NETWORK ADMINISTRATOR'S GUIDE

Document Number TND-0203-10

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.

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

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

List of Illustrations

Introduction

The Network Director's *Network Administrator's Guide* is intended to be utilized by the individual responsible for the configuration, tailoring, and maintenance of The Network Director and its associated terminal network.

This manual provides information that is Operating Environment independent and applies equally to all environments that The Network Director is operating in. Reference the *Network Operator's Guide* for information about the operation of The Network Director and the *Installation Guide* for operating system dependent information.

Section Overviews

"Configuration Parameters" on page 3 contains all the information necessary to configure The Network Director's various facilities. The various configuration options that control The Network Director's execution are discussed in detail and each of its subparameters is described.

The individual assigned the duties of the Network Administrator will be most interested in "Network Administration" on page 145. This section of the manual is concerned with the utilization of and interaction with The Network Director after it has initialized and is executing as a portion of the terminal network.

"INFO Facility" on page 225 discusses the INFO mechanism, how to manipulate it, and how to extend the contents of the Information Facility.

"Operational Issues" on page 237 generally discusses issues related to The Network Director that are of an operational nature, but not related to a specific operating environment. Specific operating environment issues are discussed in the installation and operations manual.

Finally, a Glossary of Terms and a manual Index are included to aid the reader in the use of this manual.

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.

Configuration Parameters

The Network Director accepts its execution time parameters from a single input source called the **Configuration Parameters** and/or previously saved records on the External File. The Configuration Parameters consist of 80 byte record images containing positional and keyword parameters and the saved records consist of compressed strings representing a single definition entity (control block). Regardless of the form the configuration parameters take, they dictate The Network Director's view of the network.

This section of the manual describes the individual configuration parameters and how they may be used to configure and manage The Network Director's network.

Configuration Definition Notation

Configuration definitions and individual option settings can be accomplished via the full screen SHOW processor or via keyword syntax in the Configuration Parameters. The SHOW processor utilizes standard 3270 field mapping to associate values with the configuration option. The Configuration Parameters utilize positional and keyword approaches to establishing configuration values.[1]

All of the notation used in the remainder of the manual associated with the configuration parameters follows these general rules:

Keywords

Any words or operands shown in CAPITAL letters must be entered exactly as shown. These are typically keywords and The Network Director will be scanning the Configuration Parameters looking for these words or operands. A keyword is any text string that is associated with a statement and is terminated by a equal (=) sign.

```
TARGET=
```

[1] The syntax rules for keywords, keyword values, brackets, lists, and ellipsis apply primarily to the Configuration Parameters. The SHOW processor provides these items as a fundamental portion of the formatted panel. See the *Network Operator's Guide* for additional information on the SHOW command.

Keyword Values

Words or operand targets shown in lowercase letters represent variables for which specific information should be substituted as appropriate.

```
TARGET=applid
```

Brackets

Any phrases or parameters shown in square brackets ([ ]) are optional and do not have to be specified. If you choose to use the particular operand or phrase, do not code the brackets.

```
[ TIME=(start-end)]
```

Lists

When a parameter provides a list of choices, the choices will be enclosed with braces ("{" and "}") and separated by the character "|". You should choose only one item in the list.

```
OPSYS={VS1|MVS|DOSVSE}
```

Ellipsis

An ellipsis (...) indicates that the preceding item or group may be repeated. If not otherwise stated, the maximum number if items that may be specified is 255.

```
APPLICATIONS=(application name 1, ...)
```

Punctuation

All punctuation (except square brackets) such as commas, equal signs, dashes, colons, parenthesis, and quotes must be included in the parameter statement.

```
TIME=(08:00-13:30)
```

Alpha Value

The term *alpha value* is used to indicate a alphanumeric string of characters. The string may not contain special characters or blanks unless it is enclosed in single quotes. The length of all alpha values is eight bytes or less unless otherwise specified in the detailed description of the operand. All input text will be translated to upper case unless it is enclosed in single quotes.

```
PASSWORD='B@DAYS'
EXTENSION=TEST
```

Time Specification

The term *time specification* is used to reference a time of day range in the format h1:m1-h2:m2, where h represents the hour of day (00 to 24) and m represents the minute of the hour (00 to 59). Additionally, the first specification in the range must always be an earlier time than the second time. An hour specification of 24:00 is basically equivalent to 00:00.

```
TIME=(08:30-11:59)
```

When there are multiple TIMES specified associated with a single definition statement, the TIMES are logically processed as a boolean *or* condition (if any of the TIMES are valid, then the definition is proper to use). The TIMES operand is logically processed as a boolean *and* condition with the DAYS operand.

Numeric Values

The term *numeric value* indicates a simple decimal number. It can optionally be suffixed with a M (Minutes), S (Seconds), H (Hours), K (1024 increments), or D (Days). The Network Director will convert the specification to the appropriate scale.

```
TIMEOUT=5M is the same as TIMEOUT=300
```

Day Specification

The term *day specification* is used to represent a day of the week specification or range of days in the format DAY=(d1-d2), where d1 and d2 are EBCDIC representations for the various days of the week. SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, and SATURDAY are valid values.

```
DAY=(MONDAY-FRIDAY)
```

When there are multiple DAYS specified associated with a single definition statement, the DAYS are logically processed as a boolean *or* condition (if any of the DAYS are valid, then the definition is proper to use). The DAYS operand is logically processed as a boolean *and* condition with the TIMES operand.

Parameter Statements

The Configuration Parameters are made up of one or more Parameter Statements. Each Parameter Statement is made up of a Parameter Statement Identifier, Parameter Operands, and optionally a Parameter Name. The Parameters may be coded in columns 1 to 72 of each Configuration Parameter record image (the LOGO operand is the only exception to this and is coded in columns 1 to 80).

Each Parameter Statement is in the general form:

```
Statement Identifier  Name,Operand=value, ...
```

The Statement Identifier is the text token that identifies the Statement and may begin in or after position 1. It is delimited by one or more blanks. The valid values for the Statement Identifier are described later in this section. The term used as the Statement Identifier is normally interchangeable with the entire Parameter Statement. A reference to the *USER Statement* is a reference to the Parameter Statement whose Statement Identifier is USER.

The Parameter Name is optional for some statements and, if present, must be present as a positional parameter on the statement. It must be a unique value within Statement Identifiers of its own type. Additionally, it is wise to make all network entities unique names within the entire logical network definition.

The Parameter Operands are separated from the Statement Identifier by one or more blanks and may not begin prior to column 2 on any continuation record image. Valid Parameter Operands are dictated by which of the Statement Identifiers that has been used immediately prior to the Parameter Operand.

Parameter Continuation

Continuation of a Parameter Statement to a following record image is achieved at any location that a comma will naturally occur. Simply specify a comma-blank (", ") combination to cause The Network Director to look for more Parameter Operands on the next record.

The Network Director will automatically bypass any leading spaces in a Parameter Statement up to the first non blank character. This characteristic allows the use of indentation to make the Configuration Parameters more readable.

The Network Director will complete the processing associated with a statement when a Parameter Statement does not end with the comma-blank combination.

Additional information on the Parameter Statement after a termination blank is dealt with as comments by The Network Director.

