDA builds and stores an alert.
- A static display -- a 'frozen' version of the single page dynamic display that allows the user to easily read rapidly accumulating alert data.
- A history display -- a multi-page display of all alerts stored in the NPDA data base.

```
NETWORK PROBLEM DETERMINATION APPLICATION                    02/12/82 10:50:18
NPDA-30B                      * ALERTS-STATIC *
DOMAIN: NCF11

SEL#  DATE/TIME  TYPE RESNAME  ALERT DESCRIPTION:PROBABLE CAUSE
( 1) 02/12 10:49 LINE L14040   LINK TIMEOUT:LINE DISABLED(PRIMARY END)/COMMUN.
( 2) 02/12 10:47 LINE L24030   MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM
( 3) 02/12 10:43 COMC N245F3N  ADAPTER CHECK:COMMUN. CTRLR. PGM/COMMUN. CTRLR.
( 4) 02/12 10:42 CTRL P24020E  COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE
( 5) 02/12 10:29 LINE L14040   LINK TIMEOUT:LINE DISABLED(PRIMARY END)/COMMUN.
( 6) 02/12 10:27 ADAP 1D       "N" GROUP TIMEOUTS:DEVICE/COMMUNICATIONS
( 7) 02/12 10:27 LINE L24030   MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM
( 8) 02/12 10:05 CTRL CARO     COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE
( 9) 02/12 10:02 CTRL LINE     LINK TIMEOUT:LINE DISABLED(PRIMARY END)/COMMUN.
(10) 02/12 09:47 ADAP 1D       "N" GROUP TIMEOUTS:DEVICE/COMMUNICATIONS
(11) 02/12 09:35 ADAP 1D       "N" GROUP TIMEOUTS:DEVICE/COMMUNICATIONS
(12) 02/12 09:18 CTRL P040A0EE POWER OFF DETECTED:REMOTE PROBE POWER OFF/PROBE
(13) 02/12 08:31 PROG 04B6     ACCESS EXCEPTION-SECONDARY PSV:PROGRAM
(14) 02/12 08:31 PROG 04B6     ACCESS EXCEPTION-SECONDARY PSV:PROGRAM

DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER 'A' TO VIEW ALERTS-HISTORY
ENTER SEL# (ACTION),OR SEL# PLUS ' M'(MOST RECENT),' P'(PROBLEM),' DEL'(DELETE)

13 p_
```

Figure 7. Example of NPDA Alert Static Display

The NPDA dynamic display of alert data is an outstanding tool for monitoring an SNA network. This is especially true in an environment with a central network processor, because all irregularities of the network can be focused to one location. Depending on the size and complexity of the network it might be a good idea to have one NCCF screen as a monitor just for NPDA alert dynamic display or even have several such monitor screens each for a specific part of the network.

It should be noticed that an NCCF screen which is in

- NPDA alert dynamic display mode and also
- receives the unsolicited messages

cannot run without operator intervention. NPDA alert dynamic display mode is a full-screen display which is not intermixed with the NCCF presentation of the unsolicited messages. Although a switch from NPDA display mode to NCCF display mode is done automatically, the NCCF operator is forced by NCCF to confirm a reverse switch. For example, if the NPDA alert dynamic display is shown on the screen by the time NCCF wants to present unsolicited messages, the screen is cleared and the messages appear at the upper lines of the screen. If afterwards NPDA wants to present an updated alert display, *** appears at the lower left corner of the screen as an indication that the operator has to press the ENTER key. After doing that, the latest NPDA Alert Dynamic Display is shown on the screen. This technique is independent of the NCCF autowrap mode which normally allows running an unattended NCCF session.

The NPDA alert history display can be used as a complete record of problems which exist in the network and which need attention by the network operator. To achieve this, all the network operator has to do is to delete those records from the NPDA alert part of the data base which tell about resolved problems or problems which have been already reported to other departments for solution. Records deleted from the history display can still be viewed on event or statistical data displays. So the NPDA alert history display used in this way is a good tool e.g.

- for operator communication e.g. at shift change.
- to relieve network operators of reporting minor problems somewhere else.

The technique described above may require reducing the alerts presented by NPDA to those which really demand some action. NPDA allows to reduce the data collected or displayed by means of filters. Recording filters in NPDA can be used by an installation to control what data should be recorded in the NPDA data base. Viewing filters allow each operator to control what data should be displayed on his terminal. Each of these filters consists of a number of entries, created with NPDA SRFILTER or SVFILTER commands. By means of these commands NPDA is told to either 'block' recording/viewing of events or to let them 'pass'. The following filter criteria can be specified:

- Event types, e.g.: performance, permanent errors
- Resource names
- Resource types, e.g.: communication controllers, lines

Because NPDA filters are stored only in main storage an NPDA users viewing filters are lost after logoff and recording filter are lost after NCCF close down. The filters can be automatically restored by the NCCF initial CLIST or by a users initial logon CLIST (see "NCCF initial CLISTs" on page 64 for a sample).

NPDA also provides for the transfer of selected information to the INFO/Management feature of the INFO/System program product. To transfer problem descriptions from the NPDA data base to INFO/Management data base all the NPDA user has to do is to locate the problem description on an NPDA display and enter the selection number which represents the problem followed by the character P (see Figure 7 on page 17 for an example display). The information issued by NPDA can then be supplemented under INFO/Management during further tracking of the problem.

N P A

One of the tasks network operation comprises is surely to look after certain performance degradations. Without having appropriate tools to discover the reasons for performance problems you are often dependent on speculations and your approaches to resolve such problems are not always based on the facts. In the communication network area NPA is a tool which gives you a lot of information about what is going on in communication controllers or NCPs respectively. It tells you e.g. about

- IBM 3705 utilization
- NCP buffer utilization
- message queues within the NCP
- message rates
- byte rates
- negative poll rates
- line utilization
- temporary errors

An NPA user can get this data from any NCP in the network if the NCP was generated to support NPA . Thus there is no necessity to run multiple NPAs in a centralized network. With the data provided by NPA, performance problems caused for instance by

- long NCP outbound queues
- insufficient line capacity
- excessive traffic at certain periods
- IBM 3705 over utilization
- high error rates for lines, clusters, etc. caused by temporary errors

can easily be identified. Although temporary errors are also counted by NPDA, the figures from NPA are quite different. Whereas NPDA tells you the number of temporary errors for a specific number of messages, NPA gives you the number of temporary errors per time interval. For some kinds of problems it is just as important to know the time when the errors occur as the traffic/error ratio. Here is an example: You have poor response times between 3 and 4 o'clock in the afternoon on some of your terminals connected via switched lines. NPDA tells you that you have an average percentage of temporary errors on these terminals. When you start collection and display for these terminals on NPA you can see that temporary errors between 3 and 4 o'clock increase heavily. It is now very likely that the reason for the long response times is an overload of the public network.

With its monitor function, NPA supports the network operator with an alert capability in addition to the one provided by NPDA. Low and high threshold values can be defined for things like

- negative or positive poll rates
- line utilizations
- message rates
- error counts
- IBM 3705 utilization

When the data falls outside these limits, an exception message is displayed at the NPA terminal. As an example, the operator can specify a low limit of 1 message per minute for a cross-subarea link. If the message rate on that link drops below 1 message per minute NPA alerts the operator by displaying a highlighted monitor message and sounding the alarm on the 3270 screen. This message is then interpreted by the operator as an indication of potential problems at either end of the link.

CICS/VS AND IMS/VS

CICS/VS and IMS/VS do not cause any specific problems in a centrally controlled multi-host environment. The master terminal function for any those subsystems can be made available in many different ways at the central site. This is described in the next chapter in section "CICS/VS and IMS/VS master terminal" on page 28. Multiple physical routes should be available to preserve accessibility from the central site to the subsystems.

Running CICS/VS or IMS/VS on a remote sub-host with the master terminal operator at the central site seems to be possible in many cases. There is no need for people skilled in data processing to operate the remote systems if their operations comprise just a few, well documented interventions. You may also think one step further of an unattended remote system. With the ROCF facility of an IBM 4300 processor you can do a remote IML/IPL. Physical operation is however still required in some areas as e.g. IMS/VS requires mounting of log tapes on a tape drive. But this does not mean, that the remote system has to be attended all the time. During the day, remote operation could be done on an alert basis, where the alert comes from the central operator.

INFO/MANAGEMENT

Within section "NPDA Version 2" on page 16 or a following page there is a description of how to use the problem management facility of INFO/Management in conjunction with NPDA. To illustrate all the possibilities of

Problem Management
Change Management and
Configuration Management

by means of INFO/Management is certainly beyond the scope of this paper. Therefore only one sample is given here to show how information data is presented by INFO/Management:

An installation using configuration management in INFO/Management enters descriptive information about hardware and software system components into the INFO/Management data base. This information can be used e.g. by the network operator for his specific needs. Let's assume he has a problem with a display control unit and wants to know who is responsible for that device. For that purpose, he enters the INFO command under NCCF or TSO and gets the INFO/System Primary Options Menu Display in response. He then enters a command e.g. 'DISPLAY R AB16' to get the Hardware Component Display for the device AB16:

```
BLGON100            HARDWARE COMPONENT DISPLAY            COMPONENT ID: AB16

Generic device.......... CTL                  Component status.....<H> INSTALL
Device type & model..... 327451C              Date of status.......<H> 03/11/82
Serial number........... 123A10               Network name............ P140A0F
Order number............ AB0001               Node name............... N14BF3N
Microcode EC level...... 1234-56              Program name............ ________
Date shipped............ ________             LTERM ID (IMS).......... ________
Lease begin date........ ________             CICS ID................. ________
Lease end date.......... ________             Location code........... RSC
                                              Display class........... 1
Description............. 3274 CONTROL UNIT

 SELECT ONE OF THE FOLLOWING, OR REPLY 'QUERY' FOR AVAILABLE SUBCOMMANDS

   1. Hardware component display              7. Up component ID display
   2. Hardware support display                8. Line information display
   3. Hardware EC level display               9. Up component list display
   4. History display                        10. Down component list display
   5. Freeform text and notes                11. Up & Down synopsis display
   6. Feature list display                   12. Connectivity path entry


===> _
```

Figure 8. Example of INFO/Management Hardware Component Display

When he then enters a 2 he will get the desired information on the INFO/Management Hardware Support Display:

```
BLG0N150              HARDWARE SUPPORT DISPLAY          COMPONENT ID: AB16

Component owner.....<H> RSC                 Center ID.............. RSC
Transfer-to class...<H> ________            System ID.............. ________
Contact name........<H> GTAYLOR             Finance ID............. ________
Contact department..... D40                 Service ID............. ________
Contact phone.......... 312-245-3000        Owning priv. class..... ________
Maintenance interval... __                  Entry priv. class...... ________
                                            Date entered........... 03/01/82
                                            Time entered........... 11:33
                                            Date last altered...<H> 03/01/82

 SELECT ONE OF THE FOLLOWING, OR REPLY 'QUERY' FOR AVAILABLE SUBCOMMANDS

   1. Hardware component display             7. Up component ID display
   2. Hardware support display               8. Line information display
   3. Hardware EC level display              9. Center ID display
   4. History display                       10. System ID display
   5. Freeform text and notes               11. Financial ID display
   6. Feature list display                  12. Service ID display


===> _
```

Figure 9. Example of INFO/Management Hardware Support Display

Note: The name of the control unit AB16 is independent of its network node name.

Performance considerations. Based on user experiences with NCCF and Information/System, it is reccommended that only the NPDA to INFO/Management interface be used whith NCCF. Further use of INFO/Management should be done vis a TSO session. This TSO session can be made through the TAF interface of NCCF. This technique does not impact the performance of NCCF and does not require the virtual storage of NCCF to be expanded 800K bytes for each INFO user.

Activation of a centrally controlled multi-host configuration can be divided into the following major parts:

1. Activate systems (central host and sub host(s))

2. Activate network

3. Establish central control

As central operation implies the trend to reduce remote sub-host operation as far as possible, here the most interesting question is probably: How much sub-host operator action is necessary before the sub-host can be controlled by a central operator? The answer to the question depends of course on many factors but the general answer is:

- System activation of IBM 4300 sub-hosts is possible from a remote central site.

- All other IBM /370 sub-hosts have to be activated from the sub-host site.

Activation of a multi-host SNA network with all its components can be a very complex process and it is nearly impossible to cover all the constraints of real installations in a paper like this. The procedures described here are just samples to show what is possible with the current state of the products. Subjects covered by this chapter will illustrate

- how a central host, sub-host(s), and a network can be activated with very few operator interventions.

- how a central host operator is able to take over control of sub-hosts.

- how CNM products can help in the system and network activation process.

ACTIVATION OVERVIEW

Here is a step by step overview how system and network activation is covered in this chapter:

1. IPL

2. Automatic start of VTAM, OCCF, NPDA, NCCF

3. Execute MVS/OCCF CLIST which

   - starts applications e.g.: TSO, CICS/VS, IMS/VS, etc.

   - issues MVS and JES2 commands to start e.g. NJE and lines

   - activates NCPs and locally attached 3270 control units

4. Establish NCCF to NCCF sessions

5. Transfer MVS consoles logically from sub-hosts to the central NCCF operator by establishing NCCF to OCCF sessions

6. Make the master terminal operator function of sub-host's CICS/VS and IMS/VS available at the central site

MVS operator commands except JES2 commands can be put into a COMMNDxx member of the SYS1.PARMLIB data set. These commands are internally issued by the system at system initialization time. JES2 itself is automatically started by the standard MSTRJCL definition in the SYS1.LINKLIB data set. So JES2 and some routine procedures can be started by standard MVS functions. But when one procedure requires another procedure to be started, as TSO requires VTAM, this standard facility is not sufficient.

In order to manage the scheduling of automatic starting procedures during the system activation process an MVS/OCCF CLIST can be developed which provides for starting VTAM application programs and initialization procedures with little or no operator intervention. Using this technique, all the operator is required to do is to perform the basic IPL procedures such as specifying system parameters, answering the IPL reason and then start the OCCF CLIST.

The procedure described here takes care of activating the resources in the system. It is useful not only on the sub-host but also on the central host to

- avoid operator mistakes during system activation
- reduce the skill needed for system activation
- speed up system activation

IBM 4300 sub-host processors can be IPLed and activated from the central site without intervention at the sub-host site by using ROCF, a VTAM independent tele-access capability.

After the system and the network are initialized the central operator can take over control of the whole network by logging on to the sub-hosts NCCFs. In addition to commands, CLISTs, and replies that relate to the network NCCF can be used as a port to

- a sub-hosts system console (via OCCF)
- control sub-hosts applications like CICS/VS and IMS/VS (via NCCF/TAF or OCCF)

The following shows the system activation process in more detail:

Note: Procedures and CLISTs mentioned throughout this chapter are concentrated in "Appendix B. System and network activation: Sample definitions" on page 63.

IPL

The operator executes the IPL and replies to some standard MVS messages such as

```
              IEA846I SYSTEM CONSOLE INTERFACE UNSUCCESSFUL.
IEA101A SPECIFY SYSTEM PARAMETERS FOR RELEASE 03.8 .VS2,VER=SP1.3.2 JBB1328
and
IEA347A SPECIFY MASTER CATALOG PARAMETER
```

COMMNDXX

The MVS system initialization causes JES2 to be started and the commands defined in the COMMNDxx member of the SYS1.PARMLIB data set to be executed automatically. The significant commands issued by COMMNDxx definitions are:

```
START VTAM        and
START OCCF
```

If OCCF, NCCF, and NPDA should run on the same system then starting OCCF does include starting of NCCF and NPDA because they are all placed in the same MVS address space. This in turn leads to a synchronization problem because NCCF needs an active VTAM to open its ACB. If the NCCF application node in VTAM is not in the state of CONCT (connectable) by the time NCCF comes up then NCCF writes the message

```
nn DSI800A REPLY 'RETRY','SHUTD' OR 'ABEND' TO PROCESS
           NCCF OPEN ACB FAILURE
```

to the system operator console. This message can be automatically replied to with RETRY by OCCF because OCCF has an Automatic Reply function and OCCF is already active when NCCF writes out this message. If after retry VTAM is not up yet, the same NCCF message comes again and is again replied to by OCCF with a few seconds delay. This sequence might be repeated several times until finally VTAM, OCCF, NCCF, TAF, and NPDA are all active.

NCCF INITIAL COMMAND OR CLIST

Some activation of the network can be done by specifying a CLIST or a command in the NCCFIC definition statement for automatic execution after NCCF is initialized. This initial command or CLIST execution can be used for instance to activate NCPs or set NPDA recording filters.

NCP ACTIVATION

All the NCPs in the network have to be activated from the central host to form centralized network control. The NCPs which are channel attached to remote sub-hosts have also to be activated from the respective sub-host to link the sub-host to the network. Activation of an NCP may include IPL of the IBM 3705. VTAM makes the decision and automatically reloads the IBM 3705 if necessary provided that

```
AUTOSYN=YES        and
VFYLM=NO
```

was coded in the PCCU macro instruction for the NCP and the NCP was activated by an

```
V NET,ACT,ID=....,LOAD=U
```

command (LOAD=U is also the default). NCPs should not be activated by specifying them in the ATCCONxx member of the SYS1.VTAMLST data set. The better way is to activate them after NCCF and NPDA are up to ensure that errors occurring during NCP activation are recorded in the NPDA data base.

The commands to activate the NCPs can be put into the NCCF initial CLIST or an OCCF start-up CLIST (see "MVS/OCCF start-up CLIST"). This allows to automatically activate NCPs at system initialization time without issuing VARY ACT commands manually by the operator.

