

GENERAL INFORMATION MANUAL

Document Number TND-0201-10

The Network Director

North Ridge Software, Inc.

Special Notices

This document contains proprietary information associated with a generalized software product named **The Network Director**, which is a VTAM based terminal security and productivity product developed, maintained, and marketed by North Ridge Software, Inc.

Information contained herein that is associated with other proprietary products (as identified below) is also subject to copyright law and may not be reproduced without the express written permission of the appropriate company.

All rights are reserved. No portion of this document may be reproduced, copied, distributed, transmitted, transcribed, or translated into any human or computer language, or otherwise disclosed to third parties without the express written permission of:

North Ridge Software, Inc.
12515 Willows Road N.E.
Suite 205
Kirkland, Washington 98034-8795
U.S.A.

(c) Copyright 1997

North Ridge Software, Inc. can be contacted via any of the following mechanisms:

Telephone 425/814-9000
FAX 425/823-9636
InterNet support@nrsinc.com
Homepage http://www.nrsinc.com

North Ridge Software, Inc. makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of fitness for any particular purpose.

Acknowledgements

References within this manual to the following products should be recognized as references to proprietary products and trademarks of the following firms:

Computer Associates	TOP SECRET, ACF2, UCC7, ROSCOE, EMAIL, IDMS/DC, TPX
IBM	ACF/VTAM, ACF/TCAM, NMPF, NPDA, VM/GCS, OS/VS1, NETVIEW, NLDM, NPA, CMS, MVS, DOS/VSE, CICS/VS, TSO, IMS, RACF, NPDA, and NCCF
Software AG	Com-plete
Sterling Software	VM/SECURE

Table of Contents

Introduction	1
The Manual Set	2
Manual Overview	3
Background	5
Software Subsystems	6
Terminal Access Methods	7
Access Method Evolution	8
Access Method Shortcomings	11
The Network Director	13
Shortcoming Resolutions	13
Execution Environment	15
Concepts and Facilities	17
Terms and Phrases	17
Configuration Parameters	19
The Application Selection Panel	20
Non CUA Operations	20
Configuration Parameters	21
Panel Body	22
Selecting an Application	22
Application Status	23
Logging onto the System	24
The Profile	26
CUA Operations	27
Configuration Parameters	28
Panel Body	29
Selecting an Application	29
Application Status	29
Logging onto the System	31
Options	33
The Message Facility	34
Memo	34
Note	34
Broadcast	34
Network Information File	37
Single System Image	38
The Network Administrator	39
The LOG File	42
Controlling the Logical Network	42
Issuing ACF/VTAM or VM Commands	43

Network Reporting	43
Network System Interface	44
Network Security Facilities	45
User Identification	45
Audit Facilities	45
Intruder Detection	45
System Security Packages	46
ACF2/MVS	46
ACF2/VM	47
RACF/MVS	47
RACF/VM	48
TopSecret/MVS	48
TopSecret/VM	48
VM/SECURE	49
Event Recording	50
Configuration Parameters	51
Summarization	52
Implementations	53
Logical Application Independence	54
Multiple Network Directors	55
ACF/VTAM Multiple DOMAIN Configurations	56
Summarization	57
Sample Configuration Parameters	59
Overview	59
APPLICATION	61
DEFAULT	61
GROUP	61
TERMINAL	61
USER	62
Summarization	62
Technical Characteristics	63
Storage Estimates	65
Working Set Characteristics	66
Glossary	67
Index	71

List of Illustrations

Figure 1.	The Manual Set	2
Figure 2.	Common subsystems	6
Figure 3.	Terminal Access Methods	7
Figure 4.	ACF/VTAM Terminal Connection	9
Figure 5.	The Network Director Environment	16
Figure 6.	Basic Terms and Phrases	18
Figure 7.	Basic Application Selection Panel	20
Figure 8.	Simple Configuration Parameters	21
Figure 9.	Basic Application Selection Panel with Status	23
Figure 10.	User Id Identification Panel	24
Figure 11.	Basic CUA Application Selection Panel	27
Figure 12.	Simple Configuration Parameters	28
Figure 13.	Basic CUA Application Selection Panel with Message	30
Figure 14.	CUA User Id Identification Panel	31
Figure 15.	Primary Messages Menu	35
Figure 16.	Network Administrator Application Selection Panel	40
Figure 17.	Network Administrator Display	41
Figure 18.	Issuing Network Administrator Commands	43
Figure 19.	Available Events	50
Figure 20.	Available Commands	51
Figure 21.	Logical Application Location	54
Figure 22.	Multiple DOMAIN Implementation	56
Figure 23.	Sample Configuration Parameters	60
Figure 24.	Sample PAYROLL Group Panel	62
Figure 25.	Storage Estimates	65

Introduction

This manual is the collection point for general and overview information related to the software product named **The Network Director**. The intent of the manual is to provide a relatively concise description of basic concepts, facilities, and application of the The Network Director as it functions within the IBM System 370 architectural environment.

This manual is organized such that a single reading from front to back will present a consistent narrative. It should provide sufficient information for basic understanding of what The Network Director is for, how it functions, how it may be applied, and why it can aid in the management of the terminal network.

This general information manual has been prepared expressly for the individual that may not be fully aware of all the developments that are occurring or have occurred within the data processing environment. The intent is for a high level discussion of the items within the computing environment that make the use of The Network Director beneficial to the data processing community as a whole. Those readers interested in more detail about The Network Director are referenced to other manuals associated with the product for more information.

Wherever possible, this manual has avoided the specific use of technical terms and acronyms. This has been done to improve the readability of the manual in general. Generic terms have been used when they would suffice (*terminal* instead of *logical unit*). It is hoped that this generalization has not sacrificed the content of this manual for the more technically oriented reader.

The Manual Set

This manual is one of a set related to The Network Director. The set consists of:

Number	Manual Title
TND-0201	General Information Manual
TND-0202	Network User's Guide
TND-0203	Network Administrator's Guide
TND-0204	Quick Reference Guide
TND-0205	Internals
TND-0206	Messages and Codes
TND-0210	Network Operator's Guide
TND-0219	Installation Guide
TND-0220	Single System Image
TND-0226	SecureNet Key Interface Reference
TND-0420	Version 4.2 Release Guide

Figure 1. The Manual Set

Each Network Director installation is provided with a complete set of base documentation for The Network Director. The base set consists of the *General Information Manual*, *Network User's Guide*, *Network Administrator's Guide*, *Quick Reference Guide*, *Internals*, *Messages and Codes*, the *Network Operator's Guide*, *Single System Image*, and the *Installation Guide*. Additional documentation is available, as requested.

Manual Overview

"Background" on page 5 provides the reader with a brief discussion of the data processing events that led to the implementation of The Network Director.

"Access Method Shortcomings" on page 11 discusses those characteristics of commonly used terminal access methods that are considered shortcomings by The Network Director's concepts.

"The Network Director" on page 13 provides a quick overview of how The Network Director resolves the shortcomings identified in "Access Method Shortcomings" on page 11.

"Concepts and Facilities" on page 17 describes the general capabilities of The Network Director and how its characteristics can be utilized to extend the usability of the computing facility.

"Implementations" on page 53 presents a short discussion of how The Network Director could be configured within a computing facility to best meet the needs of the network users.

"Sample Configuration Parameters" on page 59 provides example Network Director Parameters and discusses how they control The Network Director's activities.

"Technical Characteristics" on page 63 contains a description of the technical characteristics that are present in The Network Director.

Terms and acronyms commonly used within this manual are briefly identified and defined in the Glossary of Terms and cross referenced in the Index. These sections should aid in the translation of unrecognized references to various software and hardware components and in the use of this manual.

Background

Since the middle 1970's, the data processing community has experienced an unprecedented expansion of its requirements to provide generalized computing facilities to the professional community. This expansion has occurred based upon the rapidly declining cost of individual components that make up a standard computer configuration. Most commonly, the central processing unit (CPU) and its ability to execute instructions economically has led the way towards the extension of the automated system into all facets of business.

As the cost of running application systems became less expensive, the systems themselves became the driving force for improvements in the facilities provided by the computing facility. The early use of "cards" gave way to a sequential tape medium. Eventually, the tape medium was replaced by the direct access medium, which resulted in information being readily available for random inquiry.

But, the hardware was not the only evolution taking place. Software systems capable of managing large amounts of *batch* work were developed. The software systems were also extended to provide generalized facilities for the support of random queries to the data available on the direct access medium. Teleprocessing systems were paired with locally and remotely connected *terminals* to provide for timely response to operator queries.

The advent of general terminal availability to the computing community gave rise to timesharing systems, as well as, teleprocessing systems. The data processing community began to utilize the terminal provided access for improved productivity within its own ranks. Quickly, the terminal device became general purpose in its use and in its flexibility.

Today, these terminal devices are themselves programmable and can be used for a wide variety of data processing tasks. They are even used (quite commonly) for interconnection to other systems inside and outside the corporate environment that "owns" them.

Terminal devices have continued to evolve and now deliver tremendous flexibility and function to the individual desktop. Communication with host servers and mainframes across a wide variety of network protocols is now more normal than exception.

Software Subsystems

Each major software component (software subsystem) established its own primary mechanism for accessing the various terminals. Some common subsystems are:

- TSO - the Time Sharing Option
- CICS - the Customer Information Control System
- IMS - the Information Management System
- ICCF - Interactive Computing and Control Facility
- CMS - Conversational Monitor System
- NetView - Network Management Facility
- IDMS/DC - Database and Teleprocessing System
- UCC7 - CA's Job Scheduler

Figure 2. Common subsystems

There are, of course, many more subsystems within the data processing community. The fact they are not listed here is not intended to question their viability in the marketplace. The term **subsystem** will be used throughout this document to discuss all software systems that use ACF/VTAM facilities to communicate with terminals.

Terminal Access Methods

The subsystems each originally made their choices between four generally accepted methods to communicate with the terminals. The methods are:

1. EXCP - Channel Program level access
2. BTAM - Basic Telecommunications Access Method
3. TCAM - TeleCommunications Access Method
4. VTAM - Virtual Telecommunications Access Method

Figure 3. Terminal Access Methods

Each terminal access method had different characteristics and they were often used in combinations by single subsystems (CICS as an example). This combination of terminal access methods did provide the desired results, but required a heavy commitment by the data processing systems community to keep the terminals and their associated access methods providing service.

Access Method Evolution

The EXCP and BTAM approaches were used chronologically first, but their architectural limitations soon necessitated a more generalized approach. TCAM and its associated Message Control Programs became extremely viable for its consolidated terminal control along with its Time Sharing Option (TSO) interface for programmer productivity.

As the new communications protocols and architectures emerged, it became clear that TCAM, as it stood, would not suffice. The introduction of SNA architecture devices (as well as the communication protocols implied) required review of the whole *terminal access method* approach. This reorientation occurred with the full introduction of ACF/VTAM as a terminal access method capable of supporting the newer type devices as well as the older asynchronous (ASYNC) and binary synchronous (BI-SYNC) devices.

ACF/VTAM also introduced concepts necessary for the computing facility to share or *network* terminals between subsystems (like CICS, IMS, and TSO). This concept was also extended to include multiple CPUs (DOMAINs) and multiple networks (accessed via SNI gateway concepts). A large portion of the traditional terminal access method's responsibilities became the job of the terminal network hardware itself. The 370x telecommunications unit began polling BI-SYNC devices (the Network Control Program (NCP) accomplished this in the 3705 and its successors (3725, 3745, etc.)

The *evolution* of the terminal access methods was motivated by multiple factors.

1. The increased availability of the general computing facility caused an explosion in terminal connection to the CPU and the management of the large terminal network became a problem for the systems maintenance personnel.
2. As the computing facility's end user discovered the multiple subsystems, he/she desired access to all the environments without the requirement of purchasing multiple terminals.
3. The introduction of new communications protocols necessitated complete review of how terminal connections were made to the CPU. The connection had to be made in such a manner as to optimize CPU utilization, but not at the cost of the end user's response time.

As a result of these factors, the computing facility has extended into offices and work locations relatively quickly.

The following figure is a simple pictorial representation of two 3270 type terminals remotely connected to a CPU offering CICS, TSO, and IMS. ACF/VTAM has enabled either terminal and its associated user to be logically connected to any of the applications (TSO, CICS, or IMS) available in the host.¹

¹ We use the graphical representation of a basic personal computer (PC) to represent a generic terminal device. This includes any of a variety of actual hardware terminals, Personal Computers with suitably equipped 3270 connections (LANs, emulator boards, etc.) and any other appropriate 3270 work alike (session managers, etc.).

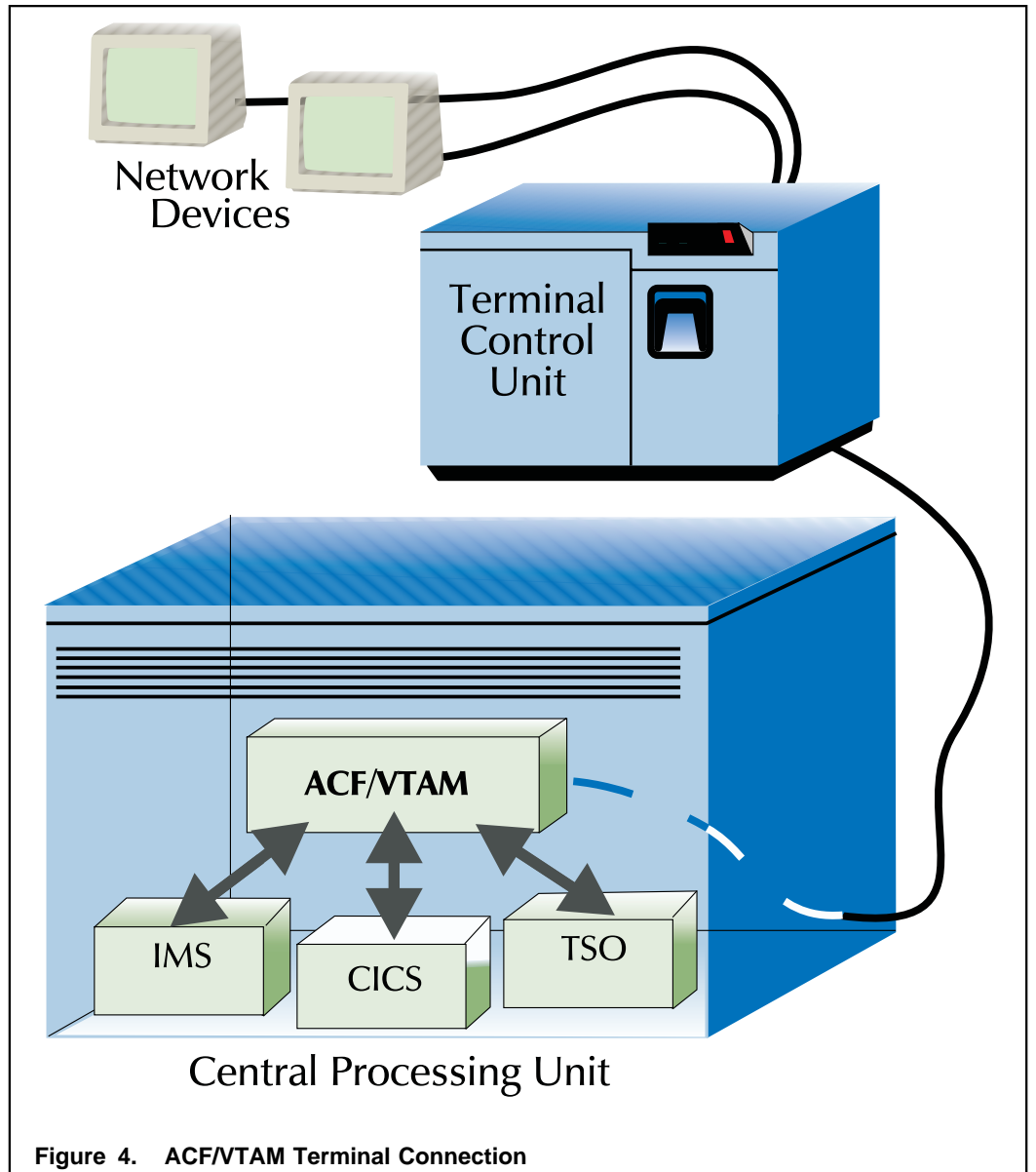


Figure 4. ACF/VTAM Terminal Connection

To summarize, the increased availability of relatively inexpensive computing facilities has led to a large increase in the number of terminals connected to the computing system.