Configuration Parameter Comments

Any Parameter Statement that begins with an asterisk ("*") will be considered a comment statement by The Network Director and will simply be printed on the output print file. Comment records may be placed anywhere within the Configuration Parameters (the LOGO operand is an exception to this rule).

Any characters on a Parameter Statement record beyond the continuation sequence (comma-blank) will also be considered comments.

Parameter Name

The Parameter Name is the logical identity that is to be assigned to a given Network Director entity. This name will be be used within The Network Director's definitions to identify network elements. It should be assigned a logical name to simplify usage within the definition statements.

Several of the Parameter Statements will reference *application name*. This is a reference to the Parameter Name that has been associated with the APPLICATION Parameter Statement that you desire. The Parameter Name is the character string that allows The Network Director's Parameter Statements to be interrelated.

Each network element Parameter Name must be unique within Statements of its own type. For example, each TERMINAL statement must have its own unique TERMINAL name. Additionally, manipulating the logical network later can be simplified by uniquely naming all network elements.

Parameter Abbreviations

The Network Director utilizes a standard mechanism to parse all Parameter Statements regardless of their origin (TNDPARMS, SYSIPT, a Network Administrator's terminal, or the Operator's Console). This mechanism allows you to abbreviate any Statement Identifier or Statement Operand to the smallest number of characters necessary to uniquely identify the Identifier or Operand.

Thus, the following expressions are identical in function:

Full Statement	Abbreviation
APPLICATION PFKEY=PF09	A P=9 APPL PF=9 APPLIC PFK=9
DEFAULT IDENTIFICATION=YES	DE IDENT=Y DEF ID=YES DEFAUL IDENT=Y
HOLD APPLICATION=TNDINFO	H A=TNDINFO HO APPL=TNDINFO
DISPLAY COUNTS	D C DISP CO
RELEASE NETWORK-ELEMENT=TM03	R N=TM03 REL NET=TM03

Figure 2. Parameter Abbreviations

Care should be exercised when using the abbreviations so that you obtain the exact results required. The abbreviation mechanism allows you to enter as many characters as you would like (up to the maximum of the Identifier or Operand). Generally, you should enter the minimum required for you to adequately identify the value you are entering.

Where there are clashes amongst the Identifiers or Operands, The Network Director has specified a minimum number of characters that must be entered to match the keyword. An example is the TERMINAL USER and USERS operands. You must enter the full five characters USERS to satisfy this operand match. U will match the USER operand and **not** the USERS operand.

Each of the following discussions of the individual definition items will underscore the minimum characters required to specify the statement if the number of characters required is greater than one.

Statement Identifier Summary

The following figure contains an alphabetical list of the available Statement Identifiers and the general function that each performs.

Statement Identifier	Usage
ACF2	Establish the rule processing characteristics for The Network Director when operating in an ACF2/MVS environment
APPLICATION	Identify a logical application subsystem
DEFAULT	Establish characteristics for all the terminals and users
DIRECTORY	Associate System Directory information with an individual user
GLOBALS	Set operating characteristics for The Network Director
GROUP	Identify a identity within The Network Director that may be used by multiple network users
KEYS	Establish keyboard mapping for LU1 type devices
PROFILE	Establish a Profile and associated values
RESOURCE	Identify a generalized item that will be utilized within The Network Director to simplify definition procedures
SITE	Define an installation connected to this installation that is also operating a Network Director
TERMINALS	Define a specific terminal (or set of terminals) and its (their) operating characteristics
USERS	Define the operating characteristics for a specific user (or set of users) and their operating characteristics

Figure 3. Statement Identifiers

Each of these Statement Identifiers, as well as available operands, is discussed in more detail in the rest of this manual.

Operand Sequence

Parameter Operands may be specified in any order within the Parameter Statements associated with a particular Parameter Statement. Multiple Parameter Operands may be specified on a single Parameter Statement as long as the statement is terminated prior to column 72 or continued with the standard Continuation Sequence.

Definition Search Sequence

The Network Director searches the defined set of definitions (control blocks) to establish the appropriate settings when a network element is ***activated***. *Activation* occurs the first time The Network Director enters a session with the device, when it returns from a subsystem, or when a user logs on or logs off.

The process of *activation* within The Network Director consists of establishing the operating characteristics for the specific network element involved. The operating characteristics are accumulated from applicable definition blocks depending upon how the network element is identified to The Network Director. The process consists of locating the definitions that are applicable to the network element and interpreting which operands from the definitions should apply to the network element.

Once The Network Director has established which definition blocks **might** be related to the network element, the located control blocks are utilized according to the following table:

Situation	User	User Group=	Terminal	Terminal Group=	Default
no USER is logged on	n/a	n/a	if present	if present	always used
USER is logged on	if present	if present	n/a	n/a	always used
USER is logged on and ATTRIBUTE EXTENDED-SEARCH is in effect	if present	if present	if present	if present	always used

Figure 4. Control Block Search Sequence

Operands are always collected from the most detailed definition to the most general (left to right in preceding table). When collecting values, a given characteristic will only be set when its value is ***not the standard setting*** for the operand. The following table demonstrates where an operand originates (dependent upon the Situation as described in the preceding table). "-" indicates the operand is not supported on the definition statement. Other values are the *standard* setting for the operand, which must be set differently to take effect. The operands collected in this manner are:

Operand	User	User Group=	Terminal	Terminal Group=	Default
ACQUIRE	NO	NO	NO	NO	NO
AUTOLOGOFF	NO	NO	NO	NO	NO
COMMANDS	NO	NO	NO	NO	NO
DIM	-	-	0	0	0
FORMAT-ID	Standard	Standard	Standard	Standard	Standard
ID-AREA	YES	YES	YES	YES	YES
IDENTIFICATION	-	-	NO	NO	YES
LOGO	null	null	null	null	null
MESSAGES	NOTES MEMOS	NOTES MEMOS	NOTES MEMOS	NOTES MEMOS	NOTES MEMOS
PROFILE	null	null	null	null	null
STATUS-INTERVAL	0	0	0	0	0
TRIES	-	-	0	0	3

Figure 5. Operand Collection Sequence

Without regard for the search sequence, The Network Director locates the first definition where the specification **is not the standard setting** for the operand. As an example:

```
DEFAULT  IDENTIFICATION=NO
GROUP    SIGNON,IDENTIFICATION=YES,ACQUIRE=NO
TERMINAL T01001,GROUP=SIGNON,IDENTIFICATION=NO,
                ACQUIRE=SELECT
```

The device T01001 will be assigned to the GROUP identified as SIGNON and will have the ACQUIRE=SELECT characteristic (it is not the standard setting), but will have the IDENTIFICATION=YES characteristic from the SIGNON GROUP definition. The IDENTIFICATION operand setting from the TERMINAL definition is not detected by The Network Director because the specification is the standard.

Wild Character

The Network Director allows a plus sign ("+") as a Wild Character in many Parameter Statement locations where a logical grouping is beneficial (TERMINAL and USER statements). The Wild Character may be used to simplify the specification of Parameter Names, generate logical groupings of terminals and users, and other general purposes.