Remote IPL of an IBM 3705 across a link not always works without intervention at the remote site. Depending on the state of the IBM 3705 it is sometimes necessary to hit the load button in order to get the box loaded. Provisions have to be made, that someone is available at the remote IBM 3705 location to do this if required.

An IBM 3705 can be equipped with channel adapter(s) plus Remote Program Loader (RPL). This allows central site IPL of an IBM 3705 which is channel attached to a remote sub-host. Remote loading of a channel attached IBM 3705 can be done e.g. for backup reasons in case of a sub-host failure. It should however be noted that the RPL can only be used if the IBM 3705 is detached from the host processor's channels. The RPL is activated by manually switching off all the channel adapters at the IBM 3705 console. This has to be considered for planning of an unattended remote sub-host.

MVS/OCCF START-UP CLIST

MVS or JES2 commands which are normally entered to a system console can be put into an MVS/OCCF CLIST for execution when required. This facility can be used here to start TSO, CICS, IMS, etc. If the applications require certain operator replies, OCCF can be used to automatically do that. However, because OCCF always replies to a specific message id with a specific response this approach is not possible for instance in IMS/VS.

The OCCF start-up CLIST can also be used to start NJE. The SNA part of NJE is a VTAM application within JES2. Here is a little problem, because JES2 is started before VTAM and JES2 therefore can not open its VTAM ACB at initialization time. NJE has to be started by JES2 operator commands after VTAM is active. By defining these commands in the OCCF start-up CLIST an automatic NJE start can be provided.

Depending on the requirements of an installation it might be a good idea to bring up some part of the network after the applications are active. This can prevent a flood of messages like

```
IST264I SESSION SETUP FOR PLU = .... SLU = .... FAILED-
        REQUIRED RESOURCE .... NOT ACTIVE
```

caused by end users trying to logon to an application that is not active. So activation of NCPs, local control units 3270, etc. can also be done by putting the proper VTAM commands into the OCCF CLIST.

The OCCF start-up CLIST has to be invoked manually by the operator because MVS/OCCF does not have an initial CLIST capability like NCCF. This can be done either through the system console or through an NCCF terminal. Before you can invoke OCCF CLISTs from an NCCF terminal you have to establish an NCCF to OCCF session (same domain or cross domain).

However, another technique is used in the samples shown in the appendix: The OCCF start-up CLIST (called %AUTO) is invoked by the NCCF initial CLIST. This is possible by the NCCF command processor 'MVS' which is used here to more automate the system activation.

ACTIVATION SYNCHRONIZATION AND CHECKPOINT

Thus far, similar procedures have to run on the central host as well as on every sub-host. The completion of the system initialization process is like a synchronization point. Before the central operator can take over control from a sub-host to the central host, the central host and the corresponding sub-host have to reach this state.

The nearly automated system activation procedure described here is almost sufficient in daily or weekly operation as long as the system is not changed. The result is that the operation procedure for IPL can be described in only one page of the operation manual. Even if the system is changed, and it requires 'CLPA' or JES2 to cold start, the OCCF procedure can still be used to start the applications.

Another approach to system activation using the FDP SOF is described in a document called 'CNM Managing Interconnected Systems, GG24-1539'.

The activation of the network is normally combined with a flood of VTAM messages and it is nearly impossible for an operator to notice failures during the network initialization process. The central operator should check the most important network components right after activation completion to identify the areas where additional activities are necessary. This should at least include a check of the subarea interconnection and a check whether something hangs in the network. If a CLIST is provided for a network check it should therefore contain a

```
D NET,PENDING      and a
D NET,STATIONS
```

as the minimum.

ACTIVATION OF A REMOTE IBM 4300 BY ROCF AND MVS/OCCF

The activation procedures described above can also be initiated and controlled from a central host on behalf of a remote IBM 4300 sub-host without any operator intervention at the sub-host site. That is possible via ROCF a feature of IBM 4300 processors which supports remote system consoles over a switched BSC line. This support includes all types of operation possible at a system console including IML/IPL. As ROCF is a hardware implementation it is independent of an operating system on the IBM 4300 processor. ROCF supports an IBM BSC 3275 model 2 terminal as the remote console.

OCCF has a function called Remote Start Up Facility (RSUF) which can be used to simulate the IBM 3275. RSUF is invoked from an NCCF terminal and requests some input from the user in order to establish the connection to ROCF in an IBM 4300 (see Figure 10).

```
                         REMOTE IML/IPL FACILITY

 SELECT ONE OF THE FOLLOWING:

                 1 = DIAL - DIAL A REMOTE SITE

                 2 = DISC - DISCONNECT A REMOTE SITE

                 3 = TERM - TERMINATE REMOTE IML/IPL COMMAND.
                            WILL ALSO DISCONNECT IF A CONNECTION
                            IS ACTIVE.

                 4 = TREQ - REQUEST MODE CHANGE



 TYPE SELECTED NUMBER HERE: 1

 IF 1 WAS CHOSEN, FURNISH TELEPHONE NUMBER FOR AUTODIAL
 OR * FOR MANUAL DIAL.
 ENTER TELEPHONE NUMBER OR * HERE: *
```

Figure 10. ROCF support in OCCF: This panel is shown by OCCF when a user enters RSUF at an NCCF terminal.

After the connection is established the NCCF terminal is logically made an IBM 4300 system console which allows any type of operation possible on such a console. So, to activate an IBM 4300 sub-host IML, IPL, start of jobs, CLISTs, etc. can all be done from an NCCF console at the central site. However, it is not necessary to keep this connection after the sub-host can be controlled from the central host through NCCF to NCCF and NCCF to OCCF sessions. As ROCF supports a switched connection, one central site port can be used to bring up several remote IBM 4300 sub-hosts.

Another advantage of the ROCF facility is that the connection to the sub-host can be reestablished at any time after activation without disrupting anything at the sub-host. This makes trouble shooting from the central site possible for all kinds of problems which do not need manual intervention at the sub-host site.

Note: As ACF/NCP does not support switched BSC lines, the port used for ROCF has to be generated as an EP line in the NCP. A DD-statement for the line has to be added to the JCL-procedure which is used to start OCCF/NPDA/NCCF.

NCCF TO NCCF AND NCCF TO OCCF SESSIONS

The NCCF to NCCF and NCCF to OCCF sessions are used to take over network and system control from a sub-host to a central host. Once the central host and the sub-host(s) are connected via cross domain link(s) and NCCF and OCCF are ready for communication, NCCF to NCCF and NCCF to OCCF sessions have to be established to further interconnect the systems. To do this, three commands have to be entered from a central NCCF terminal:

1. START DOMAIN=domain-id

2. ROUTE domain-id,oper-id,password

3. ROUTE domain-id,OCCF %QLOGON

The commands have to be synchronized, because the operator has to wait for specific messages before he can issue the second and third command.

The central NCCF operator must repeat this operation for every sub-host NCCF. To ease this tedious operation by the central NCCF operator, this sequence could be done by means of an NCCF CLIST (for a sample CLIST see "NCCF CLIST to establish NCCF-NCCF and NCCF-OCCF sessions" on page 67). It will relieve much of the host operator work every morning and also prevent the operator from forgetting to start some of the sessions.

CICS/VS AND IMS/VS MASTER TERMINAL

In order to control subsystems like CICS/VS and IMS/VS from the central host, the master terminal function of these systems needs to be available at the central site. There are several ways to achieve this. Traditionally there are two possibilities to control CICS/VS and IMS/VS:

1. From a dedicated master terminal

2. From the MVS system console

The first method is suitable for centralized network management because the central subsystem master terminal operator can logon to any subsystem from any terminal either same domain or cross domain. But, for every subsystem a physical master terminal is needed.

The second method works only, when CICS/VS or IMS/VS run on the central host or on a host which is at the same location as the central host because an MVS system console is a locally attached terminal.

Now both possibilities are expanded and the master terminal function of all subsystems in a network can be focused to one NCCF terminal. The TAF feature of NCCF allows communication from an NCCF terminal to CICS/VS and IMS/VS. The central operator can logon to CICS/VS and IMS/VS as a master terminal operator from his NCCF terminal via TAF. Without leaving his NCCF session he can enter CICS/VS or IMS/VS commands.

The other way to direct the master terminal function to an NCCF screen is via OCCF. As mentioned earlier in this chapter, an MVS system console can be logically transferred to an NCCF screen. So, if sessions from the central host's NCCF to sub-host's OCCF are established, the MVS system console functions of the sub-hosts are available at the central host. That means that master terminal operator commands can be entered at the NCCF console without any other initialization procedure. In the case of IMS/VS for instance, the central operator can enter the IMS/VS commands

```
/NRESTART ....
/START DC
/START REGION ...
```

as replies to the IMS/VS messages

```
nn DFS810A IMS/VS READY ........     or
nn DFS996I *IMS READY*  ....
```

to bring up IMS/VS .

CICS/VS requires that the OCCF console has to be defined in the CICS Terminal Control Table (TCT) with the proper authorization.

Note: The requirement to have all control functions directed through one single operator interface should be carefully considered with regard to traffic and usability before installation of only one display console for operator control.

A multi-domain SNA configuration consists of a great number of interrelated single components and there is a big chance at any time that some of these components are in an out of order state. The structure of the interrelationship between the components is not always simple and makes it necessary not only to provide for backup capabilities but also to prepare operating procedures for exception situations in advance. It is important to simulate and test the failure of each component as well as multiple failures before the emergency case to make sure that the recovery works in the way expected. To be prepared for a failure of any component and be able to take the most appropriate recovery actions results in not dropping the service for the end users under a desired and possible level.

This chapter contains some information necessary in planning recovery actions and provisions:

- Failure and restart of different components
- Impact of component failures on other parts of the network
- Special operating procedures required to back up components

Not all of the things mentioned in this chapter only relate to a centrally controlled environment but they may still be helpful for the operation of such a configuration.

Note: The failures which are covered in this chapter are of those types, where the component is not available at all for any reason. Other types of failures such as intermittent errors on a modem, a software error in a cluster controller, etc. are often not so evident and require effort in problem determination, isolation, and recognition. As this is a complex subject on its own, it is not dealt with in this paper.

SESSION FAILURE

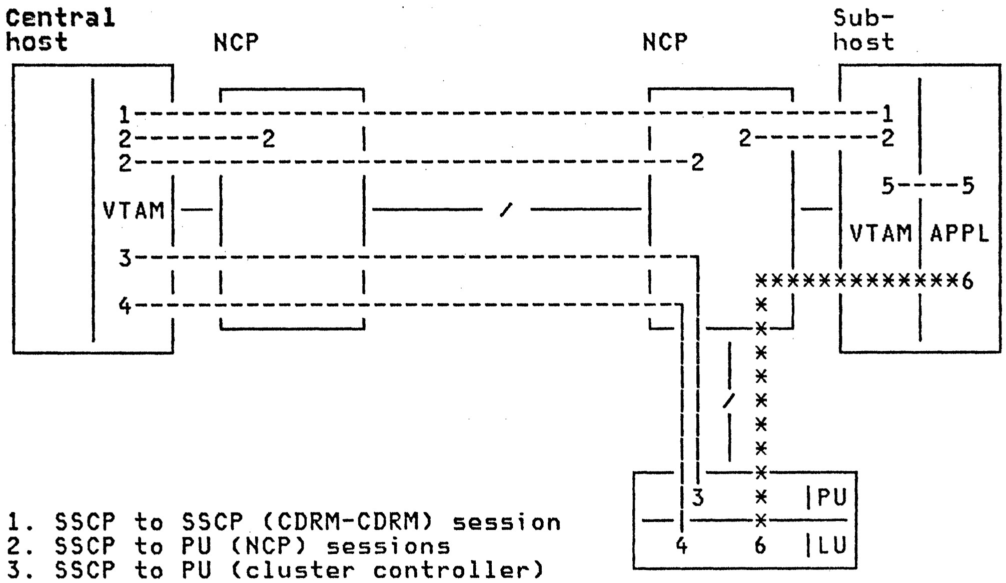
Logical connections between network components are called sessions in SNA. These sessions may be disrupted by a network component failure such as a failure of VTAM, an NCP, a line, and so on. Before the failures of different components are discussed here in this chapter, session disruption and recovery is covered more generally in this section.

As the reason for having a network is servicing the end users, the impact of network component failures on the user's data sessions has always to be considered. These sessions are called LU to LU sessions where the LU at one end is always an application program in a host and the LU at the other end can be a terminal such as an IBM 3277 display unit, or another application program located either in a host or in a cluster controller such as an IBM 8100 subsystem. LU to LU sessions are used to transfer user data.

Before an LU to LU session can be established (e.g. by logon to an application program), other sessions called control sessions have to be active. One session partner of the control sessions discussed here is always the System Service Control Point (SSCP) in VTAM. The other session partner can be another SSCP, an NCP, a cluster controller, or an LU. All these sessions are used for different tasks of network control. The control sessions are not always evident in the operational environment, though

- an SSCP to SSCP session is established by activation of a CDRM in another domain.
- an SSCP to application session is established when the application opens its ACB.
- an SSCP to PU/LU session is established by activation of the PU or LU respectively.

The following figure shows a sample which gives an overview of the control sessions needed to support a single terminal to application cross-domain session.



1. SSCP to SSCP (CDRM-CDRM) session
2. SSCP to PU (NCP) sessions
3. SSCP to PU (cluster controller) session
4. SSCP to LU (terminal) session
5. SSCP to LU (application) session
6. LU to LU (terminal to application) session

Figure 11. Sample sessions in a multiple domain configuration: The central host controls the PUs and LUs of both NCPs

In an SNA network, a non-recoverable failure of a network component breaks all sessions using that component (failure of a link in a multiple link TG is an exception). SSCP to PU/LU sessions can be automatically recovered by VTAM in case of a route failure, if there is an alternate route available. This allows an end user to re-logon to an application using a different route without operator intervention if his LU to LU session was also disrupted by the route failure. There are some more types of failures or types of sessions which are automatically recovered by VTAM. They are discussed later in this chapter. Reestablishment of broken LU to LU sessions and other sessions which are not recovered by VTAM, has to be done for instance by the end user, by the network operator, by automatically called NCCF CLISTs or by VTAM application programs.

VTAM allows separating the control sessions and the user data sessions by using different routes for them. This can diminish the impact of a session failure on other sessions and is especially true in case of the CDRM to CDRM session. Other cross-domain sessions can continue undisturbed if a CDRM to CDRM session fails.

When an SSCP to NCP session fails, e.g. by a VTAM failure, the NCP also breaks the SSCP to PU and SSCP to LU session for all resources which were activated by the lost SSCP. The LUs cannot establish new LU to LU sessions as long as VTAM has not reestablished the SSCP to NCP and SSCP to PU/LU sessions. The survival of the existing LU to LU sessions depends on various factors:

End users whose LU to LU sessions are not directly affected by the failure can continue their sessions if they use SNA terminals on none-switched lines (for the PU they are using, ANS=CONTINUE must be coded in the NCP deck). When VTAM reactivates the SSCP to NCP session it also tries to regain control over its physical and logical units by reactivating them. This process may disrupt the survived end user sessions. ACF/VTAM uses the SNA requests ACTPU(ERP) and ACTLU(ERP) when activating physical units and logical units, respectively. PUs and LUs which do not support these commands break existing sessions whenever they are activated by VTAM. At this time only a limited number of cluster controller types as for instance the

IBM SDLC 3271/3274/3275 support ACTPU(ERP) and ACTLU(ERP). The existence of ACTPU(ERP) and ACTLU(ERP) support is relevant in all types of failures where the SSCP to PU/LU sessions are broken but the terminal end user's LU to LU sessions are not touched. This can be for instance a VTAM, NCP or route failure. Let us have a look at the following figure to illustrate same examples:

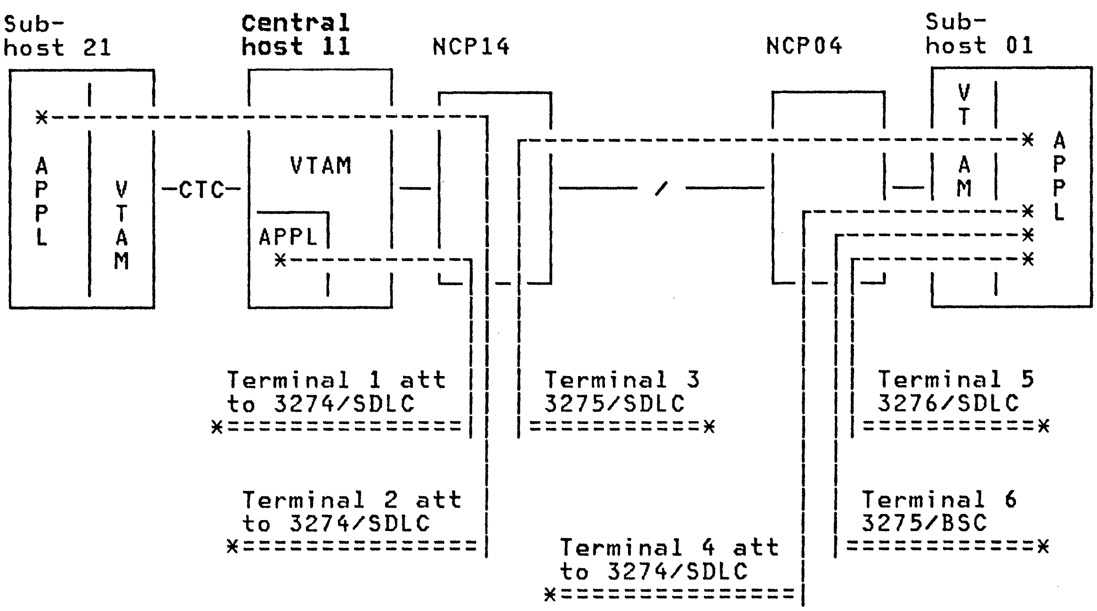


Figure 12. Sample of different LU to LU sessions

It is assumed that all terminals in the figure above are owned by the central host's VTAM. The impact on the end user's terminal to application sessions differs for different failures and terminal types. The failures considered here, are failures of VTAM on host 11, NCP14, and the cross-subarea link between NCP14 and NCP04.