Various terminal access facilities were and are being developed to respond to the need for easier and more consistent end user terminal interaction with the computing facility. The introduction of the ACF/VTAM Application Program Interface has enabled the major subsystems to utilize a standard terminal interface with which to deal with multiple terminal types.

Flexibility, usability, and productivity are of primary concern. These issues have remained throughout the entire evolution of the information processing environment. The development of Local Area Networks (LANs) and their corresponding access routines (TCP/IP, token ring, Ethernet, etc.) with associated emulation routines has only emphasized the need for providing consistent presentation to the terminal user.

Access Method Shortcomings

The terminal user has been increasingly presented with a larger variety of choices associated with utilizing data processing services. Traditionally, a single terminal was connected to a single subsystem on a single host (CICS as an example) and the terminal had no other purpose.

One of ACF/VTAM's extensions of function was the ability for the terminal user to communicate with ACF/VTAM directly and indicate that a specific terminal (the invoking terminal) should be logically connected to a specific subsystem (IMS, TSO, CICS, etc). This facility was a great aid in reducing the need to purchase multiple terminals for a single terminal operator's desk or work vicinity.

However, increased function always seems to lead to requests for more flexibility. Additional flexibility certainly can help the productivity issue as well as increase usability of the computing facility. Thus, we are led to this section's subject, **Access Method Shortcomings**, that have arisen as a result of the improved function provided by the ACF/VTAM conceptual terminal environment.

1. It is not always clear to all terminal operators how they should make their request to ACF/VTAM to *logically connect* their terminal to a particular *application*.

ACF/VTAM provides facilities to establish the "logical connections". The early releases of ACF/VTAM called the facility *NETSOL* and the more recent releases refer to it as USS (Unformatted System Services). Unfortunately, USS is truly "unformatted" and the terminal operator is typically left to entering a one to eight byte code that may or may not be meaningful to him/her.

Many installations have chosen to implement an ACF/VTAM selection menu which helps considerably (a **message 10** or USSMSG10), but the untrained operator may still have difficulties. Messages like **SESSION NOT BOUND** may still appear on a terminal operator's screen, which is not particularly meaningful to a novice user.

2. Any ACF/VTAM terminal can request any of the "applications" present in the ACF/VTAM USS tables.

The simple fact is that any device within the ACF/VTAM environment can potentially *logically connect* to all subsystems (CICS, etc). While valuable to some, this facility could be considered a security breach to others. As with most other shared type facilities within the data processing community, terminal access to applications should be controlled by the standard installation security routines. ACF/VTAM itself provides no facilities to check **who** is at the terminal and whether the individual is allowed to do the operation currently being attempted. This responsibility is left to the individual subsystem.

3. There is no common manner with which each terminal in the network can transmit information to another terminal.

Each major subsystem (TSO, etc) has facilities to transmit messages from one user to another, but the message will not arrive until the receiving terminal/user has *logged on* to the same subsystem that sent the message.

4. The terminal user has to repeatedly *log on* or *sign on* to the system.

Each subsystem has its own mechanism with which to authorize an individual user's access. Since each system has a slightly different format to sign on, the end user of the computing facility must know and understand multiple ways to identify himself.

This association of shortcomings with the terminal access methods is not totally fair. Rather, the shortcomings are general computing facility shortcomings. Therefore, they should be addressed as total system shortcomings rather than specific problems associated with the choice of a particular terminal access method.

The Network Director

The **Network Director** is a generalized software product based upon the concept that an improved and simpler interface to the terminal access method will improve the usability of the computing facility and its associated subsystems. The Network Director is many things and can be configured in many ways, but at its simplest, it is a **Menu Manager** designed to assist and secure a large ACF/VTAM based terminal network.

The Network Director considers the terminal network a valuable resource that must be capable of being controlled and managed by the computing facility, but not at the cost of ease of use by the end user.

The Network Director is a system software component that simplifies the terminal operator's access to the computing facility. It also provides additional network services not available elsewhere (network terminal security, message switching, network demographics, etc). Multiple facilities are provided to make the terminal network more manageable for the network support staff responsible for assisting in the use and reliability of the network.

Shortcoming Resolutions

The Network Director has been designed to provide relief from the previously referenced *shortcomings*. In the previous format:

1. It is not always clear to all terminal operators how they should make their request to ACF/VTAM to *logically connect* their terminal to a particular *application*.

The Network Director always maintains a user or terminal specific menu of *functional areas* that the user or terminal may select from. The terminal operator does not need to know the *name* of his/her subsystem or even which particular ACF/VTAM subsystem or operating system the desired application is executing in.

The Network Director provides an interaction mechanism that conforms to the Common User Access (CUA) principles of Systems Application Architecture (SAA) including full support for 3270 program function keys as well as supporting a wide variety of other **selection methods**. The keys are, when available and in "non CUA mode" associated with specific menu choices and can be used as a shorthand method for the operator to make a selection from the menu.

2. Any ACF/VTAM terminal can request any of the *applications* present in the ACF/VTAM USS tables.

The Network Director does not use ACF/VTAM's USS tables to construct the terminal or user specific menu. Thus, the terminal or user can be restricted to

selecting only those applications that are authorized for the specific terminal or user.

The Network Director maintains information about which operators and which terminals were routed to which other ACF/VTAM applications and when the activity occurred. This information can be used to audit the type of routing activity the terminal network is involved in.

The specific menus can be tailored to an individual based upon his/her user id and not simply the terminal name. Contents of the menus can be controlled via Network Director definitions or from information derived from the installation security package.

3. There is no common manner with which each terminal in the network can transmit information to another terminal.

The Network Director provides a simple, generalized message management facility. The message switching mechanism allows the operator to queue messages to other terminals, users, or logical groups of terminals or users. Naturally, the individual user may also view any messages intended for him and respond as the message *conversation* requires.

The Network Director also provides a generalized broadcast facility for the computing facility to post notices of general interest to the entire terminal network. Messages can be sent to individuals, group of terminal operators, to the whole network, or simply to network participants authorized for a specific selection (e.g. to all TSO users).

4. The terminal user has to repeatedly *log on* or *sign on* to the system.

The Network Director can be configured for specific terminals (or the installation as a whole) to prompt for the terminal user's *user id* and *password* and accomplish validation against the system security package (ACF2, RACF, TOP-SECRET, VM/SECURE, etc.). If The Network Director has collected this information, it will pass it along to the proper subsystem when the user requests the connection. This is called The Network Director's **Single System Image** (SSI) facility.

The Network Director also provides optional routines for specific subsystems to completely automate the sign on process. As an example: If The Network Director has been provided the user id and password at the time of a request to connect to a CICS system, The Network Director's optional CICS routines can automatically cause the user to be CSSNed. This can virtually eliminate the need for a terminal user to be familiar with differing logon procedures.

Thus, it is possible that any given user can be assigned a single user id and password combination that will be asked for only once regardless of the number of subsystems the user is involved with.

Execution Environment

The Network Director is primarily a **front end** to the ACF/VTAM provided facilities. It provides facilities similar to the original NETSOL and the current USS, but The Network Director has greatly expanded the ability for the computing facility to manage the network. It has also provided a much simpler method with which the terminal operator can communicate his/her *logical connection* requests.

The Network Director typically manages all terminals within the network that are **not currently** in session with a subsystem. All requests from the terminal operator are processed by The Network Director. When the operator has made a valid request, The Network Director simply passes *ownership* (a VTAM CLSDST PASS operation) of the terminal to the appropriate target subsystem. When the "logical connection" with the subsystem is terminated (via specific subsystem requests), the terminal returns to The Network Director (via the LOGAPPL relationship or a queued ACQUIRE) and the operator will receive the selection menu once again.

Of course, this sample assumes that network management personnel have made several decisions about how The Network Director is to control the terminals. There are several other scenarios possible. Several of the possible scenarios are discussed in this manual in "Concepts and Facilities" on page 17.

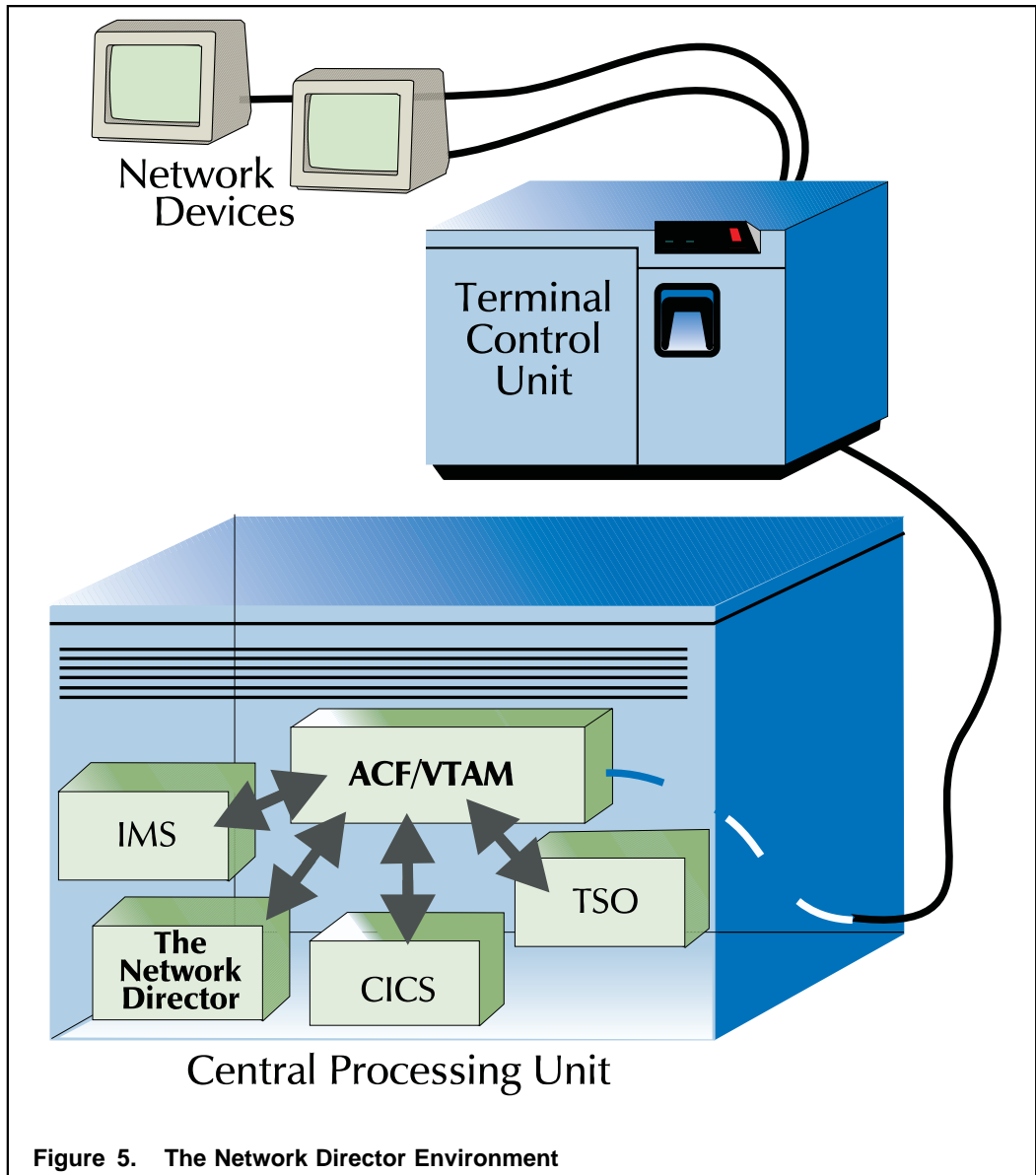


Figure 5. The Network Director Environment

The Network Director exists as any other job does within the operating system. The Network Director will operate as an independent MVS address space, or DOS partition, or a VM virtual machine. It also appears to ACF/VTAM as would any other ACF/VTAM subsystem (like TSO, etc.)

Note: This pictorial representation of a network has been greatly simplified and should be used only to logically identify how The Network Director fits in relation to other components of the network.

Concepts and Facilities

The facilities provided by The Network Director are predicated upon several basic concepts. This section of the manual will identify the concepts and generally discuss how they have been transferred into facilities.

This section of the manual first identifies the specialized phrases used when discussing The Network Director. It will then describe the Configuration Parameters followed by each of the basic facilities implemented within The Network Director. The reader is reminded that each subject explored within this manual is discussed in more detail in other Network Director manuals.

Terms and Phrases

The following terms and phrases will be used when discussing The Network Director's functional areas. Terms and phrases of a significantly larger scope are identified in the Glossary. The terms described here will be used in relation to The Network Director and may not have applicability outside The Network Director's environment.

Term	Usage
ACF/VTAM	The Virtual Telecommunications Access Method. This is used generically by The Network Director to indicate a Terminal Access Method capable of responding to the documented ACF/VTAM Application Program Interface.
application	Used to describe the User described combination of programs, files, and processes that allow a business function to occur (e.g. Payroll and Inventory are examples of applications).
computing facility	The combination of hardware, software, and personnel that provide the automated environment for the User to accomplish assigned tasks. Often referred to as <i>The Data Center</i> or other generic names.
logical connection	Identifies the software path established by ACF/VTAM between the Terminal and the Application.
Network Administrator	This is the generic title of one or more individuals authorized by the Computing Facility to manage the functioning of the terminal network.
password	The 1 to 8 byte code, when used in combination with the User Id, validates that the User using the User Id is indeed the proper individual. This is typically the first level of the Computing Facility's security mechanism.
subsystem	This is the term used to identify the software component that is host to one or more Applications. TSO, CICS, IMS, ROSCOE, CMS, IDMS/DC, ICCF, NetView, and MODEL204 are examples.
target application	This term identifies the logical Application to which the Terminal or User has requested a Logical Connection.
Terminal	The physical device managed by ACF/VTAM that can connect to multiple subsystems at the request of the User. This can also be referenced as a "workstation", that is simply a programmable device that follows defined SNA protocols.
user	The individual utilizing the Terminal to accomplish work related duties. The User can be considered either the data processing staff members or the individuals using systems developed by the data processing staff.
user id	The 1 to 8 byte User identification code assigned to the User by the Computing Facility.