A Wild Character implies to The Network Director that any character in a given location will be accepted. A Parameter Name of PAY+++++ on a TERMINAL statement includes all terminals whose logical unit name start with the letters PAY. The Network Director checks at a byte by byte level for comparison. Thus, a PAY++ specification will cover the terminal named PAY01, but will not cover the terminal named PAY001.

A Wild Character embedded in the middle of a character string represents only one character. The string PY+88 will include any logical unit with PY in bytes 1 and 2, 88 in bytes 4 and 5, and any character in byte 3. However, the terminal named PY6881 will not meet the criteria. To include terminals with this name configuration, the specification of PY+88+ would be necessary.

The Wild Character is provided to eliminate the requirement for tedious repetition within the Configuration Parameters, but it must be carefully used to identify just those entities desired.

The Wild Character may be used in the locations identified in the individual discussions of the Statements and their respective operands. If the Wild Character is not specifically referenced as allowed, you should assume it is not allowable.

Common Configuration Parameter Operands

Several of the Configuration Parameters have the same operand available to them. The operands have the same specific meaning, but may apply during processing in a slightly different manner (see "Definition Search Sequence" on page 10).

The following operand discussions are generally applicable to the DEFAULT, TERMINAL, GROUP, and USER definitions, as defined in the appropriate chapter.

LOGO

is the operand that provides the simple graphic portrayal of the installation defined identifying information. This information will be placed at the top of The Network Director's Application Selection Panel. It may be a simple string placed in quotes (LOGO="Data Center"), a more complex multiple record image (LOGO=), or a reference to a RESOURCE.

A simple string of characters 9 bytes or longer will be centered on line two of the various panels and will cause line one and three to be blanked. A string of 8 characters or less will be interpreted as a reference to a RESOURCE name. Additional information about variable information can be located under "Variables" on page 16.

The more complex specification (specified by a equals sign blank combination "= " following the operand LOGO) indicates that the LOGO will begin in column 1 of the next Configuration Parameter record (asterisks are valid) and will continue until the text string LOGO-END is encountered in some subsequent record. The Network Director assumes that the LOGO text will be in all 80 columns of the Configuration Parameter record image.

The LOGO may be multiple record images, but some restraint is necessary or the Application Selection Panel may be full of LOGO with no room left for selections. The Network Director will accept any size LOGO, but may not display the entire LOGO (dependent upon the physical screen size). This truncation will happen at execution time and is based upon the terminal in use.

If the LOGO operand is omitted, The Network Director will place its own LOGO in the LOGO area. It will include a simple graphic and The Network Director's release level (see the *General Information Manual* for an example).

SELECTIONS

All Network Director selection menus are created at execution time based upon the configuration options present in The Network Director's configuration parameters.

The SELECTIONS operand provides a manner to "express the relationship" between the APPLICATIONS= specifications that may be present on the USER, TERMINAL, and DEFAULT statements (an applicable GROUP choice can be used in addition to the USER or TERMINAL definition).

The Network Director allows you to utilize a boolean like specification describing how APPLICATIONS should be merged. The following characters are used in the SELECTIONS= syntax to implement this specification:[2]

D the DEFAULT APPLICATIONS=

U the USER and the USER GROUP= APPLICATIONS= specification (if both specified, they are combined prior to processing)

T the TERMINAL and TERMINAL GROUP= APPLICATIONS= specification (if both specified, they are combined prior to processing)

& use a boolean "AND" function to merge the two lists (the selection will be included only if it is contained in both the lists being merged)

+ use a boolean "OR" function to merge the two lists (the selection will be included if it is contained in either of the lists being merged)

() specifies a merging of two lists that should occur prior to the final merge operation

To illustrate the possible results of these specification alternatives, assume that the following three configuration statements apply:

```
DEFAULT  APPLICATIONS=(A,B,D,E),SELECTIONS=?????
TERMINAL APPLICATIONS=(A,B,C,F)
USER     APPLICATIONS=(A,C,D,G)
```

[2] You may also specify AND, OR, and the asterisk ("*") for upward compatibility from earlier releases of The Network Director.

Presuming that the letters A through G represent defined APPLICATIONs, setting the SELECTIONS= operand as indicated in the following table will present a menu with the identified items on it.

Example	SELECTIONS=	Resulting choices
1	D	A B D E
2	T	A B C F
3	U	A C D G
4	D+T	A B C D E F
5	D+U	A B C D E G
6	T+U	A B C D F G
7	D&T	A B
8	D&U	A D
9	T&U	A C
10	D+T+U	A B C D E F G
11	D&T&U	A
12	D+(T&U)	A B C D E
13	T+(D&U)	A B C D F
14	U+(D&T)	A B C D G
15	U&(D+T)	A C D
16	T&(D+U)	A B C
17	D&(T+U)	A B D
18	OR	A B C D E F G
19	AND	A B C D E
20	* (not logged on)	A B C D E F
21	* (logged on)	A B C D E G

Figure 6. SELECTIONS Operand Processing

You can specify any combination of the D, T, or U literals (representing the source for the APPLICATIONS) that you would like. Additionally, the literal "ALL" is identical to "D+T+U" or other variations and represents the inclusion of any APPLICATION specified for the user in any definition statement.

This mechanism provides tremendous flexibility in configuring The Network Director to produce the precise results you desire. It is very important that you understand the option chosen so that only the appropriate choices are delivered to the terminal user.

Variables

The Network Director contains a generalized variable processor that enables the local installation to specify many execution time variables in Network Director messages, user initiated messages (Message Facility as well as BROADCAST commands), INFO panels, within the various LOGOs, Application Selection Panel titles, and as a portion of the INITIAL-DATA strings. The variable processor is general in nature and has the following set of guidelines:

1. Data strings are scanned left to right looking for the variable substitution character, which is an ampersand ("&").

2. Variable substitution begins with the substitution character and will continue for the **length of the variable data**, or the type specification, provided sufficient space has been provided. If insufficient storage space is reserved, the variable processor will truncate the variable replacement to preserve the integrity of storage.

3. Variables are interpreted at the time a message is initially issued from within The Network Director, and is based upon the dispatchable function environment (DFB) active at the time.

4. Numeric values are replaced with leading zeroes suppressed.

Currently defined variables must all be preceded by the substitution character (the ampersand) and can be modified via use of the "type specification" as discussed under "Symbolic Variables" on page 271.

Variable	Source	Length	Contents
ACCOUNT	ANE	20	current value of the Account: field from the Identification Area
ADBMODE	ADB	8	the LOGMODE name associated with the APPLICATION definition block (may be associated with a network element currently connected to a subsystem)
ADBNAME	ADB	8	the logical name of the APPLICATION definition block
ADBTARGT	ADB	8	the first VTAM applid associated with the APPLICATION definition block
ADBTARG2	ADB	8	the second VTAM applid associated with the APPLICATION definition block
ADBTERM	ADB	8	a count of the number of terminal devices currently connected to the APPLICATION
ADBTITLE	ADB	28	the descriptive title of the APPLICATION definition block
ADBUSER	ADB	8	a count of the number of network users currently connected to the APPLICATION
BLANK	literal	1	inserts a EBCDIC blank character (you can suffix this variable with a numeric value to indicate repeating occurrences of the BLANK).