Terminal 1 will lose its session if VTAM on host 11, or NCP14 fails (because this will break the LU to LU session)

Terminal 2 same as terminal 1

Terminal 3 will lose its session only if NCP14 or the link between NCP14 and NCP04 fails (because this will break the LU to LU session)

Terminal 4 can keep its session for all the above described failures even after restarting the failed components

Terminal 5 can keep its session for all the above described failures up to the time when the failed component is reactivated. The reestablishment of VTAM's session to the IBM 3276 PU and LUs will break all LU to LU sessions of that device because the IBM 3276 does not support ACTPU(ERP) and ACTLU(ERP).

Terminal 6 is a BSC terminal and will lose its session immediately after the SSCP to NCP session failure, which happens in all the above described cases.

The survival of an LU to LU session as described above, is not dependent on whether the same or another VTAM reestablishes the VTAM to PU/LU sessions. For instance, if in case of a permanent failure of the central host 11 VTAM on sub-host 01 would be used to take over NCP14 and NCP04 to control their network resources, then the ongoing sessions of terminal 3 and 4 would not be disrupted by this process.

The above description about sessions and session failures should show that a look at the sessions necessary to run an SNA network and the implications of different session failures should be considered and could influence network planning and configuration. In case the network terminals support ACTPU(ERP) and ACTLU(ERP), complete separation of the network and application functions to different host processors can be advantageous. You have a sample of this in Figure 11 on page 30 where no VTAM end user applications run on the central host processor (applications used to control the network and the systems are still necessary). Such a configuration is also known as a Configurations Management Configuration or CMC. A CMC can improve the availability of the network for the end users. In such a configuration a failure of the central processor is not any longer a very serious problem as the network does not need control functions continually. If the central host can be reactivated or backed up rapidly, the effects of its absence on the network as a whole are minimal and most of the users would not even notice it as long as they do not logoff or logon.

HOST FAILURE, RESTART, AND BACKUP

Failure of a host means that VTAM and all applications go down. Application subsystem data recovery and transaction resynchronization can be required. The impact on the end user sessions depends on many factors as described in section "Session failure" on page 29. In addition, the failure of the network control host means complete loss of central control. If reactivation of the host is possible, it does not differ very much from the initial activation process.

Host backup

If the failure of a host is expected to take a long time to recover (as in the event of a major hardware failure) it would be necessary to backup that processor. A backup host is normally channel attached to the original host's DASD drives and communication controllers. Locally attached terminals (e.g. IBM 3270) should be switchable between the original and the backup host. You can think of some exceptions to this but provisions have to be made that at least the original host's data is available at the location of the backup host.

From the view of network operating however, it is independent of whether a backup host is at a local or a remote location. The configurations shown in this section are therefore only used to illustrate the text and do not imply configuration recommendations. The more important difference is whether a sub-host or the central host is to be backed up. Backup of a sub-host means transferring applications to another host. This may also apply to a central host but backup of a central host requires additional network operational efforts. Please refer to section "Applications on a backup host" on page 36 for network operation requirements of application transfers.

Backup of the network control host

The operator actions required to backup the central host are depending on the resources available and the techniques used. The least complicated condition is the availability of a backup host which normally runs without VTAM or has VTAM just for test purposes. In this case the VTAM definitions of the original central host can be used and because VTAM's subarea can be retained there is not much difference from the initial activation process.

It is certainly more common that the backup processor is one of the sub-hosts. In this host an up and running VTAM is used which has a subarea number different to the one normally used on the central host. The operations necessary to be done on the backup host to regain control over the network and the sub-hosts are basically:

1. Gain ownership of all NCP's network resources

2. Make the tools for network and sub-host control available on the back-up host

NCP takeover

In order to control network resources via VTAM commands, VTAM has to be the owner of the addressed resource or, in other words, the resource must be an element of a domain which is controlled by that specific VTAM. Ownership also implies, that errors of a resource are reported to the owning VTAM(s). Some resources such as NCPs and cross-subarea links allow shared ownership by up to 8 VTAMs. The NCP's PUs and LUs however, can belong to one VTAM only at a time.

In a centrally controlled network the central VTAM's domain can comprise all NCPs in the network either channel or link attached to the central processor and all of the NCP's network resources. In case of a central VTAM's failure and backup by another VTAM, takeover of the NCPs and their resources are possible without reloading the NCPs or even disrupting some of the current sessions with other hosts. This is made possible by a facility of the network control program called Automatic Network Shutdown (ANS). By the ANS facility an NCP notices when it loses the ability to communicate with one of the owners of its resources. In such a case the network control program takes the following actions on behalf of the failed VTAM:

- It cleans up all sessions which end in or pass the NCP and end in or pass the failed VTAM. This does however not include deactivation of cross-subarea links. ANS=CONTINUE must be coded for PUs representing a 3705 and this garantees that the availability of such a link is not affected by ANS.
- The actions taken for LUs which have sessions to other domains and which are owned by the failed VTAM are depending on the type of terminal and the type of connection (switched/non-switched, BSC/SDLC) as described in section "Session failure" on page 29.

After ANS is processed by the NCPs, the domain of a backup host can be expanded by taking over the NCPs and their network resources. There are basically two methods to take over an NCP's network resources to another VTAM:

1. by acquiring them
2. by just activating them

Either of those methods can be used in a centrally controlled network and either of them can be used to take over a locally attached NCP or a remote NCP attached via a cross-domain subarea link.

For simplification of the following description the configuration shown in the next figure is used to illustrate the takeover operations.

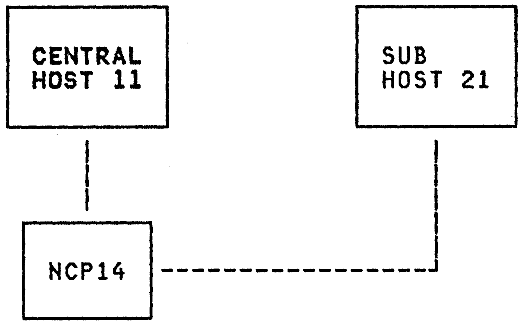


Figure 13. Sample Configuration: Two hosts share a single channel attached.NCP

Gain ownership by acquire

The first method has the advantage of being precise and of reducing the possibilities of operator mistakes. The requirements are that the NCP's network resources are pre-assigned to a specific VTAM. This is done by specifying the OWNER operand in the PCCU macro instructions and in the macro instructions that define the network resources (e.g. GROUP, LINE, PU, LU) as shown in the following figure:

```
HOST11    PCCU   .....OWNER=HOST11
            .
HOST21    PCCU   .....OWNER=HOST21,BACKUP=YES
            .
            .
P14020A   PU     .....OWNER=HOST11
```

Figure 14. NCP14 sample generation macro instructions: In addition to the OWNER operand, BACKUP=YES must be coded on the PCCU macro definition that represents a potential backup VTAM.

In respect to the above figures, an operator can activate NCP14 with any SCOPE operand from host 11 and from host 21, but he can display, activate, deactivate PU P14020A only from VTAM on host 11.

If the sub-host 21 has to backup the central host 11, the central operator has to acquire NCP14 by using the VTAM command

VARY NET,ACQ,....

The acquirement is in fact the assignment of a new owner for a given resource. If the resource is also to be activated, the ACT operand can be specified as part of the VARY ACQ command. The VARY ACQ command can be used in various combinations with SCOPE and ACT operands, but in general it must first be issued for the NCP itself and after that an individual VARY ACQ is required for every PU to be acquired. This could be a source of mistakes and time consuming in a large network. Therefore, an NCCF CLIST is very helpful to facilitate the VARY ACQ operation. Such a CLIST is shown as a sample in the appendix under headline "NCCF CLIST to ACQUIRE an NCP" on page 62.

Gain ownership by activation

The second method has the advantage that all network resources of an NCP can be taken over with only one VARY ACT command. This method requires that OWNER operands are not coded in the macro instructions that define the network resources. If a resource which cannot be shared has no pre-assigned owner, then the first VTAM to request activation of that resource becomes the owner. Thus, operational procedures have to be defined to achieve an orderly control of the NPC's resources. Referring to figure Figure 13 on page 34 the normal activation of NCP14 would be different for the central host 11 and the sub-host 21:

```
Host 11:   VARY NET,ACT,ID=NCP14

Host 21:   VARY NET,ACT,ID=NCP14,SCOPE=ONLY
           VARY NET,ACT,ID=L14....
           VARY NET,ACT,ID=L14....
```

The VARY ACT command on the central host 11 activates the NCP and all the NCP's network resources to their initial status. The first VARY ACT command on host 21 only activates the NCP. This makes the NCP an operative part of the network routes of host 21. No lines, PUs, or LUs are activated by this command. The second and third VARY ACT commands activate cross-subarea links for which sub-host 21 is a shared owner.

In case the sub-host 21 has to backup the central host 11 the central operator on host 21 only has to issue a single

```
VARY NET,ACT,ID=NCP14
```

to take over NCP14. This has the same effect as the complete take over process as described for the first method. Again, the impact on the ongoing user sessions on NCP14 is described in section "Session failure" on page 29.

Network and system control takeover

To fully control the network and the other sub-hosts from the backup host the following operations are necessary:

- Establish NCCF to NCCF and NCCF to OCCF sessions from the central backup host to the sub-hosts
- Start CNM applications like NPA and HCF if they are not already active on the backup host
- Regain control as a master terminal operator over subsystems like CICS/VS and IMS/VS

Provisions have to be made that all the CLISTs work properly on the backup host. E.g., NCCF's applid on the backup host differs from the applid on the original host. You have to take this into considerations if there are references to NCCF names in your CLISTs. These considerations should also relate to your network naming conventions as some other names are different when you run a backup central host.

Another slight problem is the NPDA data base as NPDA does not support data base sharing between hosts. If it is desirable to continually record all network errors in one data base the central host's data base has to be made available to NPDA on the backup host. For that, you have to bring down NCCF on the backup host no matter whether NPDA is running on that host or not. This is because NPDA runs in the same address space as NCCF and OCCF and the data base is statically allocated by definitions in the JCL procedure used to start OCCF/NPDA/NCCF. A modified JCL procedure which allocates the central data base to NPDA is then used for the restart of OCCF/NPDA/NCCF on the backup host. The supposition for that is naturally that the data base is physically accessible from the backup host.

NCP take back

After the failed central host has been revived, the NCP's resources have to be returned to their original owner in order to control the network from there. Neither VTAM nor NCP support an NCP take over 'in flight'. In general, the return of NCP resources to an original owner is disruptive for the sessions using the returning NCP. The non-shareable resources have to be deactivated on the backup host to make their activation from the original host possible. This will also break the LU to LU sessions. As cross-subarea links allow multiple ownership, their state can be preserved during the take back operations.

The description above implies that the reestablishment of network control from a backup sub-host to the central host is a process which can normally not be done during the main business hours. From the end user's point of view, the complete network would become unavailable for the time of the NCP take back procedure. However, if in case of a trade-off, it seems to be desirable to return NCP resources during a period of heavy network usage, there is an approach of a more soft take back. For that, the NCPs have to be artificially driven into ANS by disconnecting the backup host from the network. To disconnect a host from the network, the operator can deactivate the host's channel links. This deactivation breaks all routes between a host and the rest of the network, causing the NCPs to go through the ANS procedure with respect to the disconnected host. Channel connections are dynamically defined by VTAM when a channel attached NCP is activated. VTAM creates a name for a channel link and link station by using the communication controller's channel device name and adding -L for the link name and -S for the link station name. Channel links are addressable in a VTAM VARY INACT command. So, to disrupt a connection between a host processor and an NCP, activated e.g. through channel unit address 0C7, the network operator has to issue the VTAM command

```
VARY NET,INACT,ID=0C7-L
```

Such a command has to be issued for all NCPs channel attached to the backup host. This will disrupt the LU to LU sessions with the backup host's applications but LU to LU sessions with other hosts can be preserved as during the failure of the original host. Thereafter, the same facilities as described earlier in this section can be used for NCP take back.

APPLICATIONS ON A BACKUP HOST

For different reasons, an application may run on a backup host under a subarea number different from the one it normally uses. In order to make this situation transparent to the users of that application, the application should keep its name as it is defined to VTAM. It implies that the CDRSC definitions for that application have to be changed. This can be done by the VTAM command

```
F NET,CDRM=(new-cdrm,old-cdrm),ID=cdrsc-name
```

The command should be issued

- when the application is started on the backup host. It has to be issued on all hosts in the network, which have defined the application as a cross-domain resource, with the exception of the backup host itself.

- on every of the above mentioned hosts after IPL or VTAM restart, as long as the application executes on the backup host (this step can be avoided by using VTAM's configuration restart facility).

When the application runs on its original host again, a command causing a reverse change has to be issued.

All this is not a great thing but if it is forgotten, then complaints by the end users are inevitable. It should be therefore part of the operational procedures used to shift applications from one host to another. CLISTs can be prepared to propagate such a change of network definitions throughout the network.

VTAM FAILURE

At the current state of the product, ACF/VTAM seems to be a very reliable component in a communication network. Nevertheless, failure of VTAM is possible and it means that all sessions using that VTAM as a boundary or intermediate network node are disrupted. The recovery from a VTAM failure includes the following operations:

1. Detect VTAM failure
2. Reply to outstanding messages in TSO and NCCF
3. Cancel other VTAM applications which are in a hung state
4. Restart VTAM
5. Restart OCCF/NCCF
6. Restart other VTAM applications
7. Reactivate network nodes not included in VTAM's automatic start-up list
8. Reestablish interrupted sessions.

These operations can be more or less automated by means of CLISTs comparable to those used during system start-up. The proper commands and CLISTs have to be issued by the network operator and reestablishment of some of the interrupted sessions has to be done by the end user or by VTAM application programs.

Additional problems arise in a centrally controlled environment. The central operator's control over a sub-host is completely lost when the sub-host's VTAM fails. An automatic recovery from such a situation might be desirable but is not explicitly supported by any of the CNM products. You can put operator commands required to do step 2 to 7 in an OCCF CLIST but this CLIST has to be invoked manually at the sub-host site. Neither OCCF nor SOF can detect a VTAM failure and NCCF is dead at that time anyway. If OCCF had a facility comparable to NCCF where a specific message (e.g. the message telling that VTAM failed) can be intercepted and trigger the execution of a CLIST it would be quite helpful for automatic recovery of a VTAM abnormal termination on a remote sub-host.

Another possibility to recover from a sub-host's VTAM failure without manual intervention at the sub-host site is to restart VTAM manually from the central site. To do this, a VTAM independent access to the sub-host is required. In case the sub-host is an IBM 4300 processor the ROCF feature of these systems allows you to remotely access them via a switched line from a dedicated IBM BSC 3275 terminal or through MVS/OCCF. This access is hardware controlled at the IBM 4300 site and has nothing to do with any access method. Using ROCF makes the system console available at a remote site. With that a central operator is able to regain control of a sub-host and he can do the same things possible at a locally attached system console of a remote sub-host including IML/IPL.

There are other possibilities to remotely access sub-hosts independently of VTAM by using other teleprocessing access methods as for instance BTAM. As an example for that you can think of an NJE connection using BSC lines but those techniques are not further discussed here.

CDRM FAILURE

If a cross-domain resource manager fails, the central operator gets the message

    IST246I COMMUNICATION WITH CDRM ID=cdrmname LOST - REASON CODE ..

among others. The failure of a CDRM to CDRM session in itself does not disrupt any other sessions. Naturally, new cross-domain sessions between the affected domains cannot be established as long as the CDRM to CDRM connection is down. As VTAM does not automatically restart a failed cross-domain resource manager, message IST246I should trigger an NCCF CLIST which tries to restart the CDRM immediately. A sample CLIST is shown in the following figure.

```
&CONTROL ERR
* IST246I COMMUNICATION WITH CDRM ID = cdrmname LOST - REASON CODE nn
VARY NET,ACT,ID=&6
&WRITE &1 &2 &3 &4 &5 &6 &7 &8 &9 &10 &11
&WRITE ***************************************************************
&WRITE *    CLIST  IST246I COMPLETED FOR CDRM = &6                   *
&WRITE ***************************************************************
&EXIT
```

Figure 15. NCCF CLIST for restarting a failed CDRM to CDRM session after message IST246I

If the failure was because of a route failure and there is another operative route to the corresponding CDRM, the CDRM becomes active again. If there is no other route to the other CDRM, the operator should be alerted every 3 - 15 minutes that a CDRM to CDRM session is lost. The way to do this, is to set the I/O problem determination time-out interval through the VTAM command

```
F NET,IOPD,IOINT=time-out interval in seconds
```

to the proper value during network start-up. So, after failure of the CDRM and after the NCCF CLIST tried to restart the CDRM, the operator is notified that a CDRM to CDRM session is in a pending state every nn seconds by VTAM messages

```
IST530I AM GBIND PENDING FROM cdrm-name TO cdrm-name
IST532I EVENT ID=eventid
```

where nn is the time specified in 'F NET,IOPD...' command.

In a centrally controlled network, these messages remind the network operator that he has lost control over a whole domain.