Figure 6. Basic Terms and Phrases

Configuration Parameters

The Network Director accepts its execution time parameters from a single input file called the Configuration Parameters or from a previously stored set of definitions saved in a disk file referenced as the External File. The Configuration Parameters consist of 80 character record images containing positional and keyword parameters describing The Network Director's view of the network. The External File is a VSAM based disk file consisting of variable length records in a compressed format recognizable to The Network Director.

The initialization parameters allow the Computing Facility, through the Network Administrator, to define Users, Terminals, Applications, User Ids, Passwords, Groups, etc. The reader is referred to The Network Director's *Network Administrator's Guide* for more detailed information.

It is important to note that The Network Director identifies three basic components that, in combination, allow The Network Director to make environmental decisions about how to interact with the Terminal and/or User. These basic building blocks are the USER, TERMINAL, and APPLICATION. Note that APPLICATION does not necessarily imply subsystem, but can be the functional application system.

The Application Selection Panel

To correct the difficulties associated with the first shortcoming (how to communicate with ACF/VTAM), The Network Director presents an individually tailored **Application Selection Panel** (a menu of application choices) for the terminal operator to interact with the Computing Facility. This will be based on a global default provided to The Network Director through the Configuration Parameters, a specific menu for the specific terminal, or a specific menu for the specific user at the terminal. The Network Administrator will indicate to The Network Director which menu should take effect if a User with a defined menu sits at a Terminal with a differently defined menu.

The Network Administrator also indicates the general "form" of panel presentation that The Network Director will use with the user. Either **non CUA** or **CUA** mode will be in effect, depending upon the installation requirements.

Non CUA Operations

The following discussion assumes the Network Administrator has selected a non CUA format for panel presentation. The CUA presentation is discussed beginning with "CUA Operations" on page 27.

```
*****
***
**                               **
**           The Network Director           **
**           from North Ridge Software      **
***
*****

  _ General Personnel System      (PF01)
  _ Accounts Payable Inquiry      (PF02)
    Program Development           (PF03)
  _ Network Director Assistance    (PF04)
  _ Messages                       (PF05)

Command: _

Id: _____ Password: _____ Extension: _____ Time: 10:01:34
Ll: T01001 Account: _____ Date: 07/23/97
28
```

Figure 7. Basic Application Selection Panel

The Network Administrator has a wide variety of parameters available to tailor the usage of the computing facility for optimum usage and without compromising security. The Network Director's TERMINAL definition provides the Network Administrator with the ability to define the characteristics for the selection menu at a specific terminal. The USER definition provides the mechanism to do the same for a specific user.

The Network Administrator need only define those Terminals or Users that require special handling. The DEFAULT definition provides the Network Administrator the ability

to define a selection menu in the event that neither the User or the Terminal are otherwise defined.

Configuration Parameters

The following Network Director statements were used to create the previous Application Selection Panel:

```
APPLICATION PEOPLE, TARGET=CICS1,  
                                TITLE='General Personnel System'  
*  
APPLICATION PAYABLE, TARGET=CICS2,  
                                TITLE='Accounts Payable Inquiry'  
*  
APPLICATION CODING, TARGET=TSO,  
                                TITLE='Program Development'  
*  
TERMINAL    T01001, COMMANDS=YES,  
            APPLICATIONS= (PEOPLE, PAYABLE, CODING)
```

Figure 8. Simple Configuration Parameters

First, let's look briefly at these initialization parameters.

- The APPLICATION statements define three different logical applications with the names PEOPLE, PAYABLE, and CODING. Each of these Applications has a logical TITLE which will be used to construct the Application Selection Panel. They also have a TARGET, which corresponds to the ACF/VTAM APPLID assigned to a particular subsystem.
- The TERMINAL statement does no more than indicate which Applications are accessible from the terminal named T01001. In this manner, the Network Administrator can control which Applications the terminal can request. The COMMANDS operand indicates that the Command: line should be present. This allows the terminal operator to utilize additional methods to interact with The Network Director.
- The top six lines of the panel contain the default LOGO for The Network Director, but the Computing Facility can define its own LOGO via the LOGO operand in the Configuration Parameters.² Separate LOGOs may be specified for Users, Terminals, and Groups in any desired combination.
- The bottom lines on the panel contain identifying information about the terminal in use. The additional fields (Id, Extension, Account, and Password) will be discussed in more detail in later sections.

² A generalized color attribute scheme contained within The Network Director allows the installation to include extended attributes and colors within the LOGO and other portions of The Network Director's panels.

Panel Body

Now let's focus on the selection panel body itself. The Network Director builds the Application Selection Panel to make optimum use of the physical device. Our example is assuming a 24 by 80 3277 type device, but if a larger device is in use, The Network Director will attempt to *balance* that screen size also. The Network Director supports alternate screen sizes when available (3270 Models 2, 3, 4, 5 and the 3290 Plasma panel in native mode).

To construct the panel, the size of the LOGO and identifying information (in lines) is subtracted from terminal depth. The remainder is divided by the number of valid selections the physical device will The Network Director will leave the choices stacked *one up* and double spaced until the number of selections will no longer fit comfortably. The Network Director will then attempt to single space the selections. If the selections will still not fit, The Network Director will build the selections into two columns in order to fit additional entries onto the physical device. If there are still more entries for the terminal operator, The Network Director will allow the device to "page" forward by simply striking the ENTER key.

Selecting an Application

The user at the terminal may select any single application by:

1. moving the cursor to a location between the underscore "_" in front of the application TITLE and the right parent ")" and striking ENTER
2. entering any value in the single byte input field and striking ENTER (the modified field will be used as an indication of selection)
3. typing the application's Name on the Command: line and pressing ENTER
4. typing PF01, simply the number 1, or the literal string "ONE"
5. using the 3270 light pen or suitable alternative, for any device properly equipped
6. pressing the function key indicated on the right side of the application TITLE

Logging onto the System

The Network Director's Application Selection Panel also provides facilities for a user to identify himself to receive individual selections. Assume that the terminal we are dealing with (TM03) does not have a TERMINAL statement and IDENTIFICATION=YES is in effect.

This arrangement implies to The Network Director that the terminal is not usable with any applications until someone at the terminal identifies himself/herself and the logon combination has been validated by The Network Director or the installation security package. The Network Director will present a panel to the terminal whose only purpose is to allow the terminal operator to enter a valid User Id and password combination. The panel will appear similar to the following panel:



Figure 10. User Id Identification Panel

The User can press PF1 or otherwise mark The Network Director's Assistance entry, but the Terminal itself will not be passed to any applications until the terminal operator has successfully identified himself. If the terminal operator attempts to identify himself and fails due to invalid User Ids or User Id/Password combinations, the terminal itself can be placed onto an inactive list by The Network Director after an installation specified number of attempts. It will not be possible for any entry to occur at the device until the Network Administrator reinstates the terminal.

This retry checking can be controlled by the Network Administrator through Network Director parameters or the installation security officer if ACF2 or RACF are installed and in use. It can be turned off or the number of retries can be specified. Additionally, any violations will be logged to The Network Director's LOG file. The LOG file is accessible from a Network Administrator terminal and/or is typically printed onto hardcopy at some point in the processing day. Events like a security violation may also be recorded in the operating system's data recording medium (e.g. OS SMF, VM accounting records, etc.).

The ability for the User to identify himself in this way allows a single terminal in a shared location to take on different authorizations based on the individual sitting at the terminal.

It is also possible to intermix TERMINAL and USER definitions. A single terminal may have a default for the terminal, but a specific user may change the menu by entering a specific Id and pressing ENTER. This is useful when a terminal is in a specific location and is usually used by all the individuals in that location for a preset group of functions (the TERMINAL statement defines this condition). However, should a specific User want to change the definition for a few interactions, it can be done by simply identifying oneself.

An important concept must be raised at this point in the discussion. That is, The Network Director should not allow a Application Selection Panel that could be considered *authorized* to remain on a terminal beyond the authorized individuals presence there. Clearly, it is difficult for The Network Director to absolutely guarantee this particular situation, but it can assist.

The Network Director will begin a *timer* on any panel that has a Application Selection Panel on it that is not considered the default. If the terminal and/or user of that panel has not done anything (specifically has not interacted with the system by pressing function keys) within a Network Administrator specified time interval, the default panel will be placed upon the terminal. This will be either the User Id Identification Panel or the Application Selection Panel (as specified via the TERMINAL definition).

Important to note is that The Network Director will not actually display the password at any point. The Network Director will utilize the standard facilities associated with the 3270 terminal to make the field nondisplayable.

The Profile

The Network Director maintains for each User and Terminal an internal Profile for the individual or individuals using the network. This Profile contains generalized information about the session in progress and provides the terminal operator a manner with which to control certain aspects of The Network Director's operation as it relates to the specific terminal operator.

The Profile's contents are set initially by The Network Director based upon the contents of the configuration definitions. The operator may be authorized to modify his or her Profile. The modified Profile will remain in effect across Network Director restarts, which allows each authorized operator the opportunity to tailor The Network Director as it pertains to his or her individual needs.

The Profile mechanism allows the operator to control items like the Account field default on the Application Selection Panel. The default printer for Printed Messages is another example. However, it is important to note that the items available for modification via the Profile are only those items pertaining to the operator's use of the facilities of The Network Director. APPLICATIONS, etc. are always controlled by the Network Administrator and cannot be directly managed by the operator.

The Profile panel is reached from any other Network Director panel by entering the PROFILE command. Additional information and an example of the Profile panel can be obtained from The Network Director's *Network User's Guide*.

CUA Operations

The following discussion assumes the Network Administrator has selected a CUA format for panel presentation. The non CUA presentation is discussed beginning with "Non CUA Operations" on page 20. If you do not believe you would make use of the CUA format, you can skip this section of the manual and continue with "The Message Facility" on page 34.

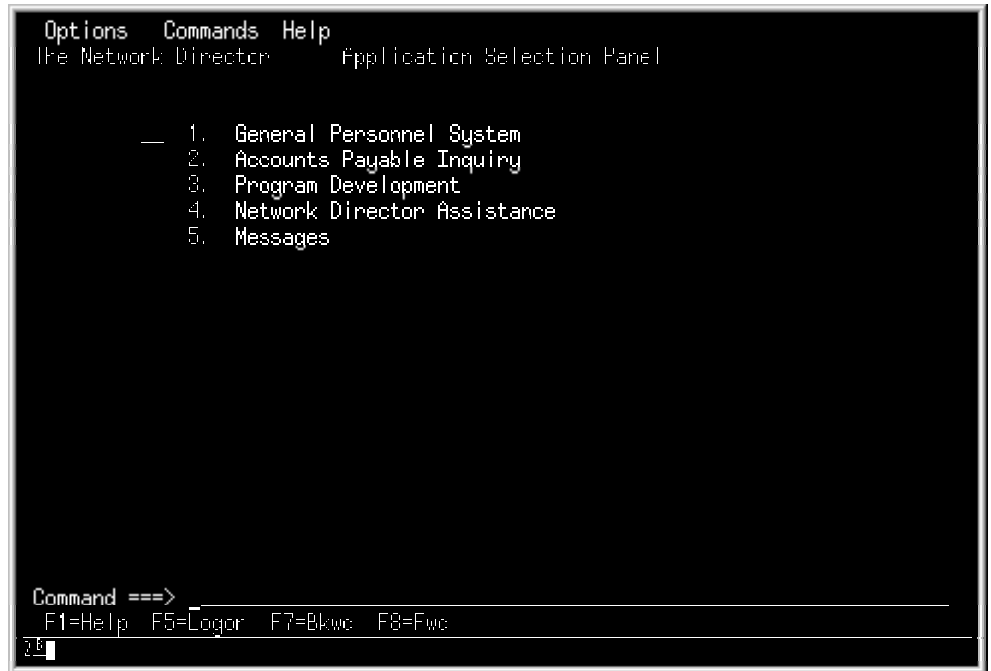


Figure 11. Basic CUA Application Selection Panel

The Network Administrator has a wide variety of parameters available to tailor the usage of the computing facility for optimum usage and without compromising security. The Network Director's TERMINAL definition provides the Network Administrator with the ability to define the characteristics for the selection menu at a specific terminal. The USER definition provides the mechanism to do the same for a specific user.

The Network Administrator need only define those Terminals or Users that require special handling. The DEFAULT definition provides the Network Administrator the ability to define a selection menu in the event that neither the User or the Terminal are otherwise defined. The DEFAULT statement can also be used to simply place certain applications on all Application Selection Panels ("Network Director Assistance" and "Messages" on this panel are an example of two applications that are active as a result of the DEFAULT definition).

Configuration Parameters

The following Network Director statements were used to create the previous Application Selection Panel:

```
DEFAULT      APPLICATIONS= (NDHELP, MESSAGES)
*
APPLICATION  PEOPLE, TARGET=CICS1,
              TITLE='General Personnel System'
*
APPLICATION  PAYABLE, TARGET=CICS2,
              TITLE='Accounts Payable Inquiry'
*
APPLICATION  CODING, TARGET=TSO,
              TITLE='Program Development'
*
TERMINAL     TM03, CUA=YES,
              APPLICATIONS= (PERSONNEL, PAYABLE, CODING)
```

Figure 12. Simple Configuration Parameters

First, let's look briefly at these initialization parameters.

- The DEFAULT statement defines two applications for everyone's use (APPLICATION definitions for NDHELP and MESSAGES are defined elsewhere)
- The APPLICATION statements define three different logical applications with the names PEOPLE, PAYABLE, and CODING. Each of these Applications has a logical TITLE which will be used to construct the Application Selection Panel. They also have a TARGET, which corresponds to the ACF/VTAM APPLID assigned to a particular subsystem.
- The TERMINAL statement does no more than indicate which Applications are accessible from the terminal named TM03. In this manner, the Network Administrator can control which Applications the terminal can request. The CUA operand activates the CUA mode of operation for the identified device.

Panel Body

Now let's focus on the Application Selection Panel body itself. The Network Director builds the Application Selection Panel to make optimum use of the physical device. Our example is assuming a 24 by 80 3277 type device, but if a larger device is in use, The Network Director will attempt to *utilize* that screen size also. The Network Director supports alternate screen sizes when available (3270 Models 2, 3, 4, 5 and the 3290 Plasma panel in native mode).

To construct the panel, the CUA Options characteristics for the specific device or user are consulted. If active, the "Function Keys" are placed in the last line of the panel and the "Command" line is placed immediately before it. The Network Director presents the current application choices in a standard CUA list format with each choice identified by a unique, ascending number value. When the choices exceed the number of lines available on the physical device, The Network Director allows the terminal user to "page" forward (and backward) by appropriate use of the F7 and F8 function keys.

Selecting an Application

The user at the terminal may select any single application by:

1. moving the cursor to any location on the same line as the application title and striking ENTER
2. entering the application's numeric value in the input field placed immediately before item number 1
3. typing the application's Name on the Command: line and pressing ENTER
4. typing the numeric value of the selection or a literal string equivalent to the numeric value (e.g. "ONE") and pressing ENTER
5. using the 3270 light pen or suitable alternative, for any device properly equipped

Application Status

The application titles indicate their availability to the user by their color or intensity (a CUA standard). Blue or low intensity applications are not available. White or high intensity titles indicate that the application is available.