Variable	Source	Length	Contents
BNDMODE	ANE	8	the LOGMODE name extracted from the CINIT RU (this is the BIND image name associated with the session between the device and The Network Director)
COMMAND	SWA	67	full image of the Command: line used to indicate the item for selection
CONNECT	ACEE	8	the current RACF connect group associated with the user
CPUID	STIDP	6	6 digit CPUID from the processor The Network Director is dispatching on (high order nibble set to zero for multi-processors)
CSP	SWA	4	a 4 digit value equivalent to the current selection page number of the selection being displayed (where a "page" is represented by the number of selections that will fit in the display area after the LOGO, Identification area, Command line, and Broadcast area are reserved from the current panel)
DATE	STCK	8	current date (as formatted via the GLOBALS DATE-FORMAT)
DATEC	STCK	8	current date with 4 digit year (as formatted via the GLOBALS DATE-FORMAT) The DATE-FORMAT operand controls where the century appears as follows: ***DATE-FORMAT*** ***&DATEC Result*** **yymmdd** yyyy/mm/dd **mmddyy** mm/dd/yyyy **ddmmyy** dd/mm/yyyy
DIRAPPL	DIR	8	the last application selected by the user (as identified in the System Directory)
DIRDEPT	DIR	8	System Directory Department value
DIRGRP	DIR	8	System Directory Group value
DIRINFO	DIR	25	the System Directory Information keyword
DIRLLU	DIR	8	the last VTAM terminal that the user logged on at (from the System Directory)
DIRSTAT	DIR	8	the value of the application selected by the user, the LU name of the terminal the user is currently logged on at, or "Inactive" (indicating that the user is not currently utilizing the system).
EXC	ANE	4	current number associated with the device's retry error counter
EXTEN	ANE	8	current Extension value from the Identification Area

Variable	Source	Length	Contents
GROUP	GDB	8	value associated with the currently active GROUP definition for a given network element
HOSTPU	PDA	8	collected from the ACF/VTAM vector list present at ACB OPEN time
INFO	IWA	5	the INFO panel number of the currently displayed INFO panel (valid only in the INFO facility).
ILNE	IWA	5	the INFO line number of the current line within the INFO panel (valid only in the INFO facility).
ILNS	IWA	5	the total number of lines in the current INFO panel (valid only in the INFO facility).
INHERIT	ACF2	8	a specialized ACF2 token useful only when forwarding a device to a subsystem. INHERIT can be utilized to eliminate the need for transferring a clear text password to an ACF2 managed subsystem.
ICPG	IWA	5	the current page number within the INFO panel (valid only in the INFO facility).
ITC	ANE	4	the current value associated with the iteration counter (consecutive session attempts)
ITPG	IWA	5	the total number of panels (pages) in the current INFO topic (valid only in the INFO facility).
JOBNAME	PDA	8	MVS EXTRACT of TIOT or VM Virtual Machine Name
K	SSE	2	current value of the pfkey value assigned to the selection on the Application Selection Panel.
LOGMODE	ANE	8	current value of the LOGMODE value associated with the device that was requested by the terminal operator via a LOGMODE or SETMODE command
MOD	STIDP	4	the host processor model type
NAME	ANE	8	the value from the Id field in the Identification Area
NETID	ANE	8	the origin NETID associated with the device
NETNAME	PDA	8	the value for the network name derived from the ACF/VTAM ACB OPEN vector list
NEWS	DIR	4	set to the constant "View" if the user has received the NEWS panel
NODE	ANE	8	the value for the current SITE the device is connected to or came from

Variable	Source	Length	Contents
OPERANDS	SWA	80	all data from the Command: line after the token that caused selection
OPSYS	PDA	8	operating system maintenance level (OS CVT or VM DIAGNOSE X'00')
PAn	PDE	8	the character string associated with the PAn key from the Profile for the network element, where n may be 1, 2, or 3
PARMnn	PDE	80	the character string associated with the PARMnn field from the Profile for the network element, where nn may be 1 through 10
PASSWORD	ANE	8	the password associated with a current network element
PFnn	PDE	8	the character string associated with the PFnn key from the Profile for the network element, where nn may be 01 through 12
PRINTER	PDE	8	the character string associated with the PRINTER field from the Profile for the network element
ROOM	PDE	8	the value associated with the Room: field of the Profile for the network element
SELECTION	SWA	67	first token from the Command: line used to indicate the item for selection
SEP	ADB	1	the character associated with an APPLICATION SEPARATOR= field
SFDARK	literal	2	a hexadecimal character string that generates the 3270 order to set *dark* intensity (non displayable) and protected mode
SFPROTECT	literal	2	a hexadecimal character string that generates the 3270 order to set normal intensity and protected mode
SITE	PDA	8	the SITE name from the GLOBALS statement
SSCP	PDA	8	the SSCPNAME derived from the ACF/VTAM ACB OPEN vector list
SMF	PDA	4	the id extracted from the OS SMCB
SUB	ANE	4	the origin subarea for the device
TERM	ANE	8	the Lu: field associated with the device
TIME	STCK	8	the time of day in the form HH:MM:SS
TSP	SWA	4	a 4 digit value equivalent to the total number of Application Selection Panels that will be required to display all the selections the individual is authorized for

Variable	Source	Length	Contents
USER-NAME	literal	20	the full name associated with the user from the System Directory (normally extracted from the applicable security system).
USER-PHONE	literal	20	the phone number associated with the network element as extracted from the System Directory. It may be extracted from the ACF2 LIDREC or the VMSECURE *PH card, if not already specified in the DIRECTORY definition.
VERS	PDA	5	version identifier for the executing Network Director
VTAM	PDA	5	The ACF/VTAM release identifier

Figure 7. Variable Summary

BLANK and SEP may also be specified with a repeating value, which is simply a numeric value suffixed to the variable indicating a repeating value. E.G., &BLANK9 causes nine blanks to be inserted starting from the physical location of the ampersand.

When variables are utilized in the Editor, the variables will only be interpreted when the Editor is in *View* mode. That is, any facility that allows you to change the contents of the message, panel, etc. will display the variable before translation. This may cause the interpreted panel to take on a slightly different format unless you specifically reserve the appropriate number of characters for variable value insertion. To demonstrate this, assume the following two statements are inserted into a LOGO and that the GLOBALS SITE value is set to the literal string **ABCDEFGH**.

```
This is the &SITE processor
This is the &SITE... processor
```

Variable replacement for SITE is 8 characters, beginning with the ampersand. Therefore, the two lines will produce the following results:

```
This is the ABCDEFGHocessor
This is the ABCDEFGH processor
```

Note: The use of the periods with **&SITE** shown above is an example of placing a positional character into the string to keep track of how many characters the &SITE variable will take.

Messages that are created via the Message Facility have their variables translated to actual values when they are *sent*.

ACF2

The ACF2 command allows a Network Administrator to cause The Network Director to reissue the ACF2 SVC to accomplish a refresh of the resident rules associated with generalized resource rule interpretation for the Application Selection Panel composition. This option is in effect when you have specified the constant "ACF2" as one of the APPLICATIONS for a network user.[3]

The format of the ACF2 statement is:

```
ACF2
[ RULES={TRANSIENT|DEMAND|RESIDENT} ]
[ TYPE={TND|character code} ]
```

Figure 8. ACF2 Syntax

RULES

This operand can be set to:

TRANSIENT indicates that the resource rules will be loaded and utilized as necessary during execution. After use they will be deleted from storage.