CROSS-SUBAREA LINK FAILURE

A cross-subarea link is always part of a network route and a transmission group (TG). The effects of a link failure are different depending on whether the routes using that link

1. stay operative.
2. become inoperative but alternate routes are available.
3. become inoperative and no alternate routes are available.

Routes stay operative

If the failed cross-subarea link is part of a multiple link TG then no sessions are disrupted as long as one link in that TG is operative. The sessions will automatically use the remaining links of the TG but obviously, performance degradation is possible.

Routes inoperative but alternate routes available

If the failed cross-subarea link was the only or last operative link in a

TG then all routes using that TG become inoperative. All sessions that used the failed link are dropped. The sessions can be reestablished on an alternate route and in case of the SSCP to PU/LU sessions this is done automatically by VTAM. For all other sessions there is no automatic recovery by VTAM. Reestablishment of the broken CDRM to CDRM and LU to LU sessions has to be done by the network operator, by CNM programs, by the end user, or by VTAM application programs.

Routes inoperative and no alternate routes available

If the only available routes become inoperative caused by a cross-subarea link failure then all sessions using that link will be dropped and in the case of a permanent failure no recovery is possible. When the link is up again the failed sessions have to be reinitiated as described above.

The failed link may be backed up by a switched line. Such a connection has to be established manually and operators on both ends are involved in that procedure. This is because there is no special support for switched cross-subarea links by the NCP. The failure of a cross-subarea link usually creates problems because it is an important network component. Even backup links often carry some part of the network traffic. So, the failure of a cross-subarea link needs high attention by the network operator and there is a risk that standard VTAM and NPDA messages will be overlooked in the mass of console output. A good solution for that problem is to 'Freeze' and highlight one of the messages that tells about the link failure on an NCCF operator screen. To freeze a message means that it will not disappear from the screen even if the operator presses the CLEAR key. The message only disappears when the operator deletes it or the link is up again. However, this method needs some customization of NCCF but you can find a sample of that in a paper called 'CNM Customizing NCCF, GG24-1554'. For that reason it is not repeated here.

Automatic restart of a cross-subarea link by VTAM is dependent on where the connection is broken. If the connection between the two modems is interrupted then the line as defined in VTAM and NCP stays up and only the PUs on both sides go to a pending state. They will recover automatically as soon as the connection is up again. If the connection between the communication controller and the modem is broken (e.g. data set ready signal dropped) then both the line and the PU go to an inactive state on that side of the link where the interruption is located. To recover from that state the line and the PU have to be activated either manually or by an automatically started CLIST.

Lines and PUs pertinent to a cross-subarea link must be active on both ends of the link in order to make the link operative. Provisions have to be made that a reactivation of them is possible without further circumstances. So, multiple ownership of cross-subarea links could be advisable to make it possible that e.g. a sub-host can activate the link to the central host from his site.

Reload (re-IPL) of a remote communication controller can become necessary following a cross-subarea link failure. This is the case when the last or only link to a stand alone remote 3705 becomes inactive e.g. by a modem failure at the remote location. The line as defined in the 3705 becomes inactive and has to be reactivated by a VTAM VARY ACT command and for that, an active link is needed to the remote NCP. SDLC monitor mode does not reactivate a line which has failed due to modem/interface errors.

A problem may arise if a failed link is up again and you would therefore like to use your primary network route instead of the overloaded backup route. There is no special support by any of the network products to help you in such a situation. You have to break the sessions flowing on the backup route and reinitiate them in the same way described under headline "Routes inoperative but alternate routes available" above.

NCP FAILURE

As an NCP is part of a network route, the implications of a route failure as described in section "Cross-subarea link failure" on page 38also apply to the failure of an NCP. All sessions which went through or ended in the failed NCP are disrupted and must be reestablished.

The failure of an NCP can only be recovered by reloading the IBM 3705. VTAM will do this automatically if AUTOIPL=YES is specified in the PCCU macro instruction of the NCP deck. VTAM will also automatically produce a dump of the failed NCP if AUTODMP=YES and DUMPDS=dumpname is specified in the PCCU macro definition.

If AUTOIPL=NO, AUTODMP=NO, and DUMPDS=dumpname are specified, the failure of an NCP is distinctly reported on an NCCF screen. NCCF presents the VTAM messages

```
P00 IST095A OPTION TO DUMP ncpname AVAILABLE - REPLY YES OR NO ...

P00 IST284A OPTION TO RELOAD 3705 ncpname REPLY YES OR NO ...
```

highlighted and they will not disappear from the screen as long as the operator has not replied to them. This applies to NCPs loaded over a channel or loaded over a cross-subarea link. The same messages with outstanding replies go to the system console if NCCF is not up or if there is no operator logged on to NCCF who is defined as a message receiver.

Although AUTODMP=YES and AUTOIPL=YES seem to be the most comfortable way to recover from an NCP failure, it has some disadvantage:

- The NCP dump dataset may be overwritten by a new dump before the preceding dump is printed or saved.
- In case there is a software problem with the running NCP and the decision is made to run a different version of that NCP after the next failure, there is no way to tell this to VTAM via VTAM commands (assumed that every NCP version has a unique name). You have to rename the NCP deck in the VTAMLST data set so that VTAM cannot find it again after failure.
- In case of some serious hardware or software problems, the system may run into a loop, where the NCP is reloaded e.g. every hour.
- Because it is not so obvious to the network operator that an NCP failed, the restart of some sessions, which have been broken by the failed NCP, e.g. NCCF to NCCF, may be deferred, if the network operator has to restart them.

On the other hand it is advisable and seems to be mandatory to specify AUTODMP=YES and AUTOIPL=YES for NCPs channel attached to remote sub-hosts. Let us have an example for one reason: There is a central host and a remote sub-host and all routes to the sub-host go through one NCP as in Figure 16 on page 41.

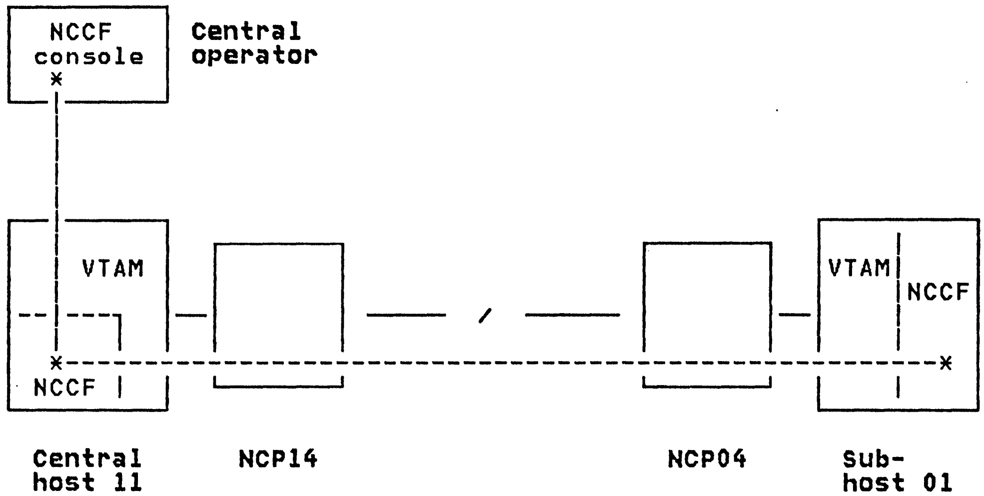


Figure 16. Configuration with a remote sub-host

AUTOIPL=NO, AUTODMP=NO, and DUMPDS=dumpname are specified in all PCCU macro definitions of NCP04. If NCP04 goes down the messages to dump and reload the NCP do not appear at any of the central operator's consoles. The link station controlling the cross-subarea link to the central host is also down if the NCP fails. The central host gets messages which tell about the route failure but it is not obvious on the central site, that an NCP went down. But even if it was obvious, there is no way to reload the NCP without intervention from the remote site.

The remote 3705 with NCP04 could have the Remote Program Load (RPL) feature installed, in order to load the NCP across the link. If RPL is active on the 3705 by the time NCP04 fails, RPL reports the failure to VTAM via the cross-subarea link which would trigger the messages

```
P00 IST095A OPTION TO DUMP ....     and
P00 IST284A OPTION TO RELOAD ....
```

on the central host 11. But this would not solve the above described problem. If an IBM 3705 has both RPL and channel attachment capability then only one of them can be active at a time. The RPL is activated by switching off the channel(s) and vice versa. In the example above, RPL must be switched off to allow sub-host 01 to access the network.

Another problem that has to be considered is more serious. An interlock condition can be created forcing part of the network into a hung state after a failure of an NCP which is channel attached to a remote sub-host and is defined with AUTOIPL=NO. The reason for this is that an NCP for which messages IST095A and IST284A are issued is in an transient state which is neither active nor inactive. VTAM notifies application programs whose LUs are affected by the NCP failure not before the decision is made whether the NCP will be reactivated again or stay inactive. The problem is, that if NCCF is to display messages IST095A and IST284A cross-domain at an NCCF console which is disconnected from NCCF due to the NCP failure, NCCF is not aware of loosing this terminal. NCCF waits indefinitely to deliver these messages and nobody in the network is notified of the NCP failure.

That is the main reason that AUTODMP=YES and AUTOIPL=YES have to be specified for NCPs channel attached to remote sub-hosts. Here is a sample to further clarify the problem: The central operator at host 11 (Figure 16) controls VTAM in sub-host 01 through an NCCF to NCCF session. He receives all the unsolicited VTAM messages from sub-host 01. If NCP04 fails, NCCF in sub-host 01 tries to send the messages

```
P00 IST095A OPTION TO DUMP ....     and
P00 IST284A OPTION TO RELOAD ....
```

to the central operator at the central host 11 because NCCF is not notified that it has already lost the session with the central host's NCCF. The messages get stuck in the VTAM buffers because of the NCP04 failure and it could take a little while until any operator realizes what really happened.

ROUTE EXTENSION AND PU FAILURE

A link from an NCP to a PU (other than an NCP) is called a route extension. Central network operation does not impact the treatment of route extension or cluster controller failures by VTAM or CNM tools. Nevertheless, some general operation hints are pointed out here in this section.

The failure of a route extension or a PU which are treated permanent by the NCP causes disruption of all sessions using that PU:

SSCP to PU
SSCP to LU
LU to LU

After the failure is cleared away, the sessions have to be reestablished. As stated earlier in this chapter, LU to LU sessions are not automatically reactivated by VTAM. For SNA terminals using a non-switched line, automatic reactivation of the SSCP to PU/LU sessions by VTAM is possible. This depends on the component causing the disruption of the sessions. This is explained in more detail in the following description in conjunction with next figure.

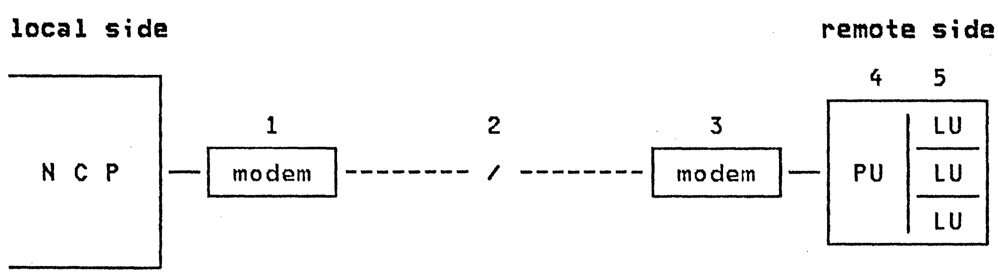


Figure 17. Sample of an NCP to cluster controller connection

You can perceive the possibility of an automatic recovery by looking at the state of the line and the PU in VTAM after the failure. Automatic recovery is attempted by VTAM if the line stays active and the PU is in a pending state. This is true in cases where the failure is located remote of the local modem(1). So, VTAM is able to automatically reestablish SSCP to PU/LU sessions in case of a

- line failure (2)
- failure of the remote modem (3)
- failure of the cluster controller (4)
- failure of an LU (5)

This includes the possibility to switch the cluster controller and the modem on and off at the remote side and resume operability without operator intervention from the central side. Failures of the modem(1) at the NCP side or a failure of the connection between the 3705 and the modem however, bring down the line, the PU, and the LUs. It requires that a VTAM VARY ACT command for them has to be issued.

Some software controlled communication controllers like the IBM 8100 require additional operator intervention in certain cases at the remote communication controller side. For instance, if the modem(3) at the PU side fails it is treated by the IBM 8100 the same way as a modem(1) failure at the local side by VTAM and the NCP. The link as defined in the IBM 8100 goes down and has to be reactivated by operator commands.

Cluster controllers on BSC lines like the IBM 3271 are not reactivated by VTAM after a permanent failure. VTAM reports a BSC controller failure by a whole bunch of messages and leaves the controller in an inactive state. Reactivation by means of an NCCF CLIST which is triggered by one of these messages is possible and can be helpful in a network with lots of IBM BSC 3271/3275.

OCCF/NCCF FAILURE

Central operator's control of a sub-host is mainly achieved via NCCF to NCCF and NCCF to OCCF sessions. The question is, what can be done when OCCF/NCCF goes down or hangs. Is there a possibility to recover from such a situation by central operation without manual intervention at the sub-host? The answer is yes. Other tools such as TSO and JES2/NJE can be used to bring OCCF/NCCF to life again. TSO helps to investigate the current state of OCCF/NCCF and JES2/NJE is used to issue JES2 and MVS commands, e.g. to cancel and restart it.

If communication from the central host's NCCF to a sub-host's OCCF/NCCF is lost because of the sub-host's OCCF/NCCF software problems the central operator can still logon to the sub-host's TSO. Within TSO he has two possibilities to get information about the state of OCCF/NCCF. The first one is the TSO OPER command. To use the OPER command the network operator's TSO user identification has to be authorized in the TSO SYS1.UADS data set. Under the OPER command a TSO user can issue a limited set of OS commands, e.g. DISPLAY R,LIST or DISPLAY A,LIST . Though he can see whether OCCF/NCCF is still active, he cannot cancel or restart it from there.

The other possibility to look at OCCF/NCCF under TSO is RMFMON. RMFMON is a program product which gives the user a lot of information about what is going on in every address space on an MVS system. So he can see whether OCCF/NCCF is swapped out or is in a loop or cannot get CPU cycles to work and so on.

After the central operator had a look at OCCF/NCCF he might decide to cancel and to restart it. For that he can use the NJE facility of JES2. The JES2 $N command is the tool to send JES2 or MVS commands through the network to other JES2 subsystems. The command carried piggy-back by the $N command is processed at the receiving host as it has been entered at the receiving host's system console. Here is a sample for what the central operator could have entered at his system console to cancel and restart OCCF/NCCF at a sub-host:

```
$N,D=N21;CANCEL OCCF

$N,D=N21;START OCCF,SA=21
```

In the above commands, N21 identifies the JES2 subsystem which is to receive the commands specified after the semicolon. If the commands are not JES2 commands, the receiving JES2 will pass the text to MVS for execution, but no attempt is made to return MVS responses. That is the reason for using TSO for MVS displays. JES2 commands sent by the $N command for execution in another JES2 subsystem will return responses to the sending JES2 console.

Command authority checks are made on all commands received from another node. Commands will be ignored if the required authority lacks. To execute the above mentioned commands the sending node needs network and system authority in the receiving node.

The $N command only works if an application to application session between the sending JES2/NJE and the receiving JES2/NJE has been established. So, the situation described here is one reason to interconnect the central host with its sub-hosts by NJE to NJE sessions during start-up time. Having an up and running TSO on every sub-host is another highly recommended provision. TSO and NJE are both standard facilities in an MVS/JES2 system.

CICS/VS AND IMS/VS

Although a break down of a CICS/VS or IMS/VS subsystem is mostly unpleasant for the end users, the restart does not cause any additional problems if CICS/VS or IMS/VS run on a central site controlled sub-host. The same procedures used to bring up the subsystems the first time after IPL can be normally used to restart them. But of course failure of other components may have an effect on the subsystem's operation, for instance what happens

- if CICS/VS or IMS/VS lose their master terminal
- if CICS/VS or IMS/VS lose their VTAM

The loss of a CICS/VS or IMS/VS master terminal does not immediately impact the subsystem's end users. Nevertheless, if in such a case the system console used as an alternate vehicle for master terminal operation is at the remote site the subsystems are out of central control. It is necessary that the central master terminal operator has to couple up to the subsystems again. He can do this in several ways: Via TAF or OCCF from an NCCF terminal or from a dedicated terminal. Provisions have to be made to allow this.

CICS/VS and IMS/VS are application programs which are able to stay up if VTAM goes down. All VTAM network traffic is disabled, therefore CICS/VS or IMS/VS close their VTAM ACB and watch for coming events. So, if VTAM comes up again communication to the end users via the SNA network can be resumed. This requires intervention by the master terminal operator. He has to issue

```
F cicsid,CSMT OPEN,VTAM     in case of CICS/VS or

R nn,/START DC              in case of IMS/VS
```

from a system console (CICS/VS or IMS/VS VTAM only environment assumed). It is logical that he cannot enter these commands from a dedicated master terminal, because all sessions from VTAM terminals to the subsystems have been disrupted. So, for a centralized network and system management the central operator needs to have access to the sub-host's system consoles and the best way to achieve this is via OCCF. Another method via NJE has the disadvantage that it is a one way access only. For the above described case the operator can transmit the commands to the sub-host but he will not get a message back (see "OCCF/NCCF failure" on page 43).