There is also an area on the physical device reserved for general Network Director messages (immediately before the Command line). Assume that the PAYABLE application is down (CICS2 is not running) and that the Network Administrator has broadcast an informational message about the condition. The Application Selection Panel will look like this:

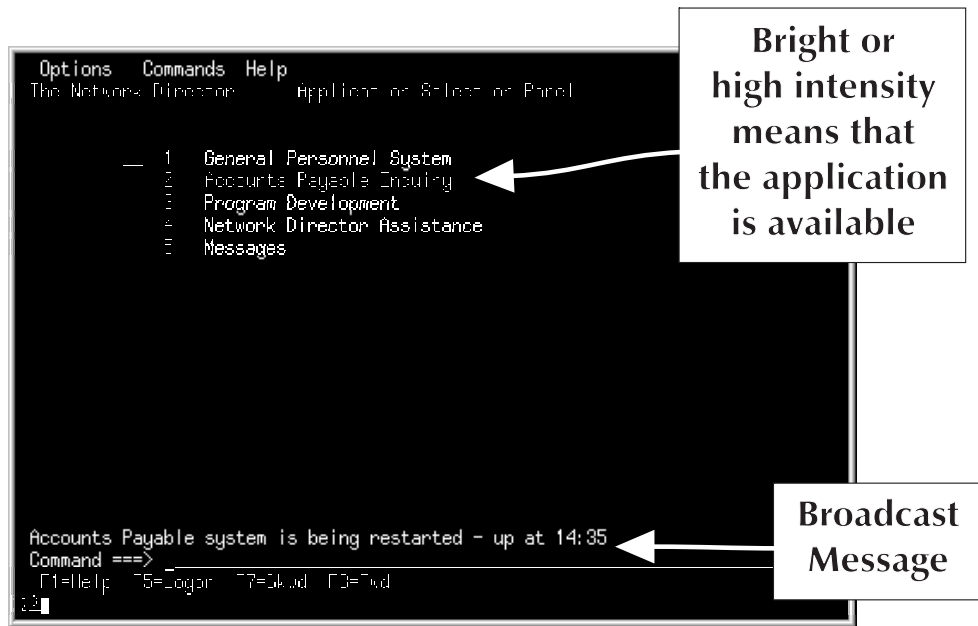


Figure 13. Basic CUA Application Selection Panel with Message

The Network Director will automatically refresh the Application Selection Panel whenever there is a change in the *status* of any one of the applications referenced on the panel, after a Network Administrator time specified interval for broadcast messages (like the sample *up at 14:35* message above), or whenever the terminal operator presses any function key.

The terminal will be usable for the displayed Applications immediately. It may also be used to identify the individual using the terminal and thereby receive another Application Selection Panel customized to that specific User.

Note: The "Messages" and "Network Director Assistance" entries on the panel are there based on the contents of the as yet undescribed DEFAULT statement. The Network Director does not automatically include these options, although they are recommended and typically provided as a default.

The ability for the User to identify himself in this way allows a single terminal in a shared location to take on different authorizations based on the individual sitting at the terminal.

It is also possible to intermix TERMINAL and USER definitions. A single terminal may have a default for the terminal, but a specific user may change the menu by entering a specific Id and pressing ENTER. This is useful when a terminal is in a specific location and is usually used by all the individuals in that location for a preset group of functions (the TERMINAL statement defines this condition). However, should a specific User want to change the definition for a few interactions, it can be done by simply identifying oneself.

An important concept must be raised at this point in the discussion. That is, The Network Director should not allow a Application Selection Panel that could be considered *authorized* to remain on a terminal beyond the authorized individuals presence there. Clearly, it is difficult for The Network Director to absolutely guarantee this particular situation, but it can assist.

The Network Director will begin a *timer* on any panel that has a Application Selection Panel on it that is not considered the default. If the terminal and/or user of that panel has not done anything (specifically has not interacted with the system by pressing function keys) within a Network Administrator specified time interval, the default panel will be placed upon the terminal. This will be either the User Id Identification Panel or the Application Selection Panel (as specified via the TERMINAL definition).

Options

The Network Director maintains for each User and Terminal an internal set of **Options** for the individual or individuals using the network. These Options contain generalized information about the session in progress and provides the terminal operator a manner with which to control certain aspects of The Network Director's operation as it relates to the specific terminal operator.

The Option's settings are set initially by The Network Director based upon the contents of the configuration definitions. The operator may modify his or her Options via the Options action, which can be selected from the Action Bar (see the *Network User's Guide* for an example of the Options pull down). The modified Options will remain in effect across Network Director restarts, which allows each authorized operator the opportunity to tailor The Network Director as it pertains to his or her individual needs.

The Options action allows the operator to control items like the where to place the Command line, whether to display the unique panel id or not, what form the function keys should be displayed in, etc. However, it is important to note that the items available for modification via the Options are only those items pertaining to the operator's use of the facilities of The Network Director. APPLICATIONS, etc. are always controlled by the Network Administrator and cannot be directly managed by the operator.

The Message Facility

The Network Director provides a self contained message switching facility. Any terminal or operator authorized to access the message facility will have it as a choice on the Application Selection Panel. In this manner, the message facility is controllable exactly as access to any other Application would be.

The message facility can provide an automated manner in which to manage and transmit information between individuals and departments within the computing facility and between multiple computing facilities where each one is operating a copy of The Network Director. It can be used to reduce the amount of one and two page notices that occur with increasing frequency within business.

The Network Director's message facility is based upon three types of *messages*. They are *notes*, *memos*, and *broadcast* messages. The message facility provides mechanisms for the originating terminal to enter, modify, delete, and send the message. The receiving terminal(s) may view or delete messages intended for it.

Memo

The term **memo** is used to describe the traditional paper correspondence. The Network Director considers a memo as a document that should be dealt with independently of other messages and assumes that it may contain a relatively large amount of information (typically multiple paragraphs).

Note

The term **note** is used to identify essentially a brief *memo*. A note is considered by The Network Director to be of a brief nature (usually a quick paragraph or two).

Broadcast

Broadcast messages are a specialized type of message in that they are limited to the size of the Broadcast Area (typically 80 characters) so that they will fit on the Application Selection Panel (remember the "up at 14:35" broadcast on the previous Application Selection Panels?). Broadcast abilities are typically limited to the Network Administrator and some of the computing facility's operations staff.

To a great extent a Memo and Note are merely categories of messages that allow the Network Administrator to differentiate processing characteristics. Each category of Message can be stored by The Network Director for differing lengths of time and can be independently stored via storage or disk queueing mechanisms. Thus, the difference between a Note and Memo is really determined by each installation and how the Message Facility will be utilized.

When the terminal operator has selected the **Messages** option on the Application Selection Panel, The Network Director will present a panel similar to the following.

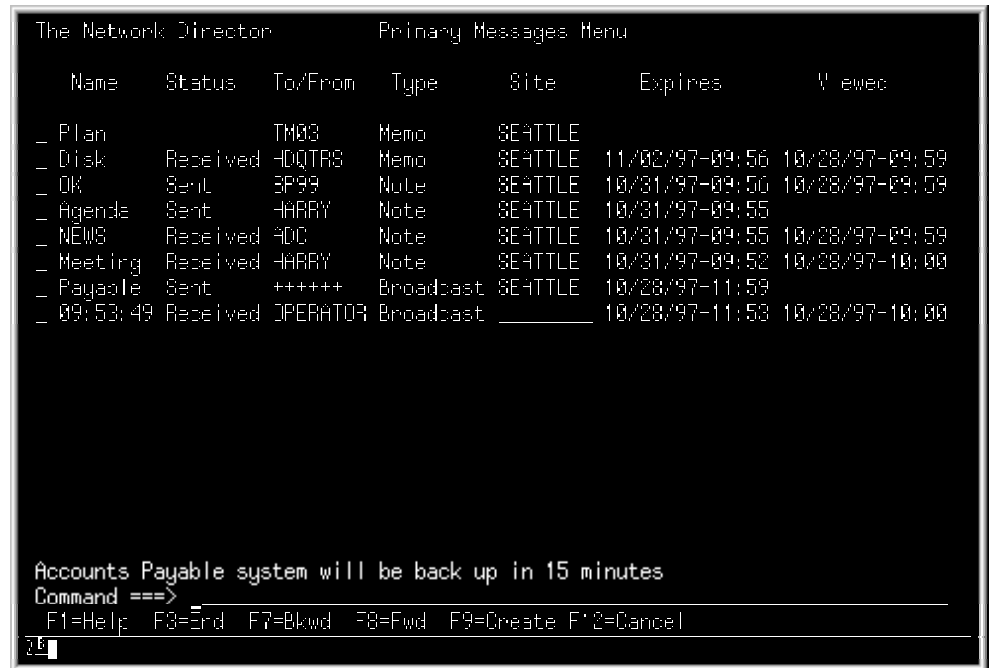


Figure 15. Primary Messages Menu

The bottom of the panel contains the **Function Key Area**, which displays the active function keys and their meanings.³

The Primary Messages Menu displays the messages you are involved with one to a line. Each individual message has multiple elements that identify it and describe its current status, which are listed in individual columns.

Each message has an underscore "_" before it that is intended to accept a message *action code* of V (View) or B (Browse), D (Delete), E (Edit), P (Print), R (Redirect), T (Extend), or S (Send). Space for creating a new message can be generated by entering the **CREATE** or **ADD** primary command (F9). This will cause a new line to be created on the menu that you may enter the message name, destination, and site values into during Edit operations.

³ This function key area conforms with IBM's Common User Access (CUA) definitions within the System Application Architecture.

The individual columns are used in the following manners:

Title	Purpose
Name	Contains the logical identifier the message originator associated with the message (this field is upper and lower case sensitive).
Status	Identifies the current disposition of the message. This field will be blank for messages you have started to create, but have not Sent yet. It will have the literal "Sent" for messages you have already forwarded and "Received" for messages that have been sent to you.
To/From	Establishes where messages you originated will be or have been Sent or the origin of messages that have been sent to you.
Type	Identifies the type of message. This will be "Note", "Memo", or "Broadcast".
Site	Is the logical identity of The Network Director that normally deals with the message originator or message destination. This is useful when your system is configured with multiple Network Director's operating in multiple VTAM domains. Messages sent or received cross domain or cross network via NSI will have the destination or origin Network Director's identity stored here.
Expires	Displays the date and time that the message will expire (if the message has been Sent).
Viewed	Displays the last date and time that a user associated with the message destination looked at the message

Our sample panel (Figure 15 on page 35) has five notes, one memo, and one broadcast destined for this terminal. The device has initiated two notes and is currently working on a Note identified as "OK" that has not been completed.

If there are more messages than can be displayed on a single panel, the terminal operator may view successive panels simply by using the functions Fwd (F8) or Bkwd (F7). The End (F3), Cancel (F12) command, or the CLEAR key will return to the Application Selection Panel.

Additional and more detailed information about how to use The Network Director's Message facility can be found in The Network Director's *Network User's Guide*.

Network Information File

The Network Director also provides a generalized, terminal oriented repository for information called the **Network Information File**. When activated, any terminal operator may access the contents of the Information file (an external VSAM file) to retrieve information associated with the use of The Network Director. The Network Director is delivered with approximately 300 24 by 80 panels that describe the various facilities that are contained and implied by The Network Director. It also contains a single panel for each of the approximately 750 Network Director messages that are issued by the system. These panels contain information similar to that contained in the *Messages and Codes* manual. The Network Director itself uses the Network Information File as an information facility to assist the terminal user's in the use of The Network Director.

The contents of the Information File can be extended or modified by each installation as appropriate. All changes are made dynamically by any authorized network user. Changes are made available immediately for usage within the network.

The Network Information File can be utilized to place information of general interest into a location that is generally accessible by the network users. It has been used to contain the computing facility's availability schedule, a list of key phone numbers and extensions, or other general documentation related to the entire system. It can be viewed as a *network bulletin board* for the posting of general notices.

Each panel in the Information File is uniquely named and numbered. The panels are logically related in an inverted tree structure with panel 0 being the initial panel. The Network Director's Information File provides for 10 panels at each point in the hierarchy and contains support for 5 levels (for a total of 100,000 possible panels).

Single System Image

One of The Network Director's goals is to present the non data processing user with a **single system image**. This effort is aimed directly at providing the user with a single User Id and Password combination that will provide access to appropriate subsystems without having to repeatedly *log on*.

This goal can only be achieved if The Network Director and all the involved subsystems use the same User Id/Password combination to identify the User. As an example, assume that The Network Director and TSO have had the same User Id/Password combinations set up. Once the terminal operator has identified himself to The Network Director and received his Application Selection Panel, he should not have to enter the User Id/Password combination again.

The Network Director will remember the user's identifying information and upon the user requesting a subsystem, The Network Director will make the identifying information available to the subsystem. In the case of TSO (CODING selection in the earlier figures), The Network Director will pass identifying information that will allow the terminal operator to become logged on to TSO without the traditional TSO **ENTER USERID** - message.

TSO is the simple case for this feature as most of the code required to accomplish this task is resident in TSO itself. But to provide this *single system image* to other subsystems, The Network Director provides specialized routines to accomplish the same task. Currently supported subsystems are: CICS, TSO, TSO/E, IMS/DC, IDMS/DC, NCCF, NetView, COM-PLETE, MODEL204, ROSCOE, CMS, and The Network Director itself.⁴

As another example, assume the following specification:

```
APPLICATION PAYROLL, INITIAL-FUNCTION=PAYR, SSI=YES
```

This Network Director APPLICATION definition instructs The Network Director to automatically signon the user to the subsystem (SSI=YES) and invoke the initial function of PAYR (INITIAL-FUNCTION=PAYR) if the signon is successful.

If the PAYROLL application is active within CICS and The Network Director's automated process is installed, the terminal operator will be automatically CSSNed onto the CICS system and the PAYR task within CICS will be started. All of these actions occur as a result of the terminal operator pressing a single key on The Network Director's Application Selection Panel.

The effect is that the terminal operator does not have to be aware of exactly where the PAYROLL application is executing, how to signon to the subsystem (CICS in this case), or even how to start the PAYROLL application (typing the PAYR transid). This eliminates the repetitive processes associated with the signon procedure between subsystems.

⁴ North Ridge Software, Inc. is continually adding new subsystems to this list. For status on a subsystem not mentioned here, contact North Ridge Software, Inc.

The Network Administrator

The Network Director provides multiple facilities to the Network Administrator. The Network Administrator can view The Network Director's LOG file, may modify any parameter provided in the initialization Configuration Parameters, may add definitions to the Configuration Parameters, view main storage in hexadecimal format, can display overview or specific information about activities occurring within the network, can issue VM CP commands (when in the GCS environment), and may interact with ACF/VTAM through the documented Program Operator ACF/VTAM facility.