DEMAND indicates that rules will be loaded and utilized as necessary during execution and will remain loaded until another Directory refresh operation is initiated or The Network Director is restarted. To refresh the contents, simply issue the ACF2 command again.

RESIDENT instructs ACF2 to load all resource rules associated with The Network Director into main storage and retain them there for use during execution. To refresh the contents of the resident rules, simply issue the ACF2 command again.

The ACF2 command can be issued from a Network Administrator's terminal or can be present in the initialization Configuration Parameters. If it is not issued, ACF2 will

---

[3] Support for the mass interpret function associated with this generalized resource rule process requires ACF2/MVS Version 5.0 or higher

schedule I/O operations as necessary to accomplish rule set interpretation, which can create a relatively high overhead for resource rule interpretation.

TYPE

This operand identifies the three byte ACF2 *type* that will identify The Network Director's related resource rules within ACF2's data bases. This will default to TND, but may be set to any three characters your installation would prefer. If you are operating multiple Network Director's, NRS recommends that you identify each Network Director with a unique TYPE code to separate the ACF2 rules associated with the individual Network Directors.

Examples

```
ACF2 TYPE=NRS,RULES=RESIDENT
```

This statement requests that the ACF2 SVC make all the rules associated with the type code of NRS resident in the address space for subsequent referencing by SVC calls.

APPLICATION

This definition element defines a logical application system to The Network Director. It will eventually represent a single entry on a terminal user's Application Selection Panel (after being authorized for this APPLICATION via the APPLICATIONS= operand).

This statement could simply identify a major software subsystem (CICS, etc), but additional flexibility within the computing facility can be achieved by logically identifying the application systems in use (such as PAYROLL, etc). This further identification process will allow the Network Administrator to move, monitor, and control individual application subsystems independently.

The format of the APPLICATION statement is:

```
APPLICATION

   application name
   [ ACTIONS=(action character,command string, ... ) ]
   [ ALARM={YES|NO} ]
   [ ATTRIBUTES=({HIDDEN|NONE|NO-ACQUIRE}, ... } ]
   [ AUTOLOGOFF={NO|YES|RETURN|SELECT} ]
   [ BALANCE=({numeric-value|1}, ... ) ]
   [ COMMENTS={Info Display Direct command} ]
   [ COMPRESS={YES|NO} ]
   [ CONCURRENT={0|numeric value ]
   [ DAYS=(day specification, ...) ]
   [ ERASE={YES|NO} ]
   [ FDE-NAME=alpha value ]
   [ INITIAL-DATA=(data, ...) ]
   [ INITIAL-FUNCTION=transid ]
   [ INITIAL-STATUS={ASIS|HELD} ]
   [ LOGMODE={0|alpha value} ]
   [ MAXIMUM={0|numeric value} ]
   [ MONITOR={YES|NO|DOWN} ]
   [ MONITOR-INTERVAL={0|numeric value } ]
   [ NAME=alpha value ]
   [ PFKEY={pfkey value|NO} ]
   [ PHONE=alpha value ]
   [ PRIVILEGE=(alpha pattern, ...) ]
   [ ROTATE=(alpha string, ... ) ]
   [ SEPARATOR={NO|character} ]
   [ SEQUENCE={0|numeric value} ]
   [ SSI={YES|NO|EXTENDED|PROTECTED|INHERIT} ]
   [ STATUS={INQUIRE|ISTnnna} ]
   [ STATUS-STRING=alpha value ]
     TARGETS=(applid 1, applid 2)
   [ TIMES=(time specification, ...) ]
   [ TIMEOUT=numeric value ]
   [ TITLE=application description ]
   [ UPDATES={NO|YES} ]
   [ USERVAR=alpha value ]
```

Figure 9. APPLICATION Syntax

application name

identifies the logical name that will be used later in an APPLICATIONS= operand to identify this APPLICATION.

is also the Command Name that may be entered on the Command line on the Application Selection Panel to "select" this APPLICATION. The first item entered on the Command line by the terminal operator will be checked against this application name for the length of the application name to decide if the operator has entered a request for this APPLICATION.

ACTIONS

establishes character values that can be entered into the Selection Character on non-CUA Application Selection Panels (the "_" immediately preceding the Selection Title). Normally, a character entered in this location indicates a choice (called the Modified Field selection method). However, with the ACTIONS operand, the Network Administrator can indicate special processing for specific characters.

When the defined action character is entered by a terminal operator, the command string paired with the action character will be executed exactly as if the terminal operator had typed it on the Command: line.

This facility can be utilized to provide a short hand method for the terminal operator to create certain command sequences. A typical use for this is activating the letters *H* or *S* for HELP about an APPLICATION or perhaps the SCHEDULE a particular APPLICATION has. You can define any character that can be entered on a 3270 keyboard. The character "?" is also used to provide entry into the INFO facility for information about the selection.

```
APPLICATION TSO,ACTIONS=(H,'HELP TSO',
                         R,'TSO RECON'),TARGET=TSO
```

indicates that a terminal operator entering an upper case H in the selection character will be given to the APPLICATION named HELP (The Network Director's INFO facility), which will then look for a TSO entry in the highest level index. The letter R will create a logon to TSO with the RECON operand being passed (presuming &OPERANDS has been set on the TSO APPLICATION definition).

ALARM

controls whether The Network Director is to activate the 3270 alarm (on appropriately equipped terminals) when this application changes status.

NO indicates that the status is to be updated, but the alarm should not be activated.

YES indicates that the alarm should be activated.

ATTRIBUTES

associates special processing characteristics with the APPLICATION being defined. The supported attributes are:

HIDDEN indicates that The Network Director should **not** display this APPLICATION on the Application Selection Panel. The terminal operator will be capable of selecting it via the Command: line or by pressing the associated PFKEY (if there is one). This APPLICATION will be "hidden" from the operator's view. Dynamic status updates for this APPLICATION will not be reflected to the terminal operator.

NO-ACQUIRE overrides the ACQUIRE=SELECT or YES option associated with the other definition statements and implies ACQUIRE=NO. This is useful when the APPLICATION definition is associated with a Network Director in another VTAM domain.

NO-ACQUIRE and the TERMINAL ACQUIRE=SELECT operands can be utilized to make the navigation throughout a large network of processors more meaningful to the terminal operator. Normally, a single device is LOGAPPLed to The Network Director in the "home" domain. When multiple Network Directors are involved it is typical for the device to select an alternate Network Director and then choose an application in the alternate domain. When the device logs off of the selection application in the alternate domain, it is returned to The Network Director in the home domain as a result of the LOGAPPL parameter.

If The Network Director in the alternate domain had TERMINAL ACQUIRE=SELECT in effect the device will return to the alternate Network Director after log off instead of the "home" Network Director. Thus, the only time a queued acquire would not be desirable is if the device is "returning" to the home Network Director. The NO-ACQUIRE option on the APPLICATION statement provides the facility to identify which APPLICATIONs should have this special characteristic.