NETWORK COMMUNICATIONS CONTROL FACILITY (NCCF) RELEASE 2

Program Product. Program Number 5735-XX6
NCCF: General Information, GC27-0429
NCCF: Installation, SC27-0430
NCCF: Messages, SC27-0431
NCCF: Terminal Use, SC27-0432
NCCF: Customization, SC27-0433

NCCF is the key product for communication network management and is mandatory for controlling remote sub-hosts from a central site. In the beginning, it was a tool to ease network operation by transferring, and thus concentrating, the network related part of a system console's input and output, of one or several systems, to an NCCF terminal. Now with NCCF Release 2, more functions are available especially in cooperation with other CNM products for which NCCF is the base. NCCF operates as a VTAM or TCAM application program in its own address space or partition in MVS, OS/VS1 or DOS/VSE. When used with DOS/VSE systems, the program can also operate as a subtask in the VTAM or OCCF partition. NCCF is activated by starting it from the system console or by other techniques comparable to that. NCCF uses IBM 3270 devices as operator terminals and hardcopy printers. To gain access to NCCF an operator must logon and identify himself to NCCF. Depending on his level of authorization he may then make use of the various functions provided. He may be authorized to control the whole network and all its systems or be limited to information only type of functions.

Here is an overview of the NCCF functions:

- **Operator control.** NCCF operators can enter VTAM and TCAM commands or invoke NCCF command lists to modify and display the network configuration. A terminal logged on to NCCF may also receive unsolicited messages indicating an unrequested change of state of a network resource.

```
NETWORK COMMUNICATIONS CONTROL FACILITY                      02/26/82 09:20:43
   NCF01     IST089I  SWSYS34  TYPE= SW SNA MAJ NODE   , ACTIV
   NCF01     IST089I  ISTCDRDY TYPE= CDRSC SEGMENT     , ACTIV
   NCF01     IST089I  N45EF3N  TYPE= PU_T4/5 MAJ NODE  , ACTIV
C  NCF11 P%  IST621I  RECOVERY SUCCESSFUL FOR NETWORK NODE P14022C
*  NCF11     DIS P140A0F
C  NCF11     DISPLAY NET,ID=P140A0F,E
   NCF11     IST075I  VTAM DISPLAY - NODE TYPE= PHYSICAL UNIT
   NCF11     IST486I  NAME= P140A0F  ,STATUS= ACTIV           ,DESIRED STATE=
             ACTIV
   NCF11     IST081I  LINE NAME= L140A0    , LINE GROUP= G14S1     , MAJNOD=
             N14BF3N
   NCF11     IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
   NCF11     IST355I  LOGICAL UNITS:
   NCF11     IST080I  T140A0F1 ACT-NOSE   T140A0F2 ACT-NOSE   T140A0F3 ACT-NOSE
   NCF11     IST080I  T140A0F4 ACT/S      T140A0F5 ACT-NOSE   T140A0F6 ACT-NOSE
   NCF11     IST080I  T140A0F7 ACT-NOSE   T140A0F8 ACT-NOSE
-  NCF23   % DSI020I OPERATOR WTCRES2  LOGGED ON FROM TERMINAL H23L3E1  USING
             PROFILE(PROFCD  ),HCL(        )
--------------------------------------------------------------------------------
   NCF01     IST089I  RENATE   TYPE= CDRSC SEGMENT     , ACTIV
   NCF01     IST089I  R91ACICS TYPE= CDRSC SEGMENT     , ACTIV
???
_
```

Figure 18. Example of NCCF display: Messages from several domains (NCF01, NCF11, NCF23) are displayed at the NCCF terminal.

- **Data security.** Operator access control is achieved through a password-protected logon. Under MVS, the password may be RACF controlled.

- **Cross-domain communication.** An NCCF operator can communicate with multiple NCCFs located in different domains simultaneously from one terminal.

- **Command lists.** Users can code sequences of VTAM, TCAM, NCCF commands and NCCF control statements into command lists (CLISTs), which are stored in a partitioned data set. This partitioned data set is defined in the NCCF start-up JCL procedure and the CLISTs are invoked by name from an NCCF terminal or another CLIST for execution when required. Furthermore CLISTs can be named after a TCAM or VTAM message number identification. The CLIST is then invoked every time the access method would issue this specific message. CLIST control statements and control variables are available to control the execution sequence, conditionally substitute values at execution time, communicate with the operator at execution time, and so on.

- **Initial commands and CLISTs.** A user specified command or CLIST can be automatically executed after NCCF is started, or after an operator's logon.

- **Timer-initiated commands and CLISTs.** By use of the NCCF commands AT and EVERY, CLISTs and commands can be scheduled for execution at a specified time or repetitively at specified intervals of time.

- **Program function key tailoring.** The meaning of IBM 3270 PF keys can be defined by the installation. So operator keystrokes can be reduced by PF key representation of NCCF functions.

- **Span of control.** An operator's control can be restricted to a subset of the network's resources.

- **Scope of commands.** An operator's control can be restricted to a subset of commands, CLISTs, and operands.

- **Customization.** Using NCCF's macro services an installation may write its own command processors, exit routines, and subtasks. These provide additional functions beyond those provided by standard NCCF.

- **Related IBM products.** As mentioned earlier NCCF is a program base upon which other IBM-supplied programs may be added. The programs available today are:

  - NCCF Terminal Access Facility
  - NPDA
  - VSE/OCCF and MVS/OCCF
  - Information/System Release 2

  They are described later in this chapter.

NCCF TERMINAL ACCESS FACILITY

The Terminal Access Facility is an optional feature of NCCF Release 2 (ACF/VTAM and ACF/VTAME only). Throughout this paper the acronyms NCCF/TAF or TAF will be used to make writing and reading easier.

NCCF/TAF is a terminal simulator program which consists of a collection of NCCF command processors and VTAM exits. It is a facility which allows communication from an NCCF terminal to

IMS/VS 1.1.6 and IMS/VS 1.2
CICS/VS 1.5
IBM 8100/DPPX through HCF Release 2
IBM 8100/DPCX through HCF Release 2

and subsequent releases. Within the following description these subsystems are jointly called 'target systems'. NCCF/TAF may be used with other applications, such as NPA, but there is no IBM support for them.

NCCF/TAF supports two distinct modes of operation: **standard control mode** and **full-screen mode**.

- In **standard control mode**, NCCF/TAF acts in a line-by-line fashion as an IBM SNA 3767. An operator using an NCCF terminal can start a session with one or more target systems. After such a command the operator is ready to send and receive commands and messages to and from these target systems. Because messages from target systems are intermixed with each other and with the NCCF output each line has a prefix which identifies the related target system.
  NOTE: Standard control mode is not supported for IBM 8100/DPCX.

- In **full-screen mode**, NCCF/TAF lets an NCCF operator interact with display-oriented applications on CICS/VS, IMS/VS, and through HCF, IBM 8100/DPPX and IBM 8100/DPCX systems without logging off from NCCF. The entire screen is 'handed over' to the target system after which the entire NCCF screen is owned by the target system application.

  A NCCF operator can establish sessions with multiple target systems from one NCCF terminal. Only one target system can use the NCCF/TAF display screen at a time, the others are in a disconnected state, but sessions are active. While the NCCF operator interacts with these full-screen application programs, messages that are intended for that operator's screen (such as ACF/VTAM messages) are kept and displayed when the operator exits from full-screen mode. The operator may optionally choose to have full-screen mode automatically interrupted when these messages arrive. The operator can logically disconnect/connect his NCCF terminal with each of the established sessions without doing a logon/logoff command sequence.

  In full-screen mode NCCF/TAF is defined as only one LU per NCCF operator. This implies that the same 'LU name' must be defined in all target systems. It also implies that HCF full-screen mode can only control one DPPX system without **DROP/**ACQUIRE or logon/logoff process. A unique 'LU name' must be defined for each operator that is to have sessions with the subsystems at the same time.

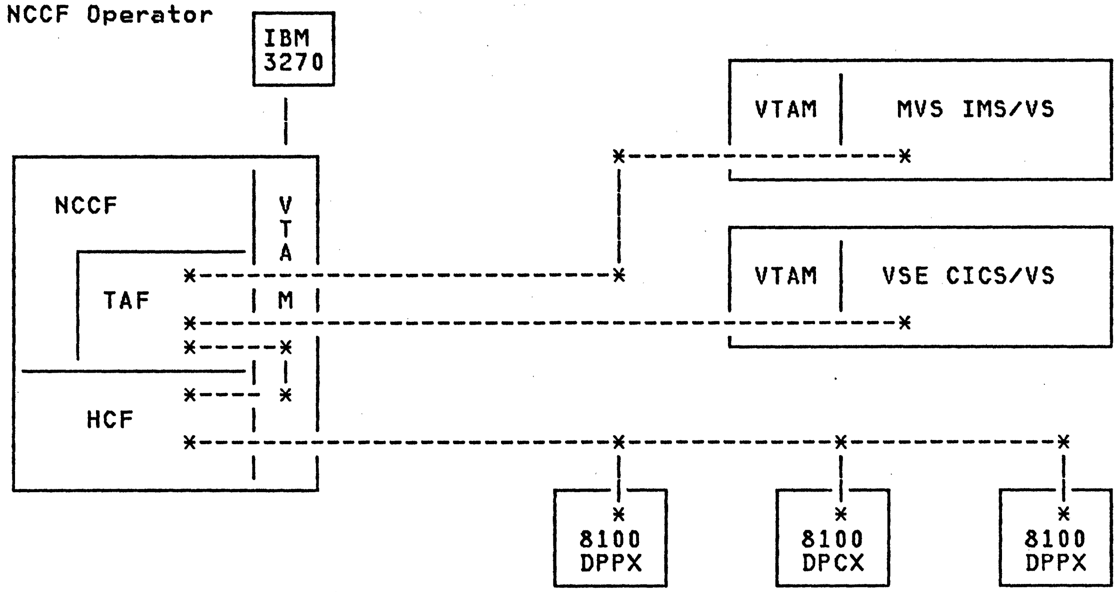


Figure 19. Centralized operation with NCCF/TAF: One NCCF operator controlling one IMS/VS, one CICS/VS, one IBM 8100/DPCX, and two IBM 8100/DPPX.

The operator interactions needed in NCCF/TAF are contained in five NCCF commands (with parameters) and a PA key function used to disconnect from a full-screen session.

BGNSESS	start a session with an application
ENDSESS	stop a session with an application
SENDSESS	send a command to an application (standard control mode)
LISTSESS	list status of NCCF/TAF sessions
DISCONNECT	Program attention key (user selected) (full-screen mode)
RTRNSESS	reconnect to a session with an application "

Some of the commands are pretty lengthy in their basic form. With NCCF's CLIST facilities, it is possible to make operations simpler and easier to use. You may refer to a paper called 'CNM NCCF Terminal Access Facility, GG24-1540' which shows sample CLISTs for use of TAF in conjunction with CICS/VS, IMS/VS, HCF, and NPA.

NETWORK PROBLEM DETERMINATION APPLICATION (NPDA) VERSION 2

Program Product. Program Number 5668-983
NPDA: General Information, GC34-2061
NPDA: Installation, SC34-2066
NPDA: User's Guide, SC34-2063
NPDA: Recommended Action Guide, SC34-2064
NPDA: Messages and Codes, SC34-2065

NPDA assists users in performing problem determination. The program automatically collects statistical data and information about unusual events detected by communications network resources and stores them into a data base. For MVS users, NPDA Version 2 extends device error support for selected tape, DASD, and printer devices in the network host processor system, as well as for the CPU and channels of that system. The NPDA user has access, via an NCCF terminal, to the accumulated information which includes:

- Identification of the resource on which a specific alert, statistic, or event has occurred.
- Description of alerts and events.
- Probable cause of alerts and events based on an analysis of the recorded data.
- Recommended actions that the user may follow to correct or override the problems described in the alert or event.
- Accumulated statistics about temporary, or recoverable, error events that may be used to help analyze performance degradation and intermittent failures.

NPDA operates as a series of command processors under NCCF in the NCCF address space or partition. Collecting data and displaying data are independent of each other and are therefore initiated at different times. The data collection is an automatically process which is started as soon as NPDA/NCCF is initialized.

```
NETWORK COMMUNICATIONS CONTROL FACILITY                     02/26/82 09:24:42 A
NPDA-40A                          * TOTAL EVENTS *               PAGE   1 OF   1
                               * FOR SELECTED RESOURCE *

DOMAIN
NCF11
-------------------------------------------------------------------------------
     **************** RESOURCE *****************        ***** ATTACHED ******
SEL# TYPE RESNAME  TOTAL      FROM         TO               TOTAL       TO
( 1) COMC N043F3M      2  02/23 08:06  02/24 12:55            231  02/25 23:19
( 2) COMC N14BF3M      0  00/00 00:00  00/00 00:00             32  02/25 22:32
( 3) COMC N14BF3N     35  02/17 09:06  02/23 15:11            106  02/26 09:21
( 4) COMC N245FNN      7  02/22 11:17  02/26 02:07            134  02/26 09:23
( 5) COMC N45EF3N      3  02/19 10:31  02/25 20:39              3  02/23 20:49
( 6) 8100 DOM2         0  00/00 00:00  00/00 00:00             19  02/24 18:31
( 7) 8100 DOM3         0  00/00 00:00  00/00 00:00             15  02/24 08:45
( 8) 8100 BABE         0  00/00 00:00  00/00 00:00              2  02/25 13:18
( 9) 8100 TTE6         0  00/00 00:00  00/00 00:00              1  02/24 15:37


ENTER 'ST'(STAT), OR SEL# (ATTACHED), OR SEL# PLUS ' M'(MOST RECENT)

??? ***
_
```

Figure 20. Example of NPDA Total Events Display: This display shows total number of events. The user is guided to other information, e.g. to a display which shows the most recent events for a specific component (see next figure).

```
NETWORK COMMUNICATIONS CONTROL FACILITY                    02/26/82 09:31:59 A
NPDA-41A                    * MOST RECENT EVENTS *               PAGE   1 OF   1
                           * FOR SELECTED RESOURCE *

DOMAIN    TYPE RESNAME  TYPE RESNAME   TYPE RESNAME
NCF11     COMC N245FNN  LINE L24020    CTRL P24020E
--------------------------------------------------------------------------------
SEL#    DATE/TIME    EVENT DESCRIPTION:PROBABLE CAUSE                   ETYP ACT
( 1)   02/26 09:23   COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE    PERM  27
( 2)   02/25 17:02   COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE    PERM  27
( 3)   02/25 14:12   COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE    PERM  27
( 4)   02/25 11:36   COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE    PERM  27
( 5)   02/24 15:26   POWER OFF DETECTED:DEVICE OFF/DEVICE               PERM  28
( 6)   02/24 11:47   DSR ON CHECK:LOCAL MODEM OFF/LOCAL MODEM           PERM  16
( 7)   02/24 11:26   POWER OFF DETECTED:DEVICE OFF/DEVICE               PERM  28
( 8)   02/23 18:12   POWER OFF DETECTED:DEVICE OFF/DEVICE               PERM  28
( 9)   02/23 16:23   POWER OFF DETECTED:DEVICE OFF/DEVICE               PERM  28
(10)   02/23 15:36   REMOTE MODEM-NO RESPONSE:MODEM OFF/LINE/MODEM      PERM  34
(11)   02/23 15:32   COMMUNICATION ERR:DEVICE/REMOTE MODEM INTERFACE    PERM  27

ENTER 'ST'(STAT), OR SEL# (ACTION), OR SEL# PLUS ' D'(DETAIL) OR ' P'(PROBLEM)

??? ***
_
```

Figure 21. Example of NPDA Most Recent Events Display

NPDA data can be displayed on an NCCF terminal only. The terminal is shared between NPDA and NCCF and no separate logon is required. NPDA commands and other commands can be entered in any sequence. A PF key can be assigned to NPDA which is then used as the NPDA enter key to allow NCCF to distinguish between NPDA commands and other input. NPDA produces full-screen displays. Output produced by NCCF will partly or completely overlay NPDA output.

The NPDA data the user can view is classified as **event data** if it relates to permanent errors, or **statistical data** if it relates to temporary errors and traffic. Included in the event data are records created by NPDA from analysis of statistical data which indicate that user specified thresholds have been exceeded. The **alert data** is a subset of the event data, which requires immediate attention.

By issuing the NCCF NPDA command the first time (pressing for instance the NPDA assigned PF key) the user gets the NPDA menu display. From that menu he selects a data type (alert, event, or statistics) and then may either step through a procedure that pinpoints a failing resource or, if he is already aware of which resource is failing, go directly to data about that resource.

In addition to having access to the information in the user's home domain, he can also view SNA data in another domain if an NCCF to NCCF cross-domain session is in progress and if a peer NPDA is operating in the target domain.

The recording of data on the data base and the display of the data can be controlled by NPDA filter commands.

NPDA also interfaces with INFO/Management for automated problem entry into the INFO/Management data base.

MVS OPERATOR COMMUNICATIONS CONTROL FACILITY (MVS/OCCF)

Program Product. Program Number 5665-288
MVS/OCCF: General Information Manual, GC24-5225

MVS/OCCF allows one or more remote MVS/SP-JES2 systems to be operated from a host and is also designed for simplifying MVS/SP-JES2 console operation. Furthermore it supports the Remote Operator Console Facility (ROCF) a hardware function of IBM 4300 processors. Here is a brief description of MVS/OCCF and its functions:

MVS/OCCF is activated by starting the OCCF task either from an MVS console or by other techniques comparable to that. NCCF or NPDA/NCCF run as subtasks of MVS/OCCF if they all run on the same processor.