The Network Administrator authorization is granted through the Configuration Parameters like any other application would be. Thus:

```
APPLICATION ADMIN, TARGET=TNDADMIN,  
                TITLE='Network Administration'  
*  
USER           SYSTEMS, APPLICATIONS=(PERSONNEL, CODING, ADMIN),  
                PASSWORD=SECRET, COMMANDS=YES
```

will result in one of the following Application Selection Panels (depending upon the operational mode for your device):

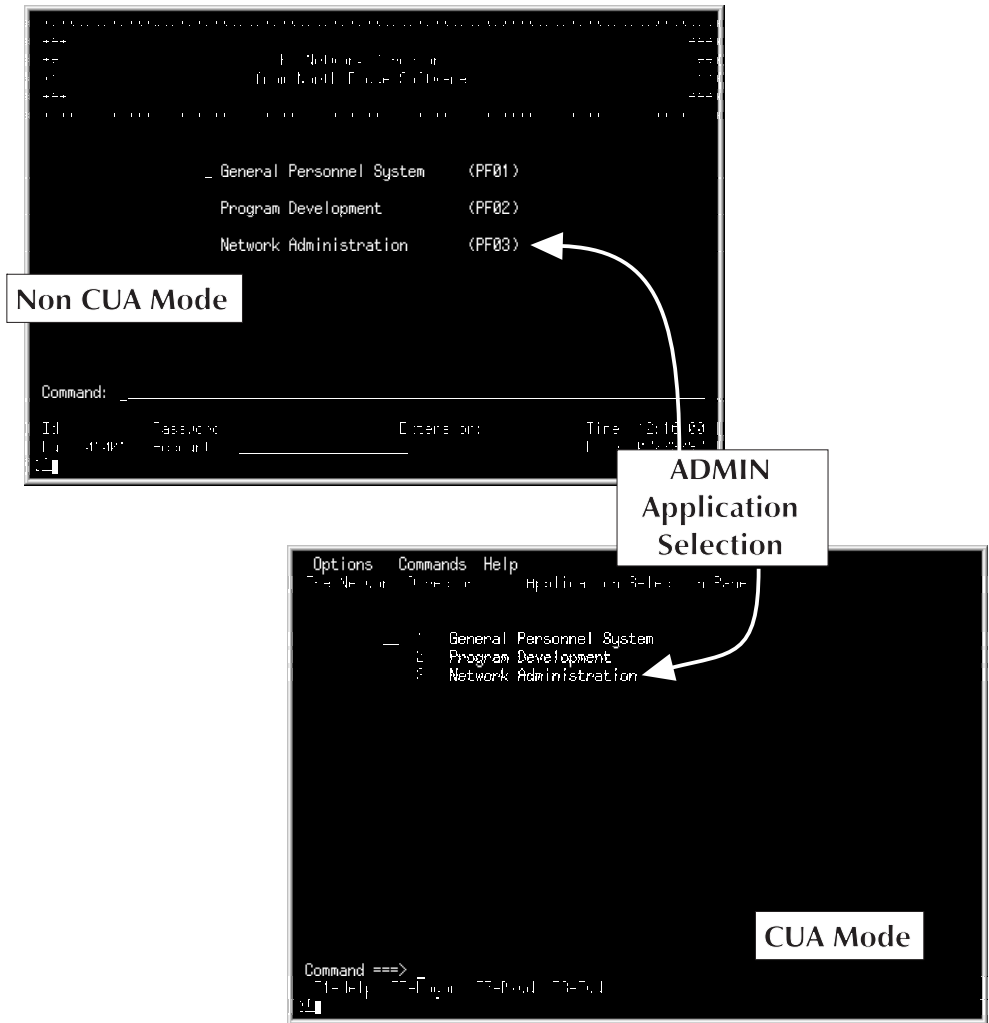


Figure 16. Network Administrator Application Selection Panel

The Application Selection Panel is similar in appearance to any other Application Selection Panel. The Network Director handles all specialized application functions (Network Administration and the Message Facility) as it would any other application. The primary difference is that The Network Director's internal functions will be handled without *passing* ownership of the terminal to another ACF/VTAM subsystem.

Additionally, this USER has been authorized to to issue *COMMANDS* directly from the *command line*. The Network Director provides this facility to allow the authorized individual to issue any generalized Network Director request. This includes *directed logon requests* as well as several Network Director based commands (LOGOFF, /RCL, RESET, etc.). These unformatted commands and the options associated with them are discussed in detail in The Network Director's *Network User's Guide*.

After selecting Network Administration or pressing PF3, a display similar to the following will be presented:

```

The Network Director      Administration      More: -
SYS140  04576 Lc T01SL104 - SYS140 - User Name has returned from CODING
SYS140  02276 Lc T01SL104 - SYS140 - User Name has selected ADMIN
ADMIN    01658 Id ADMIN - is now active at T01001 (0.000 secs)
ADMIN    02276 Lc T01001 - ADMIN - has selected CODING
ADMIN    04576 Lc T01001 - ADMIN - has returned from CODING
ADMIN    02276 Lc T01001 - ADMIN - has selected ADMIN
ADMIN    0249R Input: sh dir
ADMIN    04576 Lc T01001 - ADMIN - Network Operator has returned from ADMIN
ADMIN    02276 Lc T01001 - ADMIN - Network Operator has selected ADMIN
SYS140  04576 Lc T01SL104 - SYS140 - User Name has returned from ADMIN
SYS140  02276 Lc T01SL104 - SYS140 - User Name has selected PEOPLE
ADMIN    0249R Input: display counts
ADMIN    02886 2 terminals, 2 users active within The Network Director
ADMIN    02916 1 users have selected ADMIN - Network Administration
ADMIN    02916 1 users have selected PEOPLE - General Personnel System
SYS140  04576 Lc T01SL104 - SYS140 - User Name has returned from PEOPLE
SYS140  01668 Id SYS140 - User Name has logged off of T01SL104
OPERATOR 0224R Operator input: hold a=coding
OPERATOR 0328C Application CODING has been HELD

Command ==>
F1=Help F3=End F5=Locate F7=Bkwd F8=Fwd F10=Pref x F12=Cancel

```

Figure 17. Network Administrator Display

The Network Administrator may utilize this panel for:

1. Displaying The Network Director's LOG File
2. Controlling the Logical Network
3. Issuing ACF/VTAM or VM Commands
4. Network Reporting
5. dump main storage in hexadecimal format

Each facility has distinctly different functions and each will be briefly discussed here for informational purposes. The exact mechanism for using each of the facilities represented here is more thoroughly discussed in The Network Director's *Network Administrator's Guide*, the *Installation*, and the *Operations* manuals.

The LOG File

The Network Director maintains a *system LOG* file of all activity that occurs during the normal course of processing. The LOG initialization parameter controls the level of logging that is possible. The Computing Facility can choose to LOG every action that The Network Director does or (and more commonly) the LOG can contain only those items considered *significant activities*.

Examples of these are:

- A terminal operator that tried multiple times to identify himself without correctly entering the correct Password.
- A terminal that was placed onto or removed from The Network Director's *inactive* list.
- Any modification by a Network Administrator that affected the network definition.
- Defined Applications accepting LOGONs or rejecting them.
- A network element selecting or returning from an application.
- Any non zero ACF/VTAM return codes or sense information.
- A terminal user receiving a message from The Network Director

Each LOG entry produced by The Network Director is uniquely identified and time stamped. Additionally, LOG entries may be routed to the Operator. The Computing Facility may control which LOG entries should go to the Operator. As a default, The Network Director routes **no** messages to the console.

The Network Administrator may page through the LOG file (forward or backward). The LOG file can be an aid to network problem diagnosis, but is usually more useful in determining the sequence of events that potentially caused an end user to become confused about the availability of a subsystem. It may also be used to determine what a terminal that was placed on the inactive list was doing to cause the inactive placement.

Controlling the Logical Network

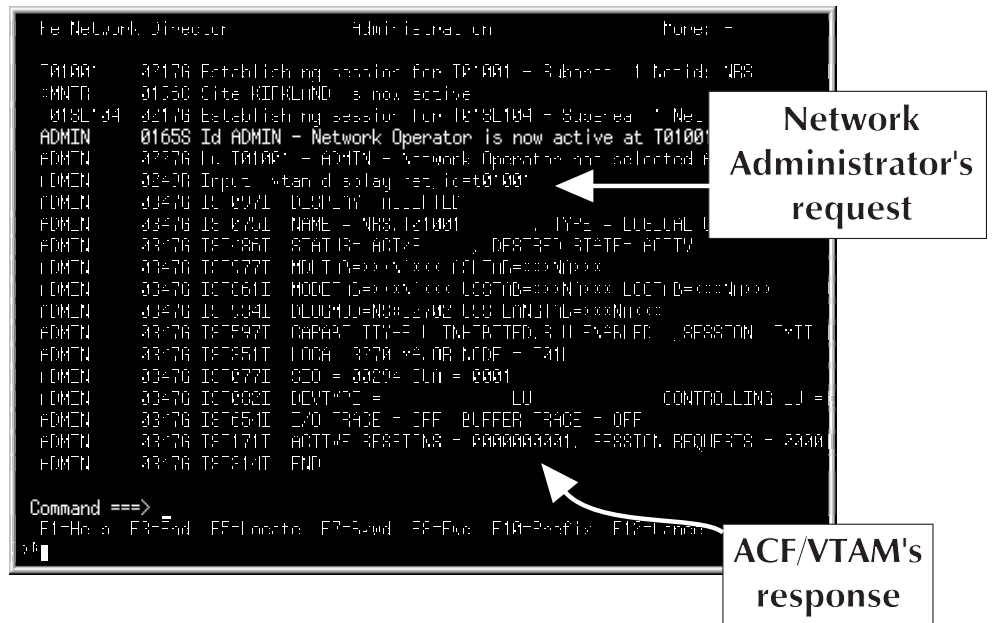
The second facility from the Network Administrator's panel allows the authorized Network Administrator to issue any Network Director parameter. The Network Administrator can temporarily or permanently add, delete, and modify APPLICATIONS, USERS, GROUPS, and TERMINALS. Any desired permanent changes made must also be made in The Network Director's physical initialization Configuration Parameters, if the installation is using only the Configuration Parameters for initialization.⁵

⁵ The SAVE and RELOAD commands are provided to allow all network definitions to be manipulated interactively via SHOW and saved in the External File.

Issuing ACF/VTAM or VM Commands

The Network Director can also interact with ACF/VTAM as a ACF/VTAM Program Operator or VM via the CP DIAGNOSE function. This third facility available from the Network Administrator's panel allows the terminal operator to issue VM or ACF/VTAM type commands and view the result on the panel.

ACF/VTAM commands as well as other Network Administrator commands are issued from the Primary Command line on physical line two of the panel. As an example:



```
The Network Director      Admin Instruction      Panel # =
T01000: 07176 Establishing session for T01001 = Subnet 1 (Lid: 085
ADMIN: 01050 Site KICKLAND is now active
01051:04 02176 Establishing session for T0101004 = Subnet 1 (Net
ADMIN: 01655 Id ADMIN - Network Operator is now active at T0100
ADMIN: 02476 Id T01001 = ADMIN - Network Operator and selected
ADMIN: 02476 Input wtan display req. (set=0100)
ADMIN: 02476 Id 0071 000100 000100
ADMIN: 02476 Id 0071 NAME = NRS, L21001 TYPE = LULOCAL
ADMIN: 02476 T0106T STATUS= ACTIVE DELETED STATE= ACTIVE
ADMIN: 02476 T0107T MOU T(=xxxxxxx) P(=xxxxxxx)
ADMIN: 02476 T0106T MOU CT(=xxxxxxx) LOSTID(=xxxxxxx) LOST(=xxxxxxx)
ADMIN: 02476 Id 0091 000000=0000 0000 LOSTID=xxxxxxx
ADMIN: 02476 T0109T CAPAB(ITY=1) UNATTENDED=0 EVALUATED=0 REASON=TEXT
ADMIN: 02476 T0105T LORA= 0076 00.00 NDR= 7311
ADMIN: 02476 T0107T SCD = 00204 LU = 0001
ADMIN: 02476 T0100T DCVTAP= LU CONTROLLING LU =
ADMIN: 02476 T0105T C/O TRACE = OFF BUFFER TRACE = OFF
ADMIN: 02476 T0107T ACTIVE REQUESTS = 0000000001, PENDING REQUESTS = 0000
ADMIN: 02476 T0104T END

Command ==>
F1-Help F3-End F5-Locate F7-Speed F8-Evt F10-Profile F12-Panel
36
```

Figure 18. Issuing Network Administrator Commands

Network Reporting

The last option associated with the Network Administrator's panel is the generalized query facility for The Network Director. The Network Administrator may display information about individual terminals, users, groups, and applications. Additionally, the Network Administrator can obtain global information about the network.

Examples of *global* information are:

- How many terminals are in the network and where are they currently connected. This can give the Computing Facility information about how many terminals are in a *logical connection* status with specific applications at any point in time.
- The Network Administrator can identify how many terminals are involved with specific Applications. This is differentiated from ACF/VTAM APPLID in that multiple Applications may exist within a single subsystem.

Additional information and detailed command syntax is contained in The Network Director's *Operator's Guide*.

Network System Interface

The Network Director provides multiple generalized facilities for the computing facility to simplify the use of the terminal network. Access to these facilities for conventional batch or teleprocessing applications is provided through the Network System Interface (NSI).

This facility allows standard installation written routines in COBOL and ASSEMBLER access to some of the facilities of The Network Director. The Network System Interface is available to the application program that can utilize the host environment's CALL mechanism.

As an example, it is possible for conventional application systems to utilize The Network Director's Message facility to transfer (Send) messages to particular terminals or users, or to generate a command (Stack Command) that will eventually be executed on behalf of a terminal user. NSI provided facilities and application program usage of the Network System Interface is fully described in The Network Director's *Network User's Guide*.

The Network Director itself uses the NSI to communicate to other Network Directors that may exist at another location (SITE definition).

Network Security Facilities

One of the key functions provided by The Network Director is generalized **Network Security**. Network security is the act of insuring that the individual sitting at any given terminal is authorized to access the system, can use the device he is at, and determining what types of activities he can accomplish. The Network Director is a tool that can implement these requirements.

User Identification

Typically, Network Director installations concerned about network security issues configure The Network Director to prompt for user id and password prior to permitting access (DEFAULT IDENTIFICATION=YES). The Network Director will then compare these items with the appropriate USER and TERMINAL definitions to determine if the individual at the terminal is authorized to access the system and whether the terminal being utilized is authorized or not.

Once this validation is accomplished, The Network Director will then present the user with a panel that can be tailored to the individual or it can be a combination of what the user and the terminal are authorized for. This menu construction can be controlled by the installation by setting the SELECTIONS= operand to the desired value.

The user can receive a menu of all items she/he is authorized to have. If the terminal is also authorized for APPLICATIONS, the user can receive a menu consisting of his selections **plus** the TERMINAL's selections. Finally, and most secure, the user can be presented with a list of selections that only he and the terminal are **both** authorized for. This has the effect of restricting certain applications, like NetView, to certain individuals and only when they are at certain terminals.

Audit Facilities

While The Network Director is operating and controlling the the network, attempts to access the system are recorded by The Network Director in the LOG. An installation can also elect to record attempted signons in OS SMF, VM accounting records, or a sequential file (designated the SAR for System Accounting Record) to provide an independent audit trail of secure access.

A record is made of every successful LOGON and LOGOFF as well as any attempted LOGON. For failed LOGONs, the reason the attempt failed is also placed into the SMR (System Measurement Record) that is placed in OS SMF or the SAR (System Accounting Record).

Intruder Detection

ACF/VTAM itself does nothing to attempt to detect repeated efforts to connect to the network. The Network Director, when configured properly, will not allow access without accomplishing a sign on process. The Network Director also counts the number of consecutive unsuccessful logon attempts and will **disable** the ACF/VTAM terminal when an installation defined maximum is hit.

The Network Director does not break its session with the device, but it will no longer accept any input from the device. A Network Administrator must RELEASE the device

before it can be utilized again. This detection is intended to detect, report, and stop individuals that do not know the proper user id and password combinations. This can also be utilized to detect and stop individuals **dialing in** or **dynamically connecting** and simply trying repeatedly to access the computing facility.