NONE specifies that there will be no specialized ATTRIBUTES associated with this APPLICATION

AUTOLOGOFF

instructs The Network Director whether to automatically LOGOFF the User at a terminal when the User selects this subsystem. Valid settings for this operand are:

NO the default value indicates that The Network Director is to remember which user has logged on to the device and to bypass any automatic logoff logic

YES indicates that The Network Director is to logoff the user when the device returns to The Network Director from the subsystem

RETURN is the same as YES

SELECT requests that the terminal user be logged off at the same time as the device is forwarded to the subsystem

BALANCE

Specifies the weighting that should be utilized by The Network Director to distribute network users of an APPLICATION that is being "load balanced" via usage of the ROTATE operand. Each list operand is associated with its corresponding ROTATE name and establishes the relative percentage of network users that should be sent to the subsystem.

You can think of the BALANCE operand as indicating the percentage of network users that should be assigned by The Network Director to the corresponding APPLICATION. As an example:

```
APPLICATION TSO1,TARGET=A01TSO
APPLICATION TSO2,TARGET=A02TSO
APPLICATION TSO3,TARGET=A03TSO
APPLICATION TSO,ROTATE=(TSO1,TSO2,TSO3),BALANCE=(40,50,10)
```

These configurations parameters will cause The Network Director to distribute users between three applications. TSO1 will receive 40% of the active users, TSO2 50%, and TSO3 10%. This distribution mechanism allows you to take into account the relative size of the processors hosting the APPLICATIONs, etc.

You can also use BALANCE to establish a "backup" role for one of the specified APPLICATIONS. A BALANCE value of 0 (zero) causes The Network Director to skip logically selecting the designated APPLICATION unless no other alternative is available.

BALANCE=(100,0) causes The Network Director to send all users selecting the item to the first APPLICATION unless it is down. If the first APPLICATION is down, The Network Director will forward the user to the second defined APPLICATION.

COMMENTS

Establishes the Info Display Direct command that will be issued when a terminal user enters an "H" (for Help) in the selection character before the selection on the Application Selection Panel.

As an example, COMMENTS='=92000' will cause The Network Director to display Info Panel 92000 when a terminal user enters H in the selection character.

COMPRESS

controls whether The Network Director will automatically compress blanks out of the SSI data stream (INITIAL-DATA=).

NO indicates that no compression logic will be utilized when constructing the SSI string.

YES indicates that embedded blanks should be suppressed.

CONCURRENT

Indicates the number of times that an individual user may select this APPLICATION at the same time. Zero indicates that there is no limit. Any other value indicates that the user may not exceed the concurrent usage specified. The specified value may be from 0 to 32,767.

When an individual user attempts to exceed the CONCURRENT value set for a specific APPLICATION, The Network Director will reject the attempt to select it and issue the following message to the terminal user:

```
TND0828 You have attempted to select [application] [number] time(s)
```

DAYS

specifies the days of the week that the application is available for use. The value of this argument is in addition to any TIME specification and both conditions must be true in order for the terminal user to select the application. A more detailed discussion of the DAYS format is under "Day Specification" on page 6.

ERASE

instructs The Network Director whether to clear the screen prior to forwarding the device to the target subsystem. This is useful for subsystems like CICS, where the initial transaction is anticipating that the device is clear (has no content).

YES indicates that The Network Director should completely clear the screen prior to forwarding the device

NO indicates that the screen does not need to be cleared.

FDE-NAME

Identifies the 8 character name that is associated with the field in the ACF2 FDR that identifies the bit in the ACF2 logonid record that permits access to this APPLICATION. The 8 character name must have been previously defined in the ACF2 FDR via a @CFDE macro and the bit to be checked must be present in the LIDREC that The Network Director is using. If you are using the mini-LID feature of the @MUSASS definition for The Network Director, make sure you include the field in the mini-LID definition.

The GLOBALS SECURITY=ACF2 operand is required to have been processed before the APPLICATION statement containing this operand can be properly processed.

INITIAL-DATA

describes the data stream that should be made available to the target subsystem. This data stream will be concatenated with the INITIAL-FUNCTION value (if provided) and provided to the subsystem initial routines or to The Network Director's Single System Image modules in the target subsystem. INITIAL-DATA is typically used to pass initial data to the target application system.

The INITIAL-DATA operands are one or more individual arguments that are separated by a comma (standard list syntax). Each argument may be an EBCDIC constant (maximum of 50 bytes per literal) or one of the supported system variables as documented in the section "Variables" on page 16.

Each variable causes The Network Director to transfer its equivalent values at execution time as portions of the INITIAL-DATA string. Thus, INITIAL-DATA=(86,&TERMINAL) will result in a string equivalent to "86TM03" for the terminal used in many of the figures in this manual.

If the &NAME variable is blank (no user has logged onto the terminal), the formatting of the SSI area is automatically terminated.

INITIAL-FUNCTION

specifies the program or transaction, etc in the target subsystem that is to be given control when the terminal operator selects this application.

When The Network Director processes a request for connection, it will pass the INITIAL-FUNCTION value to the target subsystem. Before the target application will respond to this facility, it must be supported by The Network Director's Single System Image concept. Currently supported are CICS, COM-PLETE, MODEL204, other Network Directors, IMS/DC and IDMS/DC. Contact North Ridge Software, Inc. for additional information about the exact status of other subsystems.

INITIAL-STATUS

establishes The Network Director's method for identifying the application's initial availability.

HELD will set the application's status to HELD until released by the Network Administrator.

ASIS The Network Director will establish a given application's status by interrogating its VTAM condition (via VTAM INQUIRE macro) and combining the result with TIMES and DAYS specifications

LOGMODE

indicates whether The Network Director should override the default LOGMODE for a device requesting the defined APPLICATION. 0 indicates that the target subsystem will accept the device as it is set up (the default LOGMODE). Any other specification is the name of the LOGMODE that should be used instead of the default.

MAXIMUM

establishes the maximum number of network elements that can be forwarded to the defined APPLICATION at once. 0 indicates that there is no maximum in effect. A numeric value indicates the total that The Network Director will allow to select the application.

Note: When the APPLICATION is at its defined MAXIMUM, The Network Director will **not** update the Selection Status area on the Application Selection Panel. The network element asking for an APPLICATION at its MAXIMUM will receive a message indicating that the APPLICATION is at its max and the selection will be ignored.

MONITOR

controls the manner in which The Network Director will establish the status of the defined APPLICATION.

YES instructs The Network Director to periodically check the status of the APPLICATION by issuing INQUIRE APPSTAT. The interval between checks will be controlled by the values set via the GLOBALS TIMER or the APPLICATION MONITOR-INTERVAL operands.

NO indicates that the APPLICATION should **not** have the INQUIRE APPSTAT issued. The Network Director will assume that the APPLICATION is always available. Attempts to select the APPLICATION may or may not fail (depending on whether the subsystem is up or not).

DOWN specifies that the INQUIRE APPSTAT is to be issued when the APPLICATION is not available ("Down"). If the subsystem associated with the APPLICATION is available ("Up"), the INQUIREs will not be issued. The APPLICATION will be identified as Down when an attempt by a network element to select it fails.

MONITOR-INTERVAL

establishes the elapsed time interval between INQUIRE operations. If this is set to zero or allowed to default, the monitor interval is controlled by the GLOBALS TIMER operand value.