- **Remote operations / Message routing.** An operator on an NCCF terminal can logon to MVS/OCCF located either in the same domain or in a remote domain. He may then enter MVS, VTAM, TCAM, and JES2 Commands from that NCCF terminal. He may also get all the messages (depending on MVS/OCCF start-up parameters) which normally go to the MVS console. The NCCF screen is logically made an MVS console. Although only one NCCF operator/terminal may communicate with one MVS/OCCF on a specific host, an NCCF terminal can communicate with multiple MVS/OCCFs on different hosts.

- **ROCF support.** The ROCF support allows the user to IML/IPL and operate remote IBM 4300 processors through a switched BSC 1200 baud connection from an OCCF/NCCF terminal. It gives the OCCF/NCCF user the ability to access a remote IBM 4300 host independent of the availability of VTAM on that system.

- **MVS/OCCF command lists (CLISTs).** Users can code sequences of MVS, VTAM, TCAM, JES2 commands and MVS/OCCF control statements into command lists (CLISTs), which are stored in a partitioned data set. This partitioned data set is defined in the MVS/OCCF start-up JCL procedure and the CLISTs are invoked by name from an MVS console or another CLIST for execution when required. They can of course also be invoked from an NCCF terminal from which a session with OCCF is in progress. MVS/OCCF CLISTs are distinguished from MVS and JES2 commands by the first character. This character is defined by the user as an MVS/OCCF initialization parameter (Throughout this paper a % character is used to designate an MVS/OCCF CLIST). MVS/OCCF CLIST logic and MVS/OCCF control statements supply functions like

  - substitution of variable parameters at CLIST execution time.
  - conditional flow and execution of the commands by means of "IF .... GOTO ..." logic.
  - delay processing of commands in a CLIST at execution time for a specified number of seconds.
  - WTO

- **Automatic message reply.** By specifying message replies in a so called message action table MVS/OCCF will reply to a specific message id with a specific response.

- **DISPLAY facility.** The content of MVS/OCCF CLISTs can be displayed on the MVS console. By concatenating JCL procedure libraries, NCCF CLIST libraries, etc. to the MVS/OCCF CLIST library all of the procedures specified in these libraries can be displayed on the MVS console.

MVS SECONDARY OPERATOR FACILITY (SOF)

Field Developed Program. Program Number 5798-CRE
SOF: Availability Notice, GB21-2179
SOF: Program Description/Operations Manual, SB21-2180

SOF is designed to eliminate or reduce operator errors by allowing MVS console operation with simplified commands, and automatic command or job submission. There is a CLIST capability in SOF which is very much similar to the one provided by MVS/OCCF. However, MVS/OCCF lacks some of the SOF functions and these are marked with *) in the following description of SOF functions:

- **SOF command lists (CLISTs).** Users can code sequences of MVS, VTAM, TCAM, JES2 commands and SOF control statements into command lists (CLISTs), which are stored in a partitioned data set. This partitioned data set is defined in the SOF start-up JCL procedure and the CLISTs are invoked by name from an MVS console, from another CLIST, or at *)SOF initialization time for execution when required. SOF CLISTs are distinguished from MVS and JES2 commands by a / as the first character.
  - substitution of variable parameters at CLIST execution time.
  - conditional flow and execution of the commands by means of "IF .... GOTO ..." logic.
  - delay further processing of commands in a CLIST for a specified number of seconds.
- ***)Time of Day Event Scheduler.** This facility allows the automation of job, command or SOF CLIST submission at a user specified date and time.
- ***)Initial Clist execution.** This facility allows the execution of a clist at initialization of SOF.
- ***)JES internal reader interface.** SOF CLISTs can be routed to the JES internal reader. This function makes it possible to submit MVS jobs from an MVS console or submit them at a user specified time.
- **DISPLAY facility.** The content of SOF CLISTs can be displayed on the MVS console. By concatenating JCL procedure libraries, NCCF CLIST libraries, etc. to the SOF CLIST library all of the procedures specified in these libraries can be displayed on the MVS console.

SOF itself is activated by starting the SOF task either from an MVS console or by other techniques comparable to that. SOF is a product that works independent of other communication network management tools, and it has no NCCF interface. SOF CLISTs can be invoked from an NCCF terminal only through OCCF. Although some of the SOF functions overlap with MVS/OCCF functions SOF still seems to be a valuable tool e.g. to

- automate the IPL procedure and the MVS and network activation to a certain degree either on the remote or the central site.
- check network components at user defined intervals and restart them if necessary or alert the network operator.
- reduce operator skills at the remote site by means of predefined operating procedures.
- start and stop applications, maintenance jobs, backup jobs etc. at a user specified, predefined date and time.
- Used to complement MVS/OCCF. It is not dependent on teleprocessing access method and can be used to monitor MVS/OCCF.

NETWORK PERFORMANCE ANALYSER (NPA)

Field Developed Program. Program Number 5798-CZR, 5798-CZT
NPA: Availability Notice, GB21-2478
NPA: Program Description/Operations Manual, SB21-2479

The Network Performance Analyzer (NPA) monitors, collects, and displays network performance data which may be used for:

- Highlighting causes of performance degradation
- Tuning networks for better performance
- Capacity planning for future growth

The data gathered by NPA is available for online and offline evaluation. The FDP comprises two products, a host application program (Number 5798-CZR) and an extension to the NCP (Program number 5798-CZT). They run under OS/VS1 or MVS, with VTAM and/or TCAM. NPA has a companion FDP (Network Performance Analysis Reporting System, NETPARS, program number 5798-CZX) which creates structured reports from NPA log output.

Highlights of NPA functions:

- **Collection** of 3705, NCP, message traffic, and line control statistical data by user criteria. In a multi-system network, NPA can collect data from every NCP with which it can communicate.
- Dynamically changing **immediate display** of statistics based on the collected data.
- **Review display** of previously collected statistics.
- Data of particular significance may be **monitored** against user specified criteria and exceptions reported as they occur.
- Collection, display, and monitoring can **automatically start** after NPA initialization or at a specified time of day.

```
 13:45:26  FOR RESOURCE L14022   THE ERRCNTS  VALUE OF    17  WAS ABOVE THE
MONITOR LIMIT OF     10
                     * * NETWORK PERFORMANCE ANALYZER * *                UNLOCKED
      13:44:56                  DISPLAY RESPONSE              02/25/82
  NAME        TOT   MIN.SC OUTQ MSG/M CH/S PLN% SLN% PLL/M %NEG ERRS REMSG RECHR
N14BF3N  NCP         00:47  % CCU UTIL= 16  % IN SLD= 00 CHHLDQ=   2 CHINTQ=   1
         NCP BUFFERS        FREE=1898 HIGH=1907 LOW=1897 MAX=1698 SLD LIMIT= 212
L14024   LINK        00:47                     00 NONE
L14026   LINK        00:47          16  176    02 NONE    600   97
L14028   LINK        00:47    1      7  282    03   01    600   99
L1402C   LINK        00:47           2  248    03   01    600  100
L14040   LINK        00:47              240    15   05    600  100
L140A5   LINK        00:47              120    10 NONE    600  100
L140A0   LINK        00:47    1     32  132    15   07    289   95      1
P140A0F  PU          00:47    1     32  132               289   95      1
T140A0F1 LU          00:47
T140A0F2 LU          00:47
T140A0F3 LU          00:47          12
T140A0F4 LU          00:47
T140A0F5 LU          00:47           2
T140A0F6 LU          00:47          18

                                                                     PAGE:
```

Figure 22. Example of NPA display: The upper two lines show a monitor message. The other data is displayed in response to one or several START DISPLAY commands. The display is updated at user specified time intervals.

NPA is activated by starting it either from a system console or by other techniques comparable to that. In order to use the online facilities of NPA the user has to logon to NPA from a 3270 screen. He can then enter commands and receive output from NPA such as statistic display or monitor messages. Using NPA is quite straightforward, since there are only a few NPA commands:

- START/STOP COLLECT tells NPA to begin collecting performance data on one or more network resources (immediately or at a future time).
- START/STOP DISPLAY initiates collection and display of data (the data displayed is changed at periodic intervals).
- START/STOP MONITOR is similar to Display, but accepts a range of threshold values and if the measured parameter falls outside of the range, a message is displayed in the top two lines of the screen.
- REVIEW causes the display of interval and total records for a given resource.
- STATUS shows the network resources for which START COLLECT/DISPLAY/MONITOR commands have been issued.

Note: NPA does not support terminals that have been dynamically reconfigured.

HOST COMMAND FACILITY (HCF) VERSION 2

Program Product. Program Number 5668-985
HCF: General Information Manual, GC27-0453
HCF: User's Guide, SC27-0455

HCF is a VTAM or TCAM application program for MVS and DOS/VSE, which allows a System/370 terminal user to access and control a connected IBM 8100/DPPX or IBM 8100/DPCX subsystem. HCF is essential when controlling IBM 8100 systems from an MVS or DOS/VSE host.

The user's terminal logically belongs to the IBM 8100 system, though the System/370 user has the ability to

- interactively operate and control IBM 8100 systems
- use all operation and service facilities available in an IBM 8100 system, except those requiring operator intervention, such as mounting a tape
- use any DPPX or DPCX application program in an IBM 8100 system
- perform problem determination and error diagnosis tasks that do not require manual intervention on the IBM 8100 system

HCF supports IBM 3270 displays and IBM 3767 terminals as workstations. HCF allows several users to access the same DPPX or DPCX subsystem from different terminals at the same time. Each user, however, may access only one subsystem through HCF at a time. HCF may also be used through TAF from an NCCF terminal (see "NCCF Terminal Access Facility" on page 47 for more information).

Using HCF is pretty simple. First, a user has to logon to the VTAM application HCF. After that, the HCF commands

**ACQUIRE and **DROP

are used to connect/disconnect to/from a specific application in a specific IBM 8100 system.

INFORMATION/SYSTEM(INFO/SYSTEM) RELEASE 2

Program Product. Program Number 5735-OZS
INFO/System: General and Pre-Installation Information Manual, GC34-2027
INFO/System: Installation and Customization, SC34-2029
INFO/System: Messages and Codes, SC34-2043
INFO/Management: User's Guide, SC34-2031
INFO/Management: Scenarios and Panel Flow, SC34-2045

INFO/System contains three components which are nearly independent: INFO/MVS, INFO/Management, and INFO/Access. INFO/MVS and INFO/Access allow access to IBM supplied data bases which contain technical information pertinent to the MVS environment. This information is mainly used by system programmers for software problem resolution.

The part of INFO/System most useful in the operation environment is INFO/Management. The facilities supplied by INFO/Management provide for manageability and control of the data processing operation in the areas of:

- Problem Management
- Change Management
- Configuration Management

With INFO/Management, the user creates, updates, displays, and prints records that document his installation's data processing problems, changes, and system components. These records are stored in the INFO/Management data base and can be searched according to the user's criteria. For example, he may search for all open problems that have occurred at a particular location, all changes scheduled for a specific date, the names of personnel responsible for servicing a component, or relationships between certain problems, changes, and system components.

INFO/Management is essentially a panel-driven system, whereby the user is prompted for the information necessary to create, retrieve, and update records. In addition to the panels which enables the user to create, search, and display records, a set of subcommands are used to invoke special functions and to manipulate the data collected by the panels.

The problem management part is connected to NPDA. Initial problem information can be extracted from the NPDA data base and copied to the INFO/Management data base by entering a simple command under NPDA.

INFO/System operates as a command processor under TSO or NCCF running on MVS. For DOS/VSE users, a CICS based FDP called Account Network Management Program (ANMP) provides functions similar to INFO/Management.

For the best use of system resources, INFO/SYSTEM should be executed under a TSO session and only the NPDA interface used under NCCF. The TSO session can be established via the TAF feature of NCCF.

NCCF CLIST: HELP

```
&CONTROL ERR
&A = &1
&IF .&A EQ . &THEN &GOTO -HELP
&IF &A EQ HELP &THEN &GOTO -HELP
&IF &A EQ ? &THEN &GOTO -HELP
AUTO1 NO
&B = &SUBSTR &A 1 4
CLR1                             <===  The CLR1 command is described in
HELP&B &2                              'CNM Customizing NCCF, GG24-1554'
&IF &RETCODE EQ 0 &THEN &EXIT
&A ?
&EXIT
&IF &RETCODE EQ 0 &THEN &EXIT
-HELP
CLR1
&BEGWRITE -END
******************************************************************
* HELP0000        HELP FUNCTION                                  *
*                                                                *
* SELECT ONE OF THE FOLLOWING COMMANDS FOR SPECIFIC HELP:        *
*                                                                *
* COMMAND          AREA WHERE IT IS APPLIED                      *
*---------        --------------------------                     *
* CLISTS      To show installed CLISTS for VTAM/NCCF             *
* NCCF        To show the format of NCCF commands                *
* HELPOCCF    To show the format of OCCF commands                *
* HELPTAF     To show the format of TAF commands                 *
* NPDA HELP   To show how to use NPDA                            *
* SENSE       To show the meaning of sense codes                 *
* ST(STATUS)  To determine VTAM status modifiers                 *
* INFO        To show how to use INFO/MANAGEMENT                 *
* DEMOS       To demonstrate FULL PANEL                          *
* TOOLS       To show which problem determination tools          *
* HELPPFK     To show the use of programmed functions keys       *
******************************************************************
-END
&EXIT
```

CLISTs to activate network nodes

SOF CLIST ACT is invoked by entering: /ACT ....

```
&OS OPT TE ? U
&* ISSUES A VTAM VARY ACT
&* FIRST PARM IS ID OF RESOURCE
&* SECOND PARM IS MODIFIER (DEFAULT IS U)
&IF &0 EQ ? GOTO &-HELP
&WTO V NET,ACT,ID=&0,SCOPE=&1
V NET,ACT,ID=&0,SCOPE=&1
&EXIT
&-HELP
&WTS   Correct form is ACT nodename<,ALL|COMP|ONLY|U>
&WTS   Where the SCOPE option is ALL, COMP, ONLY or U(default).
&EXIT
```

MVS/OCCF CLIST ACT is invoked by entering: %ACT ....

```
&DEF OPT TA ? U
&. ISSUES A VTAM VARY ACT
&. FIRST PARM IS ID OF RESOURCE
&. SECOND PARM IS MODIFIER (DEFAULT IS U)
&IF &1 EQ ? &GOTO -HELP
&WRITE V NET,ACT,ID=&1,SCOPE=&2
V NET,ACT,ID=&1,SCOPE=&2
&EXIT
-HELP
&WRITE Correct form is ACT nodename<,ALL|COMP|ONLY|U>
&WRITE Where the SCOPE option is ALL, COMP, ONLY or U(default).
&EXIT
```

NCCF CLIST ACT is invoked by entering: ACT ....

```
&CONTROL ERR
* VARY NET,ACT,ID=(NODE NAME),SCOPE=(COMP,ONLY,ALL,U)
&IF .&1 EQ .  &THEN &GOTO -TELL3
&IF .&1 EQ .? &THEN &GOTO -TELL2
&A = &1
&B = &2
&GOTO -TELL4
-TELL2
HELPACT
&EXIT
&GOTO -TELL
-TELL3
HELPACTO
&BEGWRITE -END1
*
*  to continue enter   GO  nodename,<scope> (to activate resource)
*                 or   CANCEL               (to cancel)
*******************************************************************
-END1
&PAUSE VARS &A &B
-TELL4
&SCOPE = &B
&IF .&SCOPE EQ . &THEN &SCOPE = U
&IF &SCOPE EQ A    &THEN &SCOPE = ALL
&IF &SCOPE EQ ALL  &THEN &GOTO -GO
&IF &SCOPE EQ C    &THEN &SCOPE = COMP
&IF &SCOPE EQ COMP &THEN &GOTO -GO
&IF &SCOPE EQ O    &THEN &SCOPE = ONLY
&IF &SCOPE EQ ONLY &THEN &GOTO -GO
&IF &SCOPE EQ U    &THEN &GOTO -GO
CLR1
&WRITE Specification error in the scope operand " &SCOPE "
HELPACT
-TELL
-END2
&EXIT
-GO
&WRITE VARY NET,ACT,ID=&A,SCOPE=&SCOPE
VARY NET,ACT,ID=&A,SCOPE=&SCOPE
```

Member: HELPACT (NCCF)

```
&CONTROL ERR
HELPACTO
&BEGWRITE -END1
*  Enter ACT without parms for prompted operation
*******************************************************************
-END1
&EXIT
```

Member: HELPACT0 (NCCF)

```
&CONTROL ERR
CLR1
&BEGWRITE -END1
**********************************************************************
* HELPACT0              ACT (VTAM CLIST)              TUTORIAL
*
*  This CLIST should be invoked to activate VTAM nodes.
*
*  Correct formats:
*
*             ACT  nodename
*             ACT  nodename,scope
*
*  nodename (required)      is the name VTAM identifies the node
*                                               to be activated
*  scope    (optional)      ALL  (A)
*                           COMP (C)
*                           ONLY (O)
*                           U(default)
-END1
&EXIT
```

MVS/OCCF CLIST: OS MOUNT command

Member: M

```
&DEF OPT TA DEFAULT DEFAULT PRIVATE
&IF &2 EQ DEFAULT &GOTO -ERR .MUST PROVIDE 2 PARMS
&IF &C GT 3  &GOTO -ERR  .MAXIMUM OF 3 PARMS
V &1,ONLINE
MOUNT &1,VOL=(SL,&2),USE=&3   .SUBMITTED THROUGH OCCF
&EXIT .WE'RE DONE NOW
-ERR .TOO MANY OR NOT ENOUGH PARMS
&WRITE MOUNT PARAMETERS ARE: UNIT SERIAL USAGE
&WRITE UNIT AND SERIAL ARE REQUIRED
&WRITE USAGE DEFAULTS TO PRIVATE, MAY BE STORAGE OR PUBLIC
```