System Security Packages

The Network Director is a logical Network Security product and has been positioned to service the security requirements of the ACF/VTAM network. In and of itself, The Network Director should be viewed only as a component of overall system security. The Network Director is an extension to the system security products currently on the market and will respond to the security product's presence as determined by the Configuration Parameters.

The majority of installations with a security product installed have packages from Sterling Software, Computer Associates, or IBM (VMSECURE, CA/SENTINEL, TOP-SECRET, ACF2 or RACF). The Network Director provides interfaces to each of these security products. The actual implementation with The Network Director and the extent that the interface controls The Network Director's activities is generally a function of the security packages characteristics. North Ridge Software, Inc. is committed to utilizing as many of the security package's facilities as possible.

ACF2/MVS

ACF2/MVS (Access Control Facility) and The Network Director in an OS operating environment offer the following features:

1. System Entry Validation (User Id/Password checking)
2. ACF2 checking of SOURCE (terminal name), and SHIFT parameters are supported
3. Ability for the terminal operator to specify a new password from The Network Director's panels
4. Support for Extended User Authentication (OIDCARDS, other authentication devices, etc.)
5. The Network Director operates as an ACF2 MUSASS via the SVCA interface. All messages that would appear during ACF2 entry validation can appear in the Message area of the Identification or Application Selection Panel.
6. Messages issued by ACF2 to a Network Director user are always placed in The Network Director's LOG
7. dynamic construction of the GROUP name from the ACF2 LOGONID or LIDREC
8. Application Selection Panel composition from logonid bit masks (FDE screening) or generalized resource rules
9. support for directory build operations
10. full support for mini-LID assignments
11. support for ACF2 *inherit* processing for cross-domain environments
12. account code validation against the contents of ACF2

ACF2/VM

ACF2/VM (Access Control Facility) and The Network Director in a VM (GCS) operating environment offer the following features:

1. System Entry Validation (User Id/Password checking)
2. ACF2 checking of SOURCE (terminal name), and SHIFT parameters are supported
3. Ability for the terminal operator to specify a new password from The Network Director's panels
4. The Network Director operates as an ACF2 SRFUSER via the SRF interface. All messages issued by ACF2 entry validation can appear in the Message area of the Identification or Application Selection Panel
5. Messages issued by ACF2 to a Network Director user are always placed in The Network Director's LOG
6. dynamic construction of the GROUP name from the ACF2 LOGONID or LIDREC

RACF/MVS

The Network Director uses the SAF (System Authorization Facility) to interface to IBM's RACF (Resource Control Facility). RACF 1.7 and above have the following basic features:⁶

1. User Id and Password checking via RACROUTE ENVIR=CREATE (RACINIT)
2. Support for the terminal source (originating terminal)
3. Ability for the terminal operator to specify a new password from The Network Director's panels
4. Display of the RACF Connect Group and User Name values
5. Dynamic assignment of the GROUP name from the Connect Group
6. Terminal users may specify RACF Connect Group at logon time
7. Application Selection Panel composition from Connect Group list associated with ACEE
8. Password expiration warning message support
9. full 31 bit support

⁶ RACF 1.9.2 and the support Secured Signon SPE is available via Network Director "PassTicket" support in SSI.

RACF/VM

The Network Director in GCS environments supports a DIAGNOSE level interface to RACF/VM that has the following characteristics:

1. User Id and Password validation
2. Dynamic assignment of the GROUP from the ACIGROUP statement specified in the VM Directory

TopSecret/MVS

The TopSecret/MVS interface utilizes the SAF (System Authorization Facility) via RACROUTE to interrogate TopSecret/MVS. The following features exist:

1. User Id and Password checking via RACROUTE ENVIR=CREATE
2. Support for the terminal source (originating terminal)
3. Ability for the terminal operator to specify a new password from The Network Director's panels
4. full 31 bit support
5. TOP-SECRET originated messages are displayed in The Network Director's LOG and appropriately reflected to the terminal operator
6. extraction of the TopSecret/MVS stored name from the user's ACID
7. Network Director GROUP establishment based upon TopSecret/MVS Department or Division assignment
8. Application Selection Panel menu contents generated via the contents of the TopSecret/MVS Facilities List associated with the user

TopSecret/VM

The Network Director interfaces with TopSecret/VM via DIAGNOSE X'A0' and X'08'. The following features are present:

1. User Id and Password validation
2. Ability for the terminal operator to specify a new password from The Network Director's panels
3. TopSecret/VM generated message displayed on The Network Director's panels and in the LOG
4. Display and support for the TopSecret/VM name, division, and department values
5. Dynamic GROUP assigned based on TopSecret/VM division or department assignments
6. Device inactivation for suspended ACID usage
7. Individual Application Selection Panel composition via TopSecret/VM resource validation

VM/SECURE

The Network Director in GCS environments supports a DIAGNOSE level interface and a CP SMSG interface to VM/SECURE offering with the following features:

1. User Id and Password validation via DIAGNOSE X'A0'
2. Dynamic assignment of the GROUP from the ACIGROUP statement specified in the VM Directory
3. New password specification
4. Last access notification
5. Storage, retrieval, and display of user's name and phone number
6. Expired password detection
7. Password expiration warning message

Event Recording

The Network Director provides an optional recording of events (called Event Recording) during its processing. This information can be utilized for generalized reporting, accounting, billing, and auditing purposes. These events are recorded in an appropriate location for the operating environment (e.g. OS SMF, VM ACCOUNT records, DOS SYSPCH, or an alternate sequential file) and can be processed after the network is no longer active. Consult the appropriate Installation manual for additional information about the Event Recording medium for your operating system.

The recording of each event is independent of the other. Available events are:

Name	Event
ADMINCMD	a Network Administrator has issued a command
APPLCNTS	a periodic measurement of how many network elements are in session with various applications
APPLSTAT	a defined APPLICATION has just changed status
LOGON	a network user has attempted to identify himself (successful or not)
LOGOFF	a network user has been logged off of The Network Director
INFOUPD	a network element just updated a portion of the Information File
MSGSEND	a message was just sent
MSGVIEW	a message was just viewed
MSGPRINT	a message was just printed
MSGDEL	a message was just deleted
RETURN	a network element has just returned from a subsystem
SELECT	a network element has just chosen a subsystem
VTAMERRS	a non zero return code was received on a ACF/VTAM operation

Figure 19. Available Events

Configuration Parameters

The following is a list of the major Configuration Parameters (network definitions) utilized within The Network Director to control it's actions and activities.

Command	Purpose
ACF2	establishes Network Director ACF2 Directory Build characteristics
APPLICATION	defines a ACF/VTAM application subsystem
BROADCAST	immediately transmit a message through the network
CANCEL	terminate an activity within The Network Director
CLOSE	de-activate the ACF/VTAM or VSAM ACB
DEFAULT	establishes processing default values
DELETE	remove a network definition from use
DIRECTORY	establish an individual entry in the System Directory
DISCONNECT	return a LU to ACF/VTAM
DISPLAY	general network reporting
DUMP	display main storage in hexadecimal format
GLOBALS	provides Operating System type default values
GROUP	defines a logical grouping of network users
HOLD	make a network element unavailable for usage
OPEN	activate the ACF/VTAM or VSAM ACB
PROFILE	establishes basic profile values for network users
RELEASE	make a network element available for usage
RELOAD	restore previously saved definitions from the External File
RESOURCE	create a generalized definition or template for subsequent reference
SAVE	stores network definition in the External File for subsequent RELOAD operations
SHOW	process network definitions in full screen mode
SIMLOGON	acquire a device from ACF/VTAM
SITE	define another computing facility
STOP	terminate Network Director execution
TERMINALS	defines characteristics to be used for one or more terminals
USERS	defines characteristics to be used for one or more users of the network

Figure 20. Available Commands

These commands make up the *language* utilized within the definition processes (Configuration Parameters or External File) and from a Network Administrator terminal to communicate with The Network Director and provide it operational instructions.

Summarization

The Network Director helps clarify which applications the terminal operator has available to him/her and provides a simple manner with which the operator can request the logical connection. The menus present the operator's choices in meaningful terms rather than cryptic eight byte identifications.

The Network Director provides full terminal security through the presentation of individualized Application Selection Panels. An operator may not request connection to a subsystem that is *unauthorized*. Interfaces to the standard system security packages are available as a standard portion of The Network Director.

The Network Director provides a comprehensive Message Switching facility that is independent of subsystem.

The Network Director can provide a *single system image* to the terminal operator which can reduce the apparent complexity of the Computing Facility with multiple subsystems.

The Network Director provides centralized management of the logical terminal network through the Network Administrator functions. The network may be monitored and modified while the network is "up". An extensive audit trail of activity is available as well as the ability to communicate directly with ACF/VTAM. Optionally, local SMF, VM ACCOUNT, or sequential records can be produced to provide an additional source for audit trail and monitoring.

The Network Director provides a mechanism to integrate batch and online processing routines with the facilities available within The Network Director through the Network System Interface.

In general, The Network Director provides an environment with which the computing facility can describe its physical network in a logical manner and then manipulate the logical network elements. The Network Director identifies the Logical Network as the resource that it will manage.

Implementations

The Network Director offers multiple facilities that can coexist with other facilities within a ACF/VTAM network of terminals. This section of the manual describes some of the implementations possible for The Network Director. It is important to note that The Network Director is simply one of the software components useful when configuring a flexible terminal network.

The Network Director is capable of contributing in many ways to the operation of the network. It can be a central network security tool, an operator productivity facility, a network monitor, etc. How it is used and configured is dependent upon each installation. Some facilities discussed may not be significant to all installations, but several topics are worthy of additional discussion.

Logical Application Independence

The Network Director can be configured to present a "logical view" of the network to the terminal operator. With this concept, the terminal operator does not need to be aware of the exact location of a specific application system. The following figure contains two different CICS systems, but the terminal operator accessing the Payable system may not be aware it is in CICS2. The Network Director's Application Selection Panel can simply say PAYABLE or something similar.

Location independence allows the computing facility to move application systems from one location to another without the need to retrain terminal operators. Their process of selecting the application remains the same, even if the PAYABLE application is subsequently moved back to CICS1.

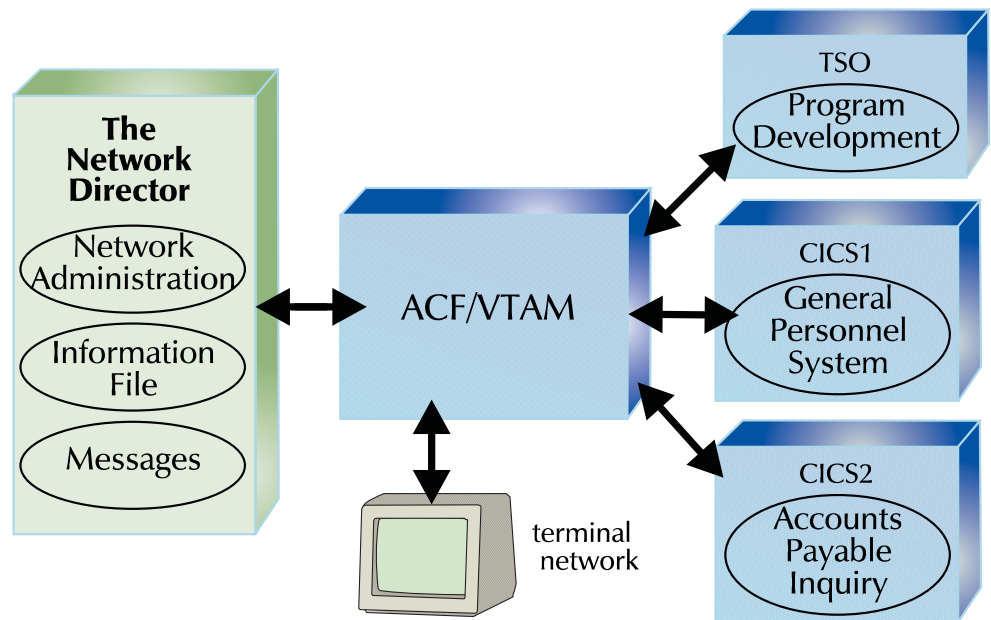


Figure 21. Logical Application Location

Note that the specific Applications are resident in different subsystems. The Network Director itself contains some *applications*. The intent is that the location of the application itself should be unimportant to the use of that application. The Accounts Payable Inquiry application should be capable of being moved to another CICS system (say CICS3 or even into CICS1) with no outward changes in the manner in which the end user accesses and uses the application system.

This implementation technique allows the computing facility to place applications together or to separate them for optimum performance without the need to retrain any operators that are accessing the application.

Multiple Network Directors

The Network Director's premise is that the terminal network is a shared and common resource to be shared and managed by a single computing facility. Often, this is not the case. The computing facility may support multiple independent and totally separate logical terminal networks. This is often the case at generalized computer service centers where multiple unrelated businesses are purchasing time and sharing the computing facility.

In this case, it is possible that a copy of The Network Director for each logical terminal network may offer a more consistent and cohesive control of the individual networks. The Network Director has no restrictions on the number of copies that can execute within a given computing facility.

As a logical extension to this discussion, there is nothing incorrect about making one of the copies of The Network Director an option on the other Network Director's Application Selection Panels. This relationship of logical networks may make sense for the Operations or Systems terminals in use to support the central computing facility. Naturally, the alternate Network Director selection is subject to all the security controls that any other application selection is.

The additional Network Directors will require only a unique ACF/VTAM APPLID within each domain with which to identify themselves to ACF/VTAM. Beyond this, all other normal rules enforced by The Network Director apply.

ACF/VTAM Multiple DOMAIN Configurations

Additionally, there is no reason that ACF/VTAM networks that span multiple DOMAINS (CPUs)⁷ cannot either share a single Network Director or run one or more copies of The Network Director in its DOMAIN. The Network Director interacts with ACF/VTAM as a standard application subsystem. This characteristic allows all aspects of the ACF/VTAM terminal environment to be active (MSNF, NPDA, NCCF, NetView, etc.) and allows the installation to make use of The Network Director's facilities exactly as it would any other ACF/VTAM subsystem.

The Network Director can also be used across *unlike* operating system environments. This becomes especially useful for large Cross Domain ACF/VTAM networks where the possibility of unlike operating systems is high. As large networks become interconnected via SNI (SNA Network Interconnect) utilizing ENA (Extended Network Addressing) this scenario becomes more and more frequent.