NAME

Is the 1 to 20 character name of the individual or department responsible for the APPLICATION. This name will be included in the message formatted as a result of the OWNER command.

PFKEY

specifies a program function key value for non-CUA Application Selection Panels that is assigned to the application (if it is available). This value will be used for this application if the PFKEY is not already assigned. PFKEYs will be assigned on the Application Selection Panel by evaluating the USERS, TERMINALS, GROUP, and DEFAULT statements first, then individual APPLICATION specifications, and finally by The Network Director simply assigning ascending sequential values.

The pfkey value can be the text string PFxx, where xx can be from 1 (or 01) to 24. Terminals that do not have function keys will have to use an alternate selection method to select the application. NO indicates that no pfkey value should be assigned to this APPLICATION. The text assigned via the GLOBALS ACTIVE-TEXT operand will be used instead to indicate that the APPLICATION is available.

You should also note that The Network Director will automatically "fold" the PFKEYs, when appropriate, if GLOBALS FOLD-PFKEYS=YES is in effect. This means that The Network Director will logically add 12 to a pfkey value lower than 12, if it is pressed and

no selection results. The Network Director will subtract 12 from the value if the key pressed is greater than 12. For example, if you define an APPLICATION with a PFKEY=1 specification and a terminal operator presses PF13 (assuming PF13 is not also assigned), The Network Director will assume that the operator is attempting to select the APPLICATION. This logic attempts to address the use of control unit RPQs that "change" the meaning of some of the 3270 devices PFKEYs. Even though they are labelled PF1, the RPQs may cause the key to actually initiate a PF13 aid key value (and the opposite).

PHONE

Is the 1 to 20 character phone number for the individual or department responsible for the APPLICATION. This number will be included in the message formatted as a result of the OWNER command.

PRIVILEGE

specifies a series of 1 to 8 character name(s) that authorizes access to the APPLICATION (wild characters are valid). The PRIVILEGE operand implies an additional check to verify that a given user is authorized for the selection (all other validation and authorization procedures remain in effect). The PRIVILEGE operand may be utilized with APPLICATION definitions in the following security environments:

RACF PRIVILEGE operand values may contain wild characters and are tested against the list of connect groups associated with the user. See "APPLICATION Authorization" on page 216 for additional information.

TopSecret/MVS PRIVILEGE operand values identify the TopSecret/MVS facilities that must be associated with the user in order for the APPLICATION to be included on the Application Selection Panel. The Network Director retrieves the FACLIST via the TopSecret/MVS application interface for comparison.

TopSecret/VM PRIVILEGE operand values identify TopSecret/VM resources that must be associated with the user (the ACID) in order for the APPLICATION to be included on the Application Selection Panel.

If specified, PRIVILEGE implies that the additional check must be complied with. That is, the user will have to be logged on via RACF or TOP SECRET.

ROTATE

Identifies a set of APPLICATION names that will be used as a pool of actual definitions for the target subsystems. A network user that selects this APPLICATION will actually be sent to one of the APPLICATIONs defined on the ROTATE operand (selection is controlled by the number of current network users of each of the ROTATE APPLICATIONS and is under the control of the BALANCE operand).

This operand will not be utilized unless the APPLICATION TARGET is left blank.

```
APPLICATION TSO1,TARGET=A01TSO
APPLICATION TSO2,TARGET=A02TSO
APPLICATION TSO3,TARGET=A03TSO
APPLICATION TSO,ROTATE=(TSO1,TSO2,TSO3)
```

These configurations parameters will cause The Network Director to evenly distribute users that select TSO amongst TSO1, TSO2, and TSO3.

This **load balancing** is useful when the full volume of the network exceeds (or is otherwise undesirable) the capacity of a single copy of the designated subsystem. E.G. A large, multiple CPU installation when The Network Director is running in a CMC host with the individual TSOs operating on multiple back end hosts with shared DASD connections (enabling any TSO user to be on any host).

SEPARATOR

specifies the single character that will be inserted into the INITIAL-DATA string between each operand. This is commonly used to delimit the multiple operands for eventual parsing by the target subsystem.

character establishes the character that will be inserted between each INITIAL-DATA operand

NO there will be no SEPARATOR character inserted between the operands.

SEQUENCE

Assigns a numeric value to this APPLICATION that will be used to "sort" the individual choices that make up the Application Selection Panel for individual users. This mechanism allows you to provide basic controls over the order in which items will be displayed.

The value assigned to the APPLICATION may be between 0 and 32,767. After The Network Director has selected which APPLICATIONs will appear on the Application Selection Panel, it will sort the selections by the SEQUENCE field in a descending order. Thus, the APPLICATION with the highest remaining value will appear at the top of the selection list and the lowest SEQUENCE value will appear at the bottom. If all the APPLICATIONs have a SEQUENCE value of zero, then no sorting will be done.

SSI

controls whether The Network Director is to create the specialized format associated with automated LOGON within the target subsystem. This format is generalized in format and will typically be acceptable only to subsystems that have also had Network Director SSI code inserted into their VTAM terminal logon procedures. CICS, IMS/DC, other Network Directors, and IDMS/DC are subsystems that utilize this approach.

EXTENDED indicates that The Network Director is to utilize the SSX control block structure to pass data, which also includes the Extension and Account code field values.

INHERIT indicates that an extended SSI buffer (the SSX) is to be passed to the subsystem and that the password contained within the SSX is to be the ACF2 inherit token. This is supported within single domain ACF2 environments and is valid for APPLICATION definitions that define CICS, IDMS, IMS, NETVIEW, or other Network Directors.

NO indicates that The Network Director should not pass the SSI formatted control block to the subsystem code field values.

PROTECTED indicates that the password should **not** be forwarded to the APPLICATION in the SSI or SSX control block

YES indicates that The Network Director should pass the &NAME and &PASSWORD to the target subsystem. If the appropriate code is present in the target subsystem, The Network Director will automatically attempt to logon the user using the passed &NAME and &PASSWORD. If the logon succeeds, The Network Director will attempt to initiate the INITIAL-FUNCTION.

STATUS

Identifies how to establish whether the APPLICATION is available for use or not. Operand values are:

INQUIRE Instructs The Network Director to make use of the VTAM INQUIRE APPSTAT macro via the Application Programming Interface to establish if the APPLICATION is available or not.

ISTnnna Indicates that The Network Director should use the Secondary Program Operator interface to issue a DISPLAY ID= command to VTAM to establish the status. When the response to the DISPLAY is returned, The Network Director will scan the responses looking for the IST message specified in this operand. If found, the APPLICATION will be determined to be "Active" (subject to STATUS-STRING logic). If the message is not found, the APPLICATION will be "Down".

STATUS-STRING

When STATUS=ISTnnna is used and the message is returned via the SPO, STATUS-STRING specifies the 1 to 20 character string that will be searched for to determine if the APPLICATION is available or not.