MVS/OCCF CLIST: /STARTGTF command

Member: STARTGTF

```
&DEF OPT TN A
&. STARTGTF PROCEDURE
&. ENTER /STARTGTF TO AUTOSTART GTF
&. NO OPERATOR ACTION IS REQUIRED.
&IF &1 EQ ? &GOTO -HELP
S GTFDISK.GTF .SUBMITTED BY SOF
&EXIT
-HELP
&WRITE STARTGTF PROCEDURE
&WRITE ENTER /STARTGTF TO AUTOSTART GTF
&WRITE NO OPERATOR ACTION IS REQUIRED.
&WRITE NCCF WILL BE NOTIFIED WHEN GTF HAS STARTED.
&EXIT
```

MVS/OCCF CLIST: /STOPGTF command

Member: STOPGTF

```
&DEF OPT TN 01
&. STOPGTF PROCEDURE
&IF &1 EQ ? GOTO &-HELP
P GTF
&EXIT
-HELP
&WRITE %STOPGTF ISSUES A STOP AND NOTIFIES NCCF
&WRITE THAT A GTF SHUTDOWN HAS BEEN REQUESTED.
&EXIT
```

NCCF CLIST to reactivate selected PUs after msg IST169I

Member: IST169I

```
&CONTROL ERR
&WRITE *IST169I &1 &2 &3 &4 &5 &6 &7 &8 &9 &10 &11 &12 &13 &14 &15 &16
*
* IST169I DISCONNECTION CAUSED VARY INACT FOR PU = xxxxxxxx
*
&IF &8  NE P14022A &THEN &GOTO -END
VARY NET,ACT,ID=&8
*
-END
&EXIT
```

CLISTs for system monitoring

NCCF CLIST: MONITOR

```
&CONTROL ERR
MVS %SYSMON &1
&EXIT
```

OCCF CLIST: SYSMON

```
&DEF OPT TE 11
&. THIS PROCEDURE IS EXECUTED BY THE SAMPLE TOD EVENTS.
&IF &1 EQ ? &GOTO -HELP
&WRITE NETWORK CHECK SA&1
%STARTNJE &1              <=== see "MVS/OCCF CLIST to start NJE" on page 66.
-HELP
%QSHOW SYSMON
&EXIT
```

Member: IST077I

```
&CONTROL ERR
* IST077I  SIO=nnnnnnnn  CUA=cuu
* NOTE THAT ARITHMETIC VARIABLES REMOVE LEADING ZEROS
* NOTE YOU CANNOT SUBSTR &1
&SIO = &1
&SIO = &SUBSTR &SIO 5
&SIO = &SIO + 0
&CUA = &2
&CUA = &SUBSTR &CUA 5
&BEGWRITE SUB -END2
IST077I  Start I/O count = &SIO ;  System address = &CUA
-END2
&EXIT
```

Member: IST097I

```
&CONTROL ERR
*IST097I   DISPLAY ACCEPTED       SUPPRESSED
&EXIT
```

Member: IST241I

```
&CONTROL ERR
* IST241I  NCPSTOR COMMAND COMPLETE   SUPPRESS IT
&EXIT
```

NCCF CLIST to ACQUIRE an NCP

```
&CONTROL ERR
&IF .&1 EQ .  &THEN &GOTO -TELL
&SA = &1
&SCOPE = &2
&IF .&SCOPE  EQ .    &THEN &SCOPE = U
&IF  &SCOPE  EQ A    &THEN &SCOPE = ALL
&IF  &SCOPE  EQ ALL  &THEN &GOTO -GO
&IF  &SCOPE  EQ C    &THEN &SCOPE = COMP
&IF  &SCOPE  EQ COMP &THEN &GOTO -GO
&IF  &SCOPE  EQ O    &THEN &SCOPE = ONLY
&IF  &SCOPE  EQ ONLY &THEN &GOTO -GO
&IF  &SCOPE  EQ U    &THEN &GOTO -GO
&GOTO -TELL
-GO
&IF &SA EQ  4 &THEN &GOTO -GO1
&IF &SA EQ 14 &THEN &GOTO -GO2
&IF &SA EQ 24 &THEN &GOTO -GO3
&WRITE SPECIFICATION ERROR:
-TELL
&WRITE **************************************************************
&WRITE * GRAB ACQUIRES THE NCP'S WITH THE SUBAREA'S 4,14 OR 24      *
&WRITE *      THEN WAITS FOR AN OPERATOR "GO" TO CONTINUE           *
&WRITE *      TAKEOVER OF THE MINOR NODE RESOURCES                  *
&WRITE *      THE FIRST OPERAND IS THE SUBAREA NUMBER OF THE NCP    *
&WRITE *      THE SECOND OPERAND IS A|ALL|C|COMP|O|ONLY|U DEFAULT   *
&WRITE *      THE NCPNAMES ARE N043F35,N14BF35,N245F35              *
&WRITE **************************************************************
-GO1
&WRITE VARY NET,ACQ,ID=N043F35,SCOPE=&SCOPE,ACT
VARY NET,ACQ,ID=N043F35,SCOPE=&SCOPE,ACT
&WRITE ******************************************
&WRITE *  REPLY "GO" IF TAKE OVER COMPLETED      *
&WRITE ******************************************
PAUSE
&WRITE ******************************************
&WRITE *  REPLY "GO" ACCEPTED                    *
&WRITE ******************************************
VARY NET,ACQ,ID=P040A0A,ACT,SCOPE=&SCOPE
          etc.
&EXIT
-GO2
&WRITE VARY NET,ACQ,ID=N14BF35,SCOPE=&SCOPE,ACT
VARY NET,ACQ,ID=N14BF35,SCOPE=&SCOPE,ACT
&WRITE ******************************************
&WRITE *  REPLY "GO" IF TAKE OVER COMPLETED      *
&WRITE ******************************************
PAUSE
&WRITE ******************************************
&WRITE *  REPLY "GO" ACCEPTED                    *
&WRITE ******************************************
VARY NET,ACQ,ID=P140A0A,ACT,SCOPE=&SCOPE
          etc.
&EXIT
-GO3
&WRITE VARY NET,ACQ,ID=N245F35,SCOPE=&SCOPE,ACT
VARY NET,ACQ,ID=N245F35,SCOPE=&SCOPE,ACT
&WRITE ******************************************
&WRITE *  REPLY "GO" IF TAKE OVER COMPLETED      *
&WRITE ******************************************
PAUSE
&WRITE ******************************************
&WRITE *  REPLY "GO" ACCEPTED                    *
&WRITE ******************************************
VARY NET,ACQ,ID=P240A0A,ACT,SCOPE=&SCOPE
          etc.
&EXIT
```

PARMLIB member COMMNDxx

```
COM='SEND '**********************************',BRDCST'
COM='SEND '**********************************',BRDCST'
COM='SEND '**                              **',BRDCST'
COM='SEND '**      MVS OPERATING SYSTEM    **',BRDCST'
COM='SEND '**      SERVICE LEVEL IS 8206   **',BRDCST'
COM='SEND '**                              **',BRDCST'
COM='SEND '**********************************',BRDCST'
COM='SEND '**********************************',BRDCST'
COM='CD SET,SDUMP=(ALLPSA,NUC,SQA,LSQA,RGN,LPA,TRT,SWA,CSA,SUM),Q=YES'
TOD=NOPROMPT
COM='S NET,,,(LIST=01),SA=01'
COM='S OCCFN,SA=01'
```

JCL procedure to start MVS/OCCF, NPDA, and NCCF

Member: OCCFN

```
//OCCFN    PROC NAME=CBFDISP,Q1=NCCFR2,Q2=NPDAV2,           <=== MVS/OCCF
//*CCFN    PROC NAME=BNJLINTX,Q1=NCCFR2,Q2=NPDAV2,              <=== NPDA
//*CCFN    PROC NAME=DSIMNT,Q1=NCCFR2,Q2=NPDAV2,                <=== NCCF
//              RGN=4000K,SA=11,
//              BFSZ=8K,SLSZ=200,OUT=L
//ST1      EXEC PGM=&NAME,TIME=1440,REGION=&RGN,PARM=(&BFSZ,&SLSZ),
//              DPRTY=(15,10),PERFORM=13
//STEPLIB   DD DSN=&Q2..NPDALIB,DISP=SHR
//SYSUDUMP  DD DUMMY
//SYSPRINT  DD SYSOUT=&OUT
//BNJLGPRI  DD DSN=BNJLGPRI,DISP=OLD                   <=== NPDA data base
//BNJLGSEC  DD DSN=BNJLGSEC,DISP=OLD                   <=== NPDA data base
//OCCFPDS   DD DSN=SYS1.PROCLIB,DISP=SHR                         <=== OCCF
//          DD DSN=SYS2.OCCFPDS,DISP=SHR
//          DD DSN=SYS2.PROCLIB,DISP=SHR
//LINENETO  DD UNIT=068                             <=== OCCF ROCF support
//DUMPNETO  DD SYSOUT=I                             <=== OCCF ROCF support
//VSAM      DD DSN=OZ.VSAM,DISP=SHR             <=== INFO/System data base
//DSICLD    DD DSN=&Q1..CLISTLIB,DISP=SHR          <=== NCCF CLISTs
//DSIPARM   DD DSN=SA&SA..DSIPARM,DISP=SHR
//DSIVTAM   DD DSN=SYS1.VTAMLST,DISP=SHR
//DSIPRF    DD DSN=SA&SA..DSIPRF,DISP=SHR
//DSIIRDR   DD SYSOUT=(A,INTRDR)
//DSILOGP   DD DSN=NCCFLOG.SA11P,DISP=SHR,AMP=AMORG
//DSILOGS   DD DSN=NCCFLOG.SA11S,DISP=SHR,AMP=AMORG
```

MVS/OCCF start-up parameters

```
Member:  OCCFPARM

DESIG=%                                                                 00010072
ATTACH=NCCF                                                             00020072
MSGBUF=500                                                              00030068
CPROC=4                                                                 00040057
CMDAUTH=PM                                                              00060056
MATAB=11          <=== suffix for the name of the message action table
```

OCCFPARM is a member of the OCCF partitioned data set which is defined by the DD statement named OCCFPDS in the JCL procedure used to start OCCF.

MVS/OCCF Message Action Table

```
Member:  MATAB01

I* ROUTE                                                                00010000
$H* ROUTE                                                               00020000
IEF005Q REPLY=U                                                         00030000
RC=(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16)                             00040000
IEC1234I REPLY=U                                                        00050000
IEF1234I REPLY=YES                                                      00060000
IEF1234 REPLY=NO                                                        00070000
IGF500D REPLY=NO                                                        00080000
IKT003D REPLY=RETRY                                                     00081000
IKT012D REPLY=U                                                         00082000
DSI800A REPLY=RETRY                                                     00090000
```

The OCCF Message Action Table is is a member of the OCCF partitioned data set.

NCCF initial CLISTs

```
&CONTROL ERR
*
* NCCF initial CLIST for subarea 01
*
&WRITE *-------------------------------------------------------*
&WRITE |                                                       |
&WRITE |                                                       |
&WRITE |  OCCF initial CLIST %AUTO 01 started via MVS command  |
&WRITE |              NPDA filters are set                     |
&WRITE |  OCCF CLIST %SYSMON will be invoked every hour and    |
&WRITE |  can be cancelled by: PURGE TIMER=SYSMON,OP=PPT       |
&WRITE |                                                       |
&WRITE |                                                       |
&WRITE *-------------------------------------------------------*
F NET,NOTNSTAT
F NET,IOPD,IOINT=25
MVS %AUTO 01
EVERY 1,PPT,ID=NPDAIN,NPDAINT
EVERY 30,PPT,ID=SYSMON,MONITOR
&EXIT
```

Member: NPDAINT

```
&CONTROL ERR
NPDASRF
PURGE TIMER=NPDAIN,OP=PPT
&EXIT
```

Member: NPDASRF

```
&CONTROL ERR
&WRITE NPDA FILTERS INITIALIZED.
NPDA SRF AREC PASS T CUST
NPDA SRF AREC PASS T IMR
NPDA SRF AREC PASS T PERF
NPDA SRF AREC PASS T PERM
NPDA SRF AREC PASS T PROC
NPDA SRF AREC PASS T TEMP
NPDA SRF AREC PASS T SNA
NPDA SRF AREC PASS T USER
NPDA SRF AREC PASS TREF CPU
&EXIT
```

Initialization of NPDA filters is deferred for one minute because NPDA is not up by the time the 'NCCF initial CLIST' is executed.

MVS/OCCF CLIST to facilitate system activation

Member: AUTO

```
&DEF OPT TE 11
&IF &1 NE ? &GOTO -GO
&WRITE SYSTEM START-UP PROCEDURE
-HELP
&WRITE FORMAT: %AUTO NN WHERE NN IS SUBAREA, DEFAULT = 11.
&EXIT
-GO
&IF &1 EQ 11 &GOTO -CEN11
&IF &1 EQ 01 &GOTO -SUB01
&IF &1 EQ 21 &GOTO -SUB21
&WRITE WRONG SUBAREA SPECIFIED
&GOTO -HELP
-CEN11
&WRITE S TSO
S TSO
&WRITE S NPA
S NPA
&WRITE S HCF
S HCF
%ACT N1401
%ACT N0421
%ACT N2403
%ACT LOC113
%ACT LOC117
&GOTO -FINAL
-SUB01
&WRITE S CICS
S CICS
&WRITE S TSO
S TSO
&WAIT 99
V 370-37F,ONLINE
%ACT N0421
%ACT LOC012
```

```
&GOTO -FINAL
-SUB21
&WRITE S APPL24
S APPL24
&WRITE S TSO
S TSO
%ACT N2403
-FINAL
&WRITE V NET,ACT,ID=M&1
V NET,ACT,ID=M&1
%STARTNJE &1
&WRITE ************************************************************
&WRITE * MVSOCCF: AUTOMATIC SYSTEM INITIALIZATION IS NOW COMPLETE *
&WRITE * FOR THE FOLLOWING DATE AND TIME                          *
D T
D T
D T
&WRITE ************************************************************
&EXIT
```

MVS/OCCF CLIST to start NJE

Member: STARTNJE

```
&DEF OPT TN 01
&IF &1 NE ? &GOTO -GO
&WRITE STARTNJE PROCEDURE
&WRITE FORMAT %STARTNJE NODE : WHERE NODE EQUALS LOCAL SA NUMBER
&WRITE USE TO CONNECT MVS TO MVS (NJE) VIA MSNF
&EXIT
-GO
$SLGN1
$SLNE1
$SLNE2
$SLNE3
  etc.
&IF &1 EQ 11 &GOTO -SA11
&IF &1 EQ 01 &GOTO -SA01
&IF &1 EQ 21 &GOTO -SA21
&EXIT
-SA11
$SLNE8
$SLNE9
&WRITE $SN,A=RDPD1MVS
$SN,A=RDPD1MVS
&WRITE $SN,A=REMJES01
$SN,A=REMJES01
&WRITE NJE SHOULD BE UP
&EXIT
-SA01
&WRITE $SN,A=RDPD3MVS
$SN,A=RDPD3MVS
&WRITE NJE SHOULD BE UP
&EXIT
-SA21
&WRITE $SN,A=RDPD3MVS
$SN,A=RDPD3MVS
&WRITE NJE SHOULD BE UP
&EXIT
```

NCCF CLIST to establish NCCF-NCCF and NCCF-OCCF sessions

```
&CONTROL ERR
&IF .&1 EQ .? &THEN &GOTO -TELL
&GOTO -GO
-TELL
&BEGWRITE -END
*------------------------------------------------*
| Enter CENTRAL to start NCCF and OCCF sessions for |
|       CENTRAL OPERATION.                          |
| Enter GO when message DSI809A appears.            |
| Enter GO SKIP if error message appears.           |
*------------------------------------------------*
-END
&EXIT
-GO
&WRITE OCCF %QLOGON
OCCF %QLOGON
&WRITE START DOMAIN=NCF01
START DOMAIN=NCF01
&WRITE Enter GO when message DSI809A appears.
&WRITE Enter GO SKIP if error message appears.
&PAUSE VARS &A
&IF .&A EQ .SKIP &THEN &GOTO -NCF21
&WRITE NCF01 NETOP,NETOP
NCF01 NETOP,NETOP
&WRITE Enter GO when NCCF session started.
&WRITE Enter GO SKIP if error message appears.
&PAUSE VARS &A
&IF .&A EQ .SKIP &THEN &GOTO -NCF21
&WRITE OCF01 %QLOGON
OCF01 %QLOGON
-NCF21
&WRITE START DOMAIN=NCF21
START DOMAIN=NCF21
&WRITE Enter GO when message DSI809A appears.
&WRITE Enter GO SKIP if error message appears.
&PAUSE VARS &A
&IF .&A EQ .SKIP &THEN &GOTO -NCF31
&WRITE NCF21 NETOP,NETOP
NCF21 NETOP,NETOP
&WRITE Enter GO when NCCF session started.
&WRITE Enter GO SKIP if error message appears.
&PAUSE VARS &A
&IF .&A EQ .SKIP &THEN &GOTO -NCF31
&WRITE OCF21 %QLOGON
OCF21 %QLOGON
-NCF31
  etc.
&WRITE AUTO NCCF and OCCF LOGON complete.
&EXIT
```

Member: NCF01

```
&CONTROL ERR
ROUTE NCF01 &PARMSTR
```

Member: OCF01

```
&CONTROL ERR
ROUTE NCF01,OCCF &PARMSTR
```

The NCCF 'MVS' command processor is one method by which an operator or the NCCF PPT can issue any commands from NCCF stations to system internal reader. The reason why 'MVS' command processor uses internal reader instead of SVC 34, is because authorization of NCCF is required to use SVC 34. A sample of 'MVS' is included. It is designed that it will pass the command to a program called SVC34 which in turn is authorized to issue almost all MVS, JES2, OCCF, and SOF commands. The source and JCL for SVC34 follows the source for the 'MVS' command processor.