As an example:

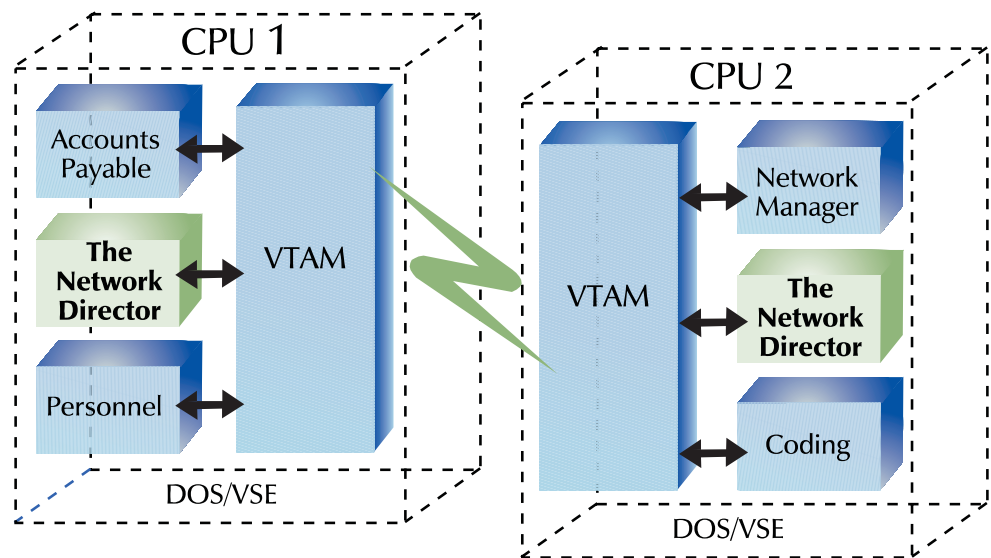


Figure 22. Multiple DOMAIN Implementation

The use of OS/MVS and DOS/VSE are only examples. VM/ESA, OS390, and/or GCS are also viable options.

In multiple Domain environments, The Network Director can be configured to communicate between the various copies of The Network Director. This includes automating the signon between the Network Director's (SSI=YES) as well as actual transmission via LU-LU sessions of any Messages generated by the Message Facility between defined SITES. Each Network Director is assigned a logical name (the SITE name), which can then be utilized by a terminal operator to refer to it.

⁷ This discussion also applies to properly configured usages of The Network Director in cross network (SNI) environments.

Summarization

The Network Director has been designed to allow almost any implementation that can assist in the management of the terminal network. The computing facility can choose to place all the terminals under the control of a single Network Director or divide up the terminal network into logical segments. A multiple CPU environment can be supported in exactly the same manner (a single or multiple Network Director's).

The Network Director has been designed to insure that the using installation has as much freedom in describing and using its logical network as possible.

Sample Configuration Parameters

The Network Director receives its configuration instructions through the Configuration Parameters or by RELOADing previously saved definitions (the SAVE and RELOAD commands allow all network definition maintenance to be done interactively). For purposes of discussion, this section of the manual will utilize the Configuration Parameters approach to providing configuration definitions.⁸

The parameters describe the logical network as it is to appear to The Network Director and identifies specific characteristics that individual components of the network are to have.

Overview

The following sample Configuration Parameters are a brief example of the parameters and how the information in the deck is interrelated. Detailed explanation of the individual parameters and their options is in The Network Director's *Network Administrator's Guide*.

The basic format for the Configuration Parameters consist of a statement identifier (TERMINAL, etc.) followed by one or more positional or keyword parameters. Statements may be continued by simply ending with a comma blank combination (", ") on a previous line. An asterisk (*) in column one indicates that the entire statement image is a comment. The Configuration Parameters should be in the following order:

1. APPLICATION definitions
2. DEFAULT assignments
3. GROUP identification
4. TERMINAL and USER definitions

⁸ The reader is reminded that all network definition can be done via usage of the online SHOW command, which presents all definitions as full screen formatted 3270 panels.

The Network Director processes the Configuration Parameters in the order that they are presented. Insofar as possible, The Network Director attempts to minimize any propagation of characteristics across parameter statements. This has been done to enable the Network Administrator to modify an individual logical definition later and have it take immediate effect on all terminals and/or users that have an implied relationship with the new definition.

```

*-----*
*   First, define all the APPLICATIONS in use   *
*-----*
APPLICATION  INFO,TARGET=TNDINFO,PFKEY=1,
              TITLE='Network Director Information'
APPLICATION  PERSONNEL,TARGET=CICS1,PFKEY=PF02,
              TITLE='General Personnel System'
APPLICATION  PAYABLE,TIME=(08:00-12:00,13:00-17:00),
              TARGET=CICS2,PFKEY=03,
              TITLE='Accounts Payable Inquiry'
APPLICATION  NETADMIN,TARGET=TNDADMIN,
              TITLE='Network Administration'
APPLICATION  CODING,TITLE='Program Development',
              TARGET=TSO,PFKEY=5
APPLICATION  MESSAGES,TARGET=TNDMSG,TITLE='Messages',PFKEY=12
*-----*
*   Second, set the DEFAULTS                   *
*-----*
              DEFAULT  COMMANDS=YES,LOGO=
                  AAAAA      DDDDDDD      CCCCCC
                  AAA  AAA      DDD  DDD      CCC  CCC
                  AAA  AAA      DDD  DDD      CCC
                  AAA  AAA      DDD  DDD      CCC
                  AAAAAAAA      DDD  DDD      CCC
                  AAA  AAA      DDD  DDD      CCC  CCC
                  AAA  AAA      DDDDDDD      CCCCCC
LOGO-END
*-----*
*   Third, identify the GROUPS                 *
*-----*
GROUP      PAYROLL,APPLICATIONS=( INFO, PAYABLE, PERSONNEL, MESSAGES) ,
           PASSWORD=PAYPASS,DAY=( MONDAY-FRIDAY)
*-----*
*   Last, list the TERMINALS and USERS         *
*-----*
TERMINAL   TM03,APPLICATIONS=( PERSONNEL, PAYABLE, CODING) ,
           TIME=(08:00-17:00)
TERMINALS  PY+++++,GROUP=PAYROLL
USER       SYSTEMS,PASSWORD=SECRET,
           APPLICATIONS=( INFO, CODING, NETADMIN, MESSAGES)
USERS      PAY+++++,GROUP=PAYROLL

```

Figure 23. Sample Configuration Parameters

Most of the parameter statements have either been discussed before in this document. However, a few comments about the sample are appropriate.

APPLICATION

Six applications have been defined. Notice that the PAYABLE application has been restricted to use between 8 am and 12 noon and between 1 pm and 5 pm. Be aware that this only controls whether a requesting terminal and/or user will be connected to the application by The Network Director. A terminal that was connected prior to 12 noon will not be disconnected automatically by The Network Director.

The Network Director's internal functions have been defined in exactly the same manner as are other typical applications. The applications INFO, NETADMIN, and MESSAGES represent The Network Director's internal applications.

DEFAULT

The DEFAULT statement lists those items that will apply to the entire network. In this example, the general system LOGO has been defined. As a default, all terminals will have the Command: line present on them (COMMANDS=YES).

The LOGO option allows the Network Administrator to define an installation specific LOGO to replace the internal Network Director default. For purposes of demonstration, ADC stands for "A Data Center". The LOGO begins on the next parameter image and will be capable of existing on the full 80 byte image. The LOGO definition will continue until the LOGO-END character string is encountered.

GROUP

This statement defines a logical GROUPing of terminals and/or Users that will have access to the specified APPLICATIONs in addition to the APPLICATIONs specified on the DEFAULT statement.

In order for a terminal operator to identify himself as a member of the PAYROLL GROUP, he must enter the password PAYPASS.

In addition, the PAYROLL GROUP will only be honored by The Network Director on the calendar days MONDAY through FRIDAY.

TERMINAL

The terminal with logical unit name TM03 will be able to access the three applications listed. Requests for terminal logical connection will only be honored by The Network Director between the hours of 8 am and 5 pm. Any other attempts will be considered security breaches and will be noted on the LOG.

The second TERMINAL statement (or TERMINALS in this case) demonstrates the method for collectively identifying terminals. Any terminal whose logical unit name begins with the string "PY" will be automatically a member of the GROUP named PAYROLL. No password will be required from these terminals to allow access. There is really no difference in the TERMINAL and TERMINALS specification in this example. TERMINAL is an acceptable abbreviation to The Network Director for the TERMINALS statement. This also applies to the USER and USERS statements following.

USER

The USER statement identifies a single user named SYSTEMS who has the authorization to access the INFO, MESSAGES, CODING, and NETADMIN applications. To establish a terminal as having the User named SYSTEMS, the operator must know the password SECRET.

The USERS definition for PAY+++++ defines a pattern of user ids that all start with the letters PAY as members of the GROUP PAYROLL. In order to logon as a user starting with the letters PAY, the terminal operator must know the password PAYPASS. This usage of the wild character "+" allows many installations to define a large portion of their user community with a few USER statements.

The following figure represents the panel that will appear on any terminal with a logical unit name starting with the letters "PY".



Figure 24. Sample PAYROLL Group Panel

Summarization

The Network Director's definitions provide an extremely flexible manner with which to describe the terminal environment. Remember that any of these definitions may also be entered online, SAVED and RELOADED through any authorized Network Administrator terminal.

Careful planning is required to properly configure the network in general. Once this is done, setting up The Network Director's Configuration Parameters is a straight forward process.

Technical Characteristics

The Network Director's technical implementation characteristics are generally discussed in this section. A detailed explanation is available in The Network Director's Internals manual. This section of this manual will provide only the major characteristics.

The Network Director is written completely in IBM System 370 ASSEMBLER code. The code is fully reentrant and internally organized into multiple functional CSECTs. Standard 370 ASSEMBLER techniques are used to transfer control from one CSECT to another. The CSECTs themselves are combined by the standard operating system LINKAGE EDITOR so that there is no loading of functional modules at execution time (an exception to this general rule is that the optional user exits may be dynamically loaded by The Network Director).

The Network Director will operate in native 31 bit addressing mode on capable processors. 24 bit addressing operations are utilized only for those access methods (QSAM) and system components (ACF2, OPEN, CLOSE, etc.) that may require it.

The Network Director executes in problem program state and requires **no authorization** of any type. If your installation wishes to make use of certain extended facilities (the VM command, OS SMF recording, the RACF interface, or SWAP=NO processing) then authorization will have to be provided to The Network Director.⁹ However, this requirement is the requirement of the extended facility and not directly The Network Director. The authorization technique necessary is a function of the Operating System The Network Director is functioning in. See the *Installation* manual for more information.

The Network Director uses no SVCs of its own.

The Network Director makes use of the documented ACF/VTAM Application Program Interface and the Program Operator interface to accomplish all communications with ACF/VTAM. Only ACF/VTAM Record mode devices are supported. This includes SNA and non-SNA implementations of LU0, LU1, LU2, and LU3 devices and any device (PC, etc.) emulating one of the above via protocol conversion, hardware board, etc.

The Network Director may run as an independent job in the operating system (as a partition, address space, or virtual machine) or may be subtasked within the environments that support it. Note that subtasking may require the effective disabling of The Network Director's operator interface. In this case, operator communications may still occur through the provided Network Administrator interface.

When The Network Director is required to provide code that will run under another subsystem's control, the provided code makes every attempt to take advantage of vendor provided exits made available within that software component. (e.g. IKJEFLD1

⁹ This applies primarily to APF authorization for MVS installations. GCS authorization requirements are discussed in the Installation Guide.

TSO preprompt exit to accomplish the *single system image* concept for TSO/E installations).

The Network Director itself provides several standardized exits available to the computing facility to further extend or check those activities that The Network Director is involved in.

The Network Director uses the standard facilities for communicating with the operating system's operators. That is, OS STOP/MODIFY, GCS WTOR, and the DOS MSG facility.

The Network Director has a specialized internal management routine to manage all storage GETMAINed or GETVISed. The usage of this storage is optimized by The Network Director to minimize the acquisition of storage after initialization has completed. This *quick cell* approach significantly reduces the number of calls to operating system service routines required to acquire and release main storage and the various ACF/VTAM and VSAM control blocks.

The Network Director will use disk queueing techniques to maintain messages that require guaranteed delivery. When disk queueing is in effect, The Network Director uses the VSAM access method (KSDS) to store the information.

The Network Director supports the 3270 family of ACF/VTAM RECORD mode devices (all communications protocols are supported for these devices) and a wide variety of LU1 or line at a time devices via NTO or commonly available protocol convertors.

The Network Director requires no "hooks" or exits from ACF/VTAM itself. The terminals are directed to The Network Director through the standard LOGAPPL parameter in the ACF/VTAM definition parameters or through queued SIMLOGONs within The Network Director itself and specified in the Configuration Parameters.

The Network Director provides several standard exit points in its processing that allow specific installation requirements to extend or monitor the function of The Network Director's environment. These exits are fully documented in The Network Director's Internals manual.

The Network Director utilizes the VTAM CLSDST function with the PASS OPTCD to forward terminals to the subsystems. Thus, The Network Director is not involved in terminal transmissions between the subsystem and the device. Once the device terminates its session with the subsystem, it will be returned to The Network Director and will receive a panel, as appropriate.

The Network Director supports all releases of ACF/VTAM and currently is operating with Releases 1.3, 2.1, 2.2, 3.0, 3.1, 4.1, 4.2, 4.3, and 4.4.¹⁰ The Network Director currently supports all releases of MVS (including MVS/ESA and OS/390), DOS/VSE, and VM/GCS (including VM/ESA) implementations capable of supporting ACF/VTAM.

The Network Director's facilities are available to networks configured utilizing ENA (Extended Network Addressing) as well as SNI (SNA Network Interconnect) concepts.

¹⁰ This list is complete as of the date of publication for this manual. It does not imply that The Network Director will not operate with releases not yet shipped by IBM, but only that validation with the listed releases has been done at the time of publication.

Storage Estimates

The Network Director typically executes within its own virtual address space or partition. The required virtual machine size, address space or partition is a function of the size of the logical network, the number of active physical terminals, and the types of activities anticipated within the network.

As a general rule, the following virtual storage estimates apply:

Executable code	500K
Fixed overhead.	160K
LOG Buffer.	16K
for each TERMINAL definition.	120 bytes
for each USER definition.	120 bytes
for each APPLICATION definition	100 bytes
for each GROUP definition	90 bytes
for each Active Network Element	750 bytes
for each selection active	16 bytes

Figure 25. Storage Estimates

These values can be utilized to compute an estimate of the amount of virtual storage required by The Network Director to support your logical network.

If The Network Director is operating in 31 bit addressing mode, approximately 90% of the storage is located above the 16M addressing line. The executable code (load module), DCBs, register save areas, ACF2 control blocks, and sequential input/output buffers remain allocated below the line in 24 bit addressable storage.

Experience has shown that the majority of the virtual storage is consumed simply handling the 750 byte increments associated with the Active Network Elements. Thus, you can roughly compute your requirements by adding the fixed storage estimate and 750 bytes for each LU you anticipate being managed by The Network Director during the course of normal processing. To this, add the overhead required for each device that will have a Application Selection Panel (figure about 100 bytes) on it.

A typical 1000 terminal logical network will take slightly more than 1.5 megabytes of virtual storage to manage. See the Internals Manual for additional information about computing actual storage requirements. These estimates do not include any storage requirements that your security package (ACF2, RACF, TOP-SECRET) may have and do not include VTAM requirements over and above the basic control blocks that are allocated by The Network Director (RPLs, NIBs, etc.).

Working Set Characteristics

The Network Director attempts to package the various control block chains it references onto the same virtual pages. This is an attempt to reduce paging activity associated with processing typical tasks.

The Network Director's Working Set is normally about 30% of the total virtual storage allocated. The 1000 terminal network will typically result in a working set of 215K during normal activity. Low or high amounts of activity may result in lower or higher working sets. Higher activity will definitely occur when The Network Director is initializing or an application subsystem terminates and terminals are returned to The Network Director's control.

Glossary

ACF2: the Access Control Facility - one of Computer Associates security systems

ACF/TCAM: Advanced Communications Facility - TeleCommunications Access Method

ACF/VTAM: Advanced Communications Facility - Virtual Telecommunications Access Method

action bar: the area at the top of a panel that contains keywords identifying actions available from the displayed panel

address space: the area within the operating environment that contains a piece of work (typically a job) for the operating system

application: identifies a collection of programs, files, and processes that make up a data processing system. Inventory, Payroll, etc. are examples of applications

APPLICATION: a Network Director statement that identifies a logical application

Application Program Interface: the documented method for interfacing to the ACF Program Products

Application Selection Panel: The Network Director's name for the panel that allows the terminal operator to select an application to be logically connected to

APPLID: the one to eight byte character string that uniquely identifies an ACF/VTAM using subsystem to ACF/VTAM

ASSEMBLER: the operating system program that will convert assembler level source code into object code

ASYNC: an acronym for the asynchronous communications protocol between the CPU and asynchronous terminals

BI-SYNC: acronym for the binary synchronous communications protocol

broadcast: a short message that is immediately sent to all terminals and/or operators connected to The Network Director

BROADCAST: a Network Director command that generates an immediate one line message to its destination

BTAM: Basic Telecommunications Access Method

CANCEL: a Network Director command that can terminate internal work elements within The Network Director

CICS: Customer Information Control System (IBM's teleprocessing system)

CLOSE: a Network Director command that makes the ACF/VTAM or VSAM ACB unavailable to The Network Director

CMS: Conversational Monitor System - the programming component of IBM's VM operating system

computing facility: the combination of hardware, software, and personnel that provide the automated environment for data processing tasks

Configuration Parameters: The Network Director's control statements

CPU: the Central Processing Unit

cross domain: a term used to describe an interconnection between two VTAM processing environments

CSECT: an ASSEMBLER Control SECTION

CUA: Common User Access, a portion of Systems Application Architecture that defines and describes the user interface to the computing system

DELETE: a Network Director command that eliminates one or more control blocks from within The Network Director's environment

DISPLAY: The Network Director's statement invoking general reporting and query facilities

DASD: Direct Access Storage Device (also referred to as *disk*)

DISCONNECT: a Network Director statement that breaks the session between The Network Director and a identified device

DOMAIN: an ACF/VTAM term to define a logical sphere of influence within the computing facility

DOS: IBM's Disk Operating System

DUMP: a Network Director statement that allows a Network Administrator to display the hexadecimal contents of main storage (virtual addresses only)

ENA: Extended Network Addressing - the facility within IBM's networks that allows for 24 bit addressing of terminals and ACF/VTAM domains

EXCP: EXecute Channel Program - typically used to identify a *low* level of programming I/O devices

gateway: the "*portal" into an SNA network other SNA network terminals (connected via SNI) will pass

GCS: Group Control System - a portion of VM/370 that provides an environment supporting ACF/VTAM in the VM operating environment

GETMAIN: an OS MACRO used to acquire virtual storage

GETVIS: the DOS MACRO used to acquire virtual storage

GLOBALS: a Network Director statement that identifies key operating environment characteristics

GROUP: The Network Director's term to identify multiple terminals and/or users

HOLD: The Network Director's statement to remove an item from availability in the network

ICCF: IBM's programming facility for DOS/VSE environments

IDMS/DC: a teleprocessing system from Computer Associates

IMS: the Information Management System (IBM's data base management system)

KSDS: Key Sequenced Data Set - a VSAM term to identify the characteristics a particular VSAM file has

Linkage Editor: the Operating System program that will process one or more object modules (DOS Relo) and produce a single executable load module (DOS Core Image)

LOG: The Network Director's term for the audit trail of all activity that has occurred

LOGO: describes the identifying information placed by The Network Director at the top of the non CUA Application Selection Panel

LOGON: the act of identifying yourself to the computing facility

logical connection: describes the path from the physical unit (terminal) to the subsystem currently processing the terminal's requests

memo: The Network Director's term for a fairly lengthy message

message: identifies information that the terminal operator would like transferred somewhere

Messages Menu: The Network Director's primary vehicle for interacting with the user for purposes of using the message facility

message facility: The Network Director's internal application that is capable of managing messages within the network

MODEL204: the data base manager and teleprocessing system provided by CCA (Computer Corporation of America)

MVS: Multiple Virtual Storage, or OS/MVS, is an IBM operating system

NCP: the Network Control Program manages the 370x transmission control units

NETSOL: NETwork SOLicitor - used by early versions of ACF/VTAM

network: describes the combination of hardware and software that enables a user to utilize the computing facility via terminals

network element: identifies an active user of The Network Director. The network element can be a User or a Terminal within the logical network.

Network Administrator: an individual responsible for the maintenance and reliability of the network

NSI: The Network Director's Network System Interface. A facility that allows communication with The Network Director from other than a terminal (batch or online programs).

note: The Network Director's term for a short message

NTO: the Network Terminal Option

OPEN: The Network Director's statement to activate on of the external ACBs (ACF/VTAM or VSAM)

OS: IBM's Operating System

partition: the area within DOS or early OS systems available to run jobs. Similar to an MVS' address space

panel: an arrangement of information grouped together for presentation to a terminal user on a physical device

password: the normally secret 1 to 8 byte code that is used with the User Id to identify that the proper individual is using the User Id

PFKEYs: the 3270's Program Function keys

PROFILE: The Network Director's statement establishing the initial values for a network profile

profile: contains operator specific defaults used by The Network Director to manage the operator's session

protocol converter: a hardware unit commonly used to convert incoming ASCII data streams to 3270 data streams suitable for usage by ACF/VTAM and the subsystems

pull down: an extension of the action bar that displays a list of choices available for a selected action bar choice

RACF: Resource Access and Control Facility - IBM's security package

RELEASE: The Network Director's statement to allow a network element to be made available for use

ROSCOE: the programming environment available from Computer Associates

SDLC: Synchronous Data Link Control - a terminal communications protocol

signon: the process of identifying oneself to the computing facility. Same as LOGON.

SIMLOGON: the ACF/VTAM MACRO used by a ACF/VTAM subsystem to indicate that it wants to obtain a session with a LU

single system image: identifies The Network Director's goal of presenting the end user with a singular view of the computing facility

SITE: another computing facility also operating The Network Director and described by the name associated with the SITE statement

SNA: Systems Network Architecture - a comprehensive approach to the total network

SNI: SNA Network Interconnect - a method to connect individual SNA networks to each other via a gateway

STOP: The Network Director's statement that terminates the execution of The Network Director

subsystem: the term used to identify the host environments for applications

SVC: SuperVisor Call

teleprocessing: the combination of the network and one or more subsystems that allows applications to be performed in a realtime manner

teleprocessing systems: the software subsystems that allow applications to take on realtime characteristics

TERMINAL: The Network Director's statement setting additional processing characteristics associated with one or more network devices.

terminal id: the character string that uniquely identifies a terminal within the network. The ACF/VTAM LU name.

The Network Director: the software component that simplifies the terminal operator's access to the computing facility, while providing additional network security and functions

timesharing: the process of dividing the use of the CPU between multiple terminal users

TOP-SECRET: a security system from Computer Associates

UCC7: the job scheduling package from Computer Associates

user: the individual using the terminal to accomplish job related tasks

USER: The Network Director's statement identifying one or more user ids and the characteristics associated with them

user id: the 1 to 8 byte character string assigned by the computing facility to identify the user

USS: ACF/VTAM's Unformatted System Services

VM: a Network Administrator command that enables the issuing of VM commands via DIAGNOSE X'08' to the virtual machine that is the host for The Network Director

VM/370: Virtual Machine/370 - an operating system to run multiple virtual CPUs in a single CPU

VSAM: Virtual Storage Access Method

VS1: Virtual Storage 1 - an OS operating system

VSE: Virtual Storage Extended - an acronym commonly used to reference recent releases of DOS

VTAM: the Virtual Telecommunications Access Method. Also, a Network Administrator command that allows the issuing of VTAM operator commands from the Network Administrator panel

window: an area of the physical screen with visible boundaries through which a panel or a portion of a panel is displayed

WTO: Write to Operator - the mechanism used in an OS system to display information on the operator's console

3270: a generic term used to describe the family of full screen devices that are commonly in use as network terminals

3271/4: terminal control units for 3270 type devices

370x: the IBM Transmission Control Unit

Index

/RCL 40
@CFDE 46
@MUSASS 46

3

3270
 defined 70
3270 models 22, 29
3271
 defined 70
3274
 defined 70
3290 22, 29
370x 8
 defined 70
37x5 8

A

Accessor Id 48
account code validation 46
accounting 45
ACEE 47
ACF/VTAM 17
 defined 67
ACF2 24, 31
 defined 67
ACF2 directory build 46
ACF2/MVS 46
ACF2/VM 47
ACID 48
ACIGROUP 48, 49
ACQUIRE 15
action bar
 defined 67
action codes 35
address space 16
 defined 67
API

 defined 67
application 17, 21, 28, 59
 defined 67
application command selection 22, 29
application program interface 9
Application Selection Panel 20, 27
 defined 67
APPLID
 defined 67
ASSEMBLER
 defined 67
ASYNC 8
 defined 67
audit
 DOS 45
 OS 45
audit trail 45
automated sign on 38
automatic update 23, 30

B

BI-SYNC 8
 defined 67
broadcast 34
 defined 67
BTAM 7
 defined 67
bulletin board 37
BYSYNC 8

C

CANCEL
 defined 67
changing network definitions 42
CICS 6, 14
 defined 67
CLOSE
 defined 67

CLSDST 64
CLSDST PASS 15
CMS 6
 defined 67
command line 40
command line commands 40
commands 40
communication between Directors 44
Computer Associates 46, 47, 48
computing facility 17
 defined 67
Configuration Parameters
 defined 67
 options 56
 sample 21, 28, 60
connect group 47
controlling access 46
CP commands 39
CPU
 defined 67
cross domain 56
 defined 67
CSECT
 defined 67
CSSF 40
CSSN 14
CUA 13
 defined 68
cursor selection 22, 29

D

DASD
 defined 68
DEFAULT 21, 23, 27, 30, 59
defining a GROUP 61
defining a TERMINAL 61
defining a USER 62
defining an APPLICATION 61
DELETE
 defined 68
detecting intruders 45
DIAGNOSE 43, 48
dial up protection 45
disable 45
DISCONNECT
 defined 68
DISPLAY
 defined 68
documentation 2
DOMAIN 8, 56
 defined 68
DOS 16

 defined 68
DOS SYSPCH 50
DOSVSE 56
DUMP
 defined 68
dynamic network definitions 42
dynamic status update 23, 30

E

electronic mail 34
ENA 56
 defined 68
estimating storage 65
event recording 50
EXCP 7
 defined 68
external file 37

F

facilities list 48
FAX ii
FDE 46

G

Gateway
 defined 68
GCS 39, 47, 48, 56
 defined 68
GETMAIN 64
 defined 68
GETVIS 64
 defined 68
GLOBALS
 defined 68
GROUP 59
 defined 68

H

hackers 45
HELP 37
help facility 37
HOLD
 defined 68
homepage ii

I

IBM 47
ICCF 6
 defined 68
IDENTIFICATION 45
IDMS/DC 6
 defined 68
implied pfkey selection 22
IMS 6
 defined 68
inactive list 42, 45
INFO 37
information file 37
inherit 46
InterNet address ii
intruders 45

K

KSDS 64
 defined 68

L

LIDREC 46, 47
light pen selection 22, 29
linkage editor
 defined 68
location independence 54
LOG file 24, 31, 42
 defined 68
LOGAPPL 15, 64
logging on 24, 31
logical application 54
logical connection 11, 13, 17
 defined 68
LOGO 21, 61
 defined 68
LOGOFF 40
logon 12, 14
 defined 68
LOGONID 46, 47
LU
 defined 69
LU6 44, 56

M

making a choice 22, 29
manual set 2
memo 34
 defined 68
menu 20
menu processing 22, 29
message
 defined 68
Message Facility
 actions 35
 defined 68
 definition 34
Messages Menu
 defined 68
mini-LID 46
MLID 46
MODEL204
 defined 68
modified field selection 22
MSG 64
multiple Domain 56
MUSASS 46
MVS 16, 56
 defined 68

N

NCP 8
 defined 68
NETSOL 11, 15
 defined 68
NetView 6
network
 defined 68
Network Administrator 17, 39, 40
 defined 69
Network Control Program 8
network element
 defined 68
network information file 37
network security 45
Network System Interface 44
 defined 69
note 34
 defined 69
NSI 44
 defined 69
NTO
 defined 69

O

OIDCARD 46
OPEN
 defined 69
operating systems 64
OPTCD=PASS 64
options 33
OS
 defined 69
OS390 56

P

panel
 defined 69
panels
 basic selection 20, 27
 identification 24, 31
 network administration 41
 Network Administrator 39
 selection example 62
parameters
 definition 19
partition 16
 defined 67
password 17, 25, 38
 defined 69
password checking 45
PF keys
 defined 69
pfkey selection 22, 29
primary menu 20
profile 26
 defined 69
program operator 39, 43
protecting dial up devices 45
protocol converter 45
 defined 69
protocol convertors 45
pull down
 defined 69
PUT 42

R

RACF 24, 31, 47
 defined 69
RACF/VM 48
RACINIT 47, 48
RACROUTE 47
RELEASE
 defined 69
RESET 40
restricting applications 45
ROSCOE
 defined 69

S

SAA 13
SAF 47, 48
SAR 45
SDLC 8
 defined 69
security packages 46
selection panel 20, 27
selection techniques 22, 29
SELECTIONS 45
setting defaults 61
shortcomings 11
SHOW 59
sign on 12, 14
signing on 24, 31
signon
 defined 69
SIMLOGON
 defined 69
single system image 38
 defined 69
SITE 44, 56
 defined 69
SMF 45, 50
SNA 8
 defined 69
SNI 56
 defined 69
SRFUSER 47
status 23, 29
status area 23
status update 23, 30
STOP
 defined 69
STOP-MODIFY 64
storage allocations 65
storage estimates 65

- subsystem 6, 18, 38
 - defined 69
- supported operating systems 64
- supported terminals 22, 29
- supported VTAM releases 64
- SVC 63
 - defined 69
- SVCA 46
- SYSPCH 50
- system entry 46, 47

T

- target application 18
- TCAM 7
 - defined 67
- teleprocessing
 - defined 69
- terminal 18, 20, 21, 27, 28, 59
 - defined 69
- terminal access methods 7
- terminal host connection 9
- terminal id
 - defined 69
- The Network Director 13
 - defined 69
- timesharing
 - defined 69
- TOP-SECRET 48
 - defined 70
- TopSecret/VM 48
- TRIES 45
- TSO 6, 38

U

- UCC7 6
 - defined 70
- Unformatted Services 11
- user 18, 20, 27, 59
 - defined 70

- user authentication 46
- user id 18, 24, 31, 38
 - defined 70
- USS 11, 13
 - defined 70
- USSMSG10 11

V

- VCNA 56
- virtual machine 16
- VM 16, 48, 49, 56
 - defined 70
- VM accounting 45
- VM accounting records 50
- VM commands 39
- VM/SECURE 49
- VM370
 - defined 70
- VS1
 - defined 70
- VSAM 64
 - defined 70
- VSAM file 37
- VSE
 - defined 70
- VTAM 7
 - defined 70
- VTAM releases 64

W

- window
 - defined 70
- workstation 18
- WTO 42
 - defined 70