To implement this 'MVS' command processor, the following steps are required:

(1) Assemble and link edit MVSCMD source code into the NCCF program library(default: SYS1.LINKLIB).
(2) Define a CMDMDL statement for the 'MVS' command processor in the DSICMD member of the NCCF defintion:
===> MVS CMDMDL MOD=MVSCMD,TYPE=R,CTL=N
(3) Restart NCCF
(4) Assemble and link edit 'SVC34' sample program.

NCCF 'MVS' Command Processor (SVC34 interface)

```
* NCCF 'MVS' COMMAND PROCESSOR (SVC34 INTERFACE).
* THE DATA DEFINED AT THE LABEL JOBCARD SHOULD BE CHANGED TO
* REFLECT THE SYSTEM REQUIRED JOBCARD.
* AN INTERNAL READER STATEMENT IS REQUIRED IN THE NCCF PROCEDURE
* TO SUPPORT THIS COMMAND.
MVSCMD   CSECT
R0       EQU   0
R1       EQU   1
R2       EQU   2
R3       EQU   3
R4       EQU   4
R5       EQU   5
R6       EQU   6
R7       EQU   7
R8       EQU   8
R9       EQU   9
R10      EQU   10
R11      EQU   11
R12      EQU   12
R13      EQU   13
R14      EQU   14
R15      EQU   15
         PRINT NOGEN
         DSICBS DSICBH,                                                X
               DSICWB,                                                 X
               DSISWB,                                                XX
               DSIMVT,                                                 X
               DSITIB,                                                 X
               DSITVB,                                                 X
               DSIPDB,                                                 X
               DSISCE,                                                 X
               PRINT=NO
         PRINT GEN
MVSCMD   CSECT
         SAVE  (14,12)
         LR    R12,R15
         USING MVSCMD,R12
         USING DSICWB,R1
         LA    R10,CWBSAVEA
         ST    R10,8(R13)
         ST    R13,4(R10)
         LR    R13,R10
         USING CWBSAVEA,R13
```

```
         DROP  R1
         L     R11,CWBTIB
         USING DSITIB,R11
         L     R8,TIBTVB
         USING DSITVB,R8
         L     R10,TVBMVT
         USING DSIMVT,R10
         L     R9,CWBPDB
         USING DSIPDB,R9
         DROP  R8
*
         MVI   WORKAREA,X'00'
         MVC   WORKAREA+1(255),WORKAREA
         MVI   CMDAREA,X'40'
         MVC   CMDAREA+1(79),CMDAREA
         L     R4,CWBBUF
         LH    R5,0(R4)           GET MESSAGE LENGTH
         SH    R5,CMDLNGTH        TEST FOR INPUT LENGTH
*        BM    LONGCMD            INPUT TOO LONG
         CLI   PDBNOENT+1,X'01'
         BE    NOOSCMD            NEEDS OS COMMAND AS PARM
         OPEN  (INTRDR,(OUTPUT))
         L     R6,CWBBUF
         AH    R6,22(R9)          POINTS OPERAND PORTION
         LH    R5,0(R4)
         SH    R5,22(R9)
         AH    R5,18(R9)          LENGTH OF OPERAND
         ST    R5,SETUP
         MVI   SETUP,X'40'
         L     R7,SETUP
* TESTS TO LIMIT SCOPE COULD BE DONE AT THIS POINT
*        CLI   0(R6),C'$'
*        BE    JES2CMD
*        CLI   0(R6),C'/'
*        BE    SOFCMD
*        CLI   0(R6),C'%'
*        BE    OCCFCMD
OCCFCMD  EQU   *
SOFCMD   LA    R9,78
         LA    R8,CMDAREA
         MVCL  R8,R6
         PUT   INTRDR,JOBCARD
         PUT   INTRDR,EXECSOF
* THE NEXT STATEMENT IS REQUIRED IF THE PROGRAM SVC34 IS NOT IN A
* LIBRARY IN LINK LIST. THE STEPLIB MUST BE AUTHORIZED.
         PUT   INTRDR,STEPLIB
         PUT   INTRDR,UT1CARD
         PUT   INTRDR,OSCMD
         PUT   INTRDR,ENDCARD
         CLOSE (INTRDR)
         LA    R1,MSG001
         MVI   RETCODE,X'00'
         B     PUTMSG
*
LONGCMD  EQU   *
         LA    R1,MSG001
         MVI   RETCODE,X'08'
         B     PUTMSG
NOOSCMD  EQU   *
         LA    R1,MSG002
         MVI   RETCODE,X'08'
         B     PUTMSG
PUTMSG   EQU   *
         MVC   MSGAREA(50),0(R1)
         LA    R2,BUFFER
         USING BUFHDR,R2
         LA    R1,50
         STH   R1,HDRMLENG
         BAL   R14,PUTBUFF
RETURN   EQU   *
         SLR   R15,R15
         IC    R15,RETCODE
         L     R13,4(R13)
         LM    R0,R12,20(R13)
         L     R14,12(R13)
```

```
         BR    R14
*
PUTBUFF  EQU   *
         ST    R14,SAVE14A
         CLI   HDRTDISP+1,X'00'
         BNE   HALFDONE
         LA    R0,BUFHDRND-BUFHDR
         STH   R0,HDRTDISP
         MVC   HDRDOMID(8),MVTCURAN
         MVI   HDRMTYPE,C'U'
         LA    R0,120
         STH   R0,HDRBLENG
HALFDONE EQU   *
         BAL   R14,GETTIME
         ST    R1,HDRTSTMP
         L     R1,CWBSWB
         DSIPSS SWB=(R1),TYPE=OUTPUT,BFR=(R2)
         L     R14,SAVE14A
         BR    R14
*
GETTIME  EQU   *
         ST    R14,SAVE14B
         DSIDATIM AREA=PACKAREA,FORMAT=BINARY
         L     R1,PACKAREA+4
         L     R14,SAVE14B
         BR    R14
CMDLNGTH DC    X'0021'
MSG001   DC    CL50'MVSCMD COMMAND ISSUED VIA INTRDR'
MSG002   DC    CL50'MVSCMD INPUT IS REQUIRED'
JOBCARD  DC    CL80'//DSIDUMMY JOB MSGCLASS=S,CLASS=I                 '
EXECSOF  DC    CL80'// EXEC PGM=SVC34                                 '
STEPLIB  DC    CL80'//STEPLIB DD DSN=CNM.DEMO.LINKLIB,DISP=SHR'
UT1CARD  DC    CL80'//SYSUT1 DD DATA                                  '
ENDCARD  DC    CL80'/*                                                '
PREFIX   DC    CL3'// '
PREJES2  DC    CL2'/*'
INTRDR   DCB   DSORG=PS,MACRF=(PM),LRECL=80,BLKSIZE=80,RECFM=F,        C
               DDNAME=DSIIRDR
*
DSICWB   DSECT
         ORG   CWBADATD
WORKAREA DS    0CL256
COMMAND  DS    0CL32
CMDLNG   DS    H
CMDFLG   DS    H
OSCMD    DS    0CL80
CMDAREA  DS    CL80
         DS    CL8
         DS    CL8
PACKAREA DS    D
SAVE14A  DS    F
SAVE14B  DS    F
SETUP    DS    F
RETCODE  DS    C
         DS    CL3
BUFFER   DS    0F
         DS    XL(BUFHDRND-BUFHDR)
MSGAREA  DS    0CL96
LABEL1   EQU   *
         DS    XL(256-(LABEL1-WORKAREA))
*
         END
```

<u>**'SVC34' Sample Program Source**</u>

This load module must be placed in an authorized library.

```
//ASM     EXEC ASMFCL
//SYSIN    DD  *
SVC34    TITLE 'SVC 34 - COMMAND ISSUE ROUTINE                         M*M'
```

```
*        PRINT NOGEN
* this program must be placed in an authorized library.
SVC34    CSECT
         STM   R14,R12,12(R13)     SAVE REGISTERS
         LR    R11,R15             LOAD ENTRY ADDRESS TO BASE REGISTER
         USING SVC34,R11           ESTABLISH ADDRESSA BILITY
         B     AROUNDID            AROUND MODULE ID
         DC    CL8'SVC34           MODULE ID
AROUNDID DS    0H
         ST    R13,SAVE+4          *
         LR    R10,R13              LINKAGE
         LA    R13,SAVE              CONVENTION
         ST    R13,8(R10)             *
*
         MODESET KEY=ZERO,MODE=SUP
*
         OPEN  (SYSUT1,(INPUT))
READ     GET   SYSUT1,INAREA       READ COMMAND
         MVC   $CMD,INAREA         MOVE COMMAND TO BUFFER
         SR    R0,R0               CLEAR FOR SVC 34
         LA    R1,COMMAND          POINT COMMAND AREA
         SVC   34                  ISSUE COMMAND
         B     READ                READ NEXT COMMAND FROM SYSUT1
EOF      DS    0H                  END OF FILE ENTRY
         CLOSE (SYSUT1)            CLOSE FILES
         L     R13,SAVE+4
         LM    R14,R12,12(R13)     RESTORE REGISTERS
         XR    R15,R15             SET RETURN CODE = 0
         BR    R14                 EXIT
*
R0       EQU   0
R1       EQU   1
R2       EQU   2
R3       EQU   3
R4       EQU   4
R5       EQU   5
R6       EQU   6
R7       EQU   7
R8       EQU   8
R9       EQU   9
R10      EQU   10
R11      EQU   11
R12      EQU   12
R13      EQU   13
R14      EQU   14
R15      EQU   15
*
         DS    0D
SAVE     DS    18F                 SAVE AREA
INAREA   DC    CL80' '             COMMAND INPUT AREA
COMMAND  DC    AL2(32,0)           LENGTH & FLAGS
$CMD     DC    CL28' '
*
         TITLE 'D C B --- SYSUT1, SYSUT2'
SYSUT1   DCB   DDNAME=SYSUT1,DSORG=PS,MACRF=GM,EODAD=EOF,              *
               RECFM=F,BLKSIZE=80,LRECL=80
*
         END
/*
//LKED.SYSLMOD DD DSN=SYS2.LINKLIB,DISP=SHR
//LKED.SYSIN DD *
  ENTRY SVC34
  SETCODE AC(1)
  NAME SVC34(R)
/*
```

Sample procedure to test the program SVC34

```
//DSIDUMMY JOB MSGCLASS=S,CLASS=I
// EXEC PGM=SVC34
//SYSPRINT DD SYSOUT=S
//SYSUT1 DD DATA
%AUTO 11
/*
```

NETWORK MANAGEMENT

GG24-1539-0
Communication Network Management/
Managing Interconnected Systems

The aim of this paper was to examine central site management of distributed processing systems. Situations were examined that included either a OS/MVS system or a DOS/VSE system as central host. The requirements for controlling these situations from a central site fell broadly into three areas. These were:
Network Operation,
Program Maintenance and Batch Data Transfer, and
Problem Determination.

GG24-1540-0
Communication Network Management/
NCCF Terminal Access Feature

This document contains an overview of the Terminal Access Facility of NCCF. The document was produced as a by-product of an early testing of the product and provides useful scenarios on how the product can be used.

GG24-1546-0
Communication Network Management/
Using Information/Management

The intent of this paper is to ease the initial use of some functions of Information/Management (INFO/MGMT) and its interface to NPDA.
It presents examples on defining a network containing multiple systems.

GG24-1554-0
Communication Network Management/
Customizing NCCF

This document is intended to supplement the NCCF Customization Manual (SC27-0433) with further hints, comments and examples on writing CLISTs, Command Processors and User Exits for NCCF.
It should be read in conjunction with the NCCF Customization Manual.

INSTALLATION SUPPORT

GG24-1547-0
Advanced Communications
Function Primer

This document provides overviews on some of the SNA products and expands on the examples in the ACF Product Installation Guide (GG24-1557).

GG24-1557-0
Advanced Communications Function
Products Installation Guide

The purpose of this guide is to provide
information that may help in installing SNA products
on either a DOS/VSE or OS/VS operating system using MVS.
This guide supports ACF/VTAM V1R3 and V2R1.
It supports ACF/NCP V1R3.
The samples in this guide will support the following products:
IMS/VS, CICS/VS, TSO, JES2(MVS),
ACF/VTAM,
ACF/NCP/VS, NCCF, NPDA, VSE, POWER, FTP, JEP, and VSE/OCCF.

GG24-1509-0
SNA Product Installation Guide/
ACF/VTAM Release 2

The purpose of this guide is to provide
information that may help in installing SNA products
on either a DOS/VSE or OS/VS operating system using MVS.
This guide supports ACF/VTAM V1R2 and ACF/NCP V1R2 and V1R3.
The samples in this guide will support the following products:
IMS/VS, CICS/VS, TSO, JES2(MVS),
ACF/VTAM,
ACF/NCP/VS, NCCF, and NPDA.

GG24-1519-0
Small Communications Systems
Installation Primer
IBM 4331/ACF/VTAME

This publication contains basic information needed to assist the user in adding the telecommunications capability to an IBM 4331 DOS/VSE System. It is specifically directed to the installation of IBM 3270, ACF/VTAME, and CICS/VS systems.

GG24-1552-0
Small Communications Systems
Installation Primer
VSE System IPO/E & IBM 3705-80

The purpose of this guide is to assist the user in the installation of a telecommunications system based on
- IBM Systems Network Architecture (SNA)
- An IBM 4300 Processor
- VSE System IPO/Extended
- CICS/VS
- An IBM 3705-80 Communication Controller
- IBM 3270 Information Display System

PROBLEM DETERMINATION

GG24-1514-0
SNA Problem Determination Guide/
ACF R3 Volume 1

This paper is part of a two volume series dealing with system problem determination in a ACF/VTAM environment. It discusses and illustrates problem determination techniques and tools.

GG24-1523-0
Availability: May 1982
SNA Problem Determination Guide/
ACF R3 Volume 2

ABEND	Abnormal End of a program
ACB	Access Control Block (VTAM)
ACF/NCP	Advanced Communications Function for Network Control Program
ACF/TCAM	Advanced Communications Function for the Telecommunications Access Method
ACF/VTAM	Advanced Communications Function for the Virtual Telecommunications Access Method
applid	Application identification (VTAM definitions)
BSC	Binary Synchronous Communication
BTAM	Basic Telecommunications Access Method
CDRM	Cross-Domain Resource Manager
CDRSC	Cross-Domain Resource
CICS/VS	Customer Information Control System / Virtual Storage
CLIST	Command List
CLPA	Clear Link Pack Area (MVS)
CMC	Communication Management Configuration
CNM	Communication Network Management
CPU	Central Processing Unit
CTC	Channel to Channel Adapter
DASD	Direct Access Storage Device
DD	Data Definition (MVS JCL)
DOS/VSE	Disk Operating System / Virtual Storage Extended
DPCX	IBM 8100 Distributed Processing Control Executive
DPPX	IBM 8100 Distributed Processing Programming Executive
EP	IBM 3705 Emulation Program
FDP	Field Developed Program
GTF	Generalized Trace Facility
HCF	IBM 8100 Host Command Facility
ID	Identification
IML	Initial Micro-program Load
IMS/VS	Information Management System / Virtual Storage
INFO	Information System
IPL	Initial Program Load
JCL	Job Control Language
JES	Job Entry Subsystem (JES2 or JES3)
LU	Logical Unit (SNA)
MSS	Mass Storage System
MVS	Multiple Virtual Storage (OS/VS2)
MVS/OCCF	MVS Operator Communications Control Facility
NCCF	Network Communications Control Facility
NCP	ACF/NCP
NPA	Network Performance Analyzer
NPDA	Network Problem Determination Application
OCCF	MVS/OCCF
OS	Operating System
PA key	Program Action key (3270)
PARMLIB	Parameter library (MVS)
PDS	Partitioned Data Set
PF key	Program Function key (3270)
PU	Physical Unit (SNA)
RACF	Resource Access Control Facility
RMFMON	Resource Measurement Facility Monitor
ROCF	Remote Operator Control Facility
RPL	IBM 3705 Remote Program Loader
SDLC	Synchronous Data Link Control
SNA	System Network Architecture
SOF	Secondary Operator Facility
SSCP	System Services Control Point
SVC	Supervisor Call (OS)
TAF	Terminal Access Facility
TCAM	ACF/TCAM
TCT	Terminal Control Table (CICS)
TG	Transmission Group
TSO	Time Sharing Option
VTAM	ACF/VTAM
WTO	Write To Operator (MVS console support)
WTOR	Write To Operator and request Reply (MVS console support)

Note: Staples can cause problems with automated mail sorting equipment.
Please use pressure sensitive or other gummed tape to seal this form.

GG24-1558-0

COMMUNICATION NETWORK MANAGEMENT
CENTRAL SITE OPERATION

READER'S COMMENT FORM

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, is deemed appropriate. Comments may be written in your own language; use of English is not required.

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: ________________

Reader's Comment Form

Cut or Fold Along Line

Fold

IBM Europe / Middle East / Africa Corporation
World Trade Systems Center
Department 985 / H594
Building 622-3
P.O. Box 12195
Research Triangle Park
Raleigh, North Carolina 27709
U.S.A.

Fold

IBM

GG24-1558-0

COMMUNICATION NETWORK MANAGEMENT - CENTRAL SITE OPERATION GG24-1558-0

IBM®