As an example, assume that the following Configuration Parameters were coded:

```
APPLICATION CMS,TARGET=A01VM,
         INITIAL-FUNCTION=LOGON,
         INITIAL-DATA=(&NAME,'/',&PASSWORD,' ',&OPERANDS),
         TITLE='Conversational Monitoring System',
         STATUS=IST486I,
         STATUS-STRING='STATUS= ACTIV'
```

When The Network Director attempts to establish the status for the CMS APPLICATION, it will issue a VTAM D NET,ID= command internally. When ACF/VTAM delivers the response, The Network Director will look for any IST486I messages. When found, The Network Director will scan the message text looking for the precise string coded in the STATUS-STRING operand. If the message and string are found, then The Network Director will treat the APPLICATION as being active. If either the message or string are not found or ACF/VTAM does not respond in the proper NETWORK-WAIT interval, The Network Director will mark the APPLICATION as down.

To determine the STATUS-STRING value applicable at your installation to a specific APPLICATION, you can manually issue the VTAM D NET,ID= command from Network Administration.

```
IST097I  DISPLAY  ACCEPTED
IST075I  NAME = A01VM            , TYPE = APPL
IST486I  STATUS= ACTIV     , DESIRED STATE= ACTIV
IST977I  MDLTAB=***NA*** ASLTAB=***NA***
IST861I  MODETAB=***NA*** USSTAB=***NA*** LOGTAB=***NA***
IST934I  DLOGMOD=***NA*** USS LANGTAB=***NA***
IST597I  CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I  APPL     MAJOR NODE = A01NRS
IST212I  ACBNAME = VM
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST869I  USERID = VTAM
IST171I  ACTIVE SESSIONS = 0000000000, SESSION REQUESTS = 0000000000
IST314I  END
```

Visually scan the resulting output for which combination of characters in a message you would like to represent the "Active" condition.

TARGETS

specifies the 1 to 8 byte VTAM Applid that the using terminal should be passed to when a request is made for this APPLICATION (applid 1). This will be the "host" environment for the application subsystem and should match the host system's VTAM APPLID as specified in the VTAM APPL definition statement.

Specifying only one applid indicates that the entire function associated with the APPLICATION is contained with a single VTAM subsystem. If you specify a second applid, The Network Director will automatically begin checking the status of both VTAM targets in order to establish the availability of the subsystem. **Both** applids must be available in order for The Network Director to reflect the selection as active.

This *multiple target* option is generally useful when the target subsystem contains a configuration where the facilities to accomplish the application function are distributed across multiple VTAM subsystems (like CICS MRO, etc.).

There are several reserved TARGETs that The Network Director recognizes. They are TNDADMIN, TNDINFO or TNDHELP, TNDCMD, TNDMSG, and TNDCENTR. See the Notes at the end of this parameter statement discussion for more information.

TIMES

is the range in hours that the APPLICATION is available for use. The Application Selection Panel will portray this selection as HELD if the time is outside of this interval. All attempts by the terminal user to logically connect his terminal will be rejected. The time specification format is discussed in detail under "Time Specification" on page 5.

TIMEOUT

specifies the value that will represent the elapsed time interval associated with a network element that has connected to this APPLICATION. This parameter applies only to The Network Director's internal facilities (Network Administration, INFO, or Messages). The APPLICATION TIMEOUT= overrides any TIMEOUT specification that may be in effect for the terminal user and will only remain in effect for terminal operations controlled by the specific APPLICATION component.

The default of zero specifies that there will be no timeout interval for network elements connected to this APPLICATION.

TITLE

is the 1 to 50 byte general description for the APPLICATION. It should represent a short descriptive phrase that will identify the selection to the terminal user. The TITLE will be the text string included on the Application Selection Panel to identify the logical selection available to the terminal user. Non CUA Application Selection Panels will use a maximum of 28 characters of the title. CUA Application Selection Panels will use all 50 characters.

If it is not present, The Network Director will use the TARGET value for the TITLE.

To support light pen selection, the first character of the title must be a blank. This will cause The Network Director to place the appropriate combination in the output stream to create the title as a "light pen detectable" field.

UPDATES

controls whether this APPLICATION and its authorized Users will have the ability to accomplish UPDATE type activities. This parameter only applies to the special Network Director INFO and Network Administration TARGETs. UPDATES=NO will restrict the operator to simple query type use of the facility represented by the APPLICATION selection. The Network Administrator should define two APPLICATIONs if both UPDATES=NO and UPDATES=YES users are to be defined.

NO update type operations will not be allowed (the default). INFO users will be prohibited from using the EDIT or DELETE command. Network Administration users will be capable only of issuing the DISPLAY, VTAM, and VM commands.

YES when specified with the INFO APPLICATION, any network user that is authorized to use this APPLICATION will be allowed to enter the Editor to create and modify INFO topics. When used with the Network Administration APPLICATION definition, any user with authorization to use the APPLICATION will be able to modify the logical network, issue VTAM Modify commands, and modify other user's Messages (within the scope of the associated AUTHORIZATION operand).

USERVAR

establishes the eight character value associated with this APPLICATION subsystem that will be identified by ACF/VTAM as a USERVAR variable.[4]

To establish the availability of this APPLICATION, The Network Director will interrogate ACF/VTAM about the USERVAR value's current setting and will, in turn, establish the actual identity of the subsystem for status displays and terminal forwarding.

The process of identifying which subsystem is operating as the USERVAR is accomplished only when the APPLICATION is *Down*. If the subsystem terminates, The

---

[4] This facility is generally useful on ACF/VTAM systems utilizing XRF concepts. This is not available on ACF/VTAM systems prior to Version 3.1.1.

Network Director will dynamically repeat the interrogation of the USERVAR to identify the new target subsystem.

The usage of USERVAR causes The Network Director to dynamically set the TARGET value for the APPLICATION. Therefore, the initial TARGET value is not meaningful and does not have to be provided.

Examples

```
APPLICATION   PAYROLL,TARGET=PRODCICS,
                       TITLE='Employee Payroll',
                       TIME=(07:30-17:45),
                       DAYS=(MONDAY-FRIDAY),
                       PFKEY=PF4
```

This application (PAYROLL) is available from 7:30 am to 5:45 pm each weekday. When a terminal has requested this application, The Network Director should CLSDST OPTCD=PASS this terminal to the VTAM APPL named PRODCICS. When constructing the Application Selection Panel for any terminal that includes this application, The Network Director will assign program function key 4 (PF04) to this application (if possible).

```
APPLICATION   CODING,TARGET=TSO
```

This application (CODING) is always eligible for use (as far as The Network Director is concerned) and may be selected on a Application Selection Panel by looking for the descriptive title CODING. The Network Director will assign a program function key to this selection on a next available basis.

```
APPLICATION   CICS,TARGET=DBDCCICS,
              TITLE='CICS Teleprocessing',
              SSI=YES,INITIAL-FUNCTION=CSFE
```

This application (CICS) can be selected by looking for "CICS Teleprocessing". When selected, The Network Director will format the appropriate information to automatically logon the user and initiate the transaction CEMT.

```
APPLICATION TSO,TARGET=TSO,
            TITLE='TSO - Time Sharing Option',
            SEPARATOR=NO,INITIAL-FUNCTION=LOGON,
            INITIAL-DATA=(&NAME,'/',&PASSWORD,'  ',&OPERANDS)
```

This application (TSO) can be selected from the Command Line by entering TSO. The user will be automatically logged on if his Id and Password contain a current valid combination for TSO. The terminal user may also pass additional parameters to TSO by entering them on the Command Line after the token TSO.

Specialized APPLICATIONs

The Network Director contains several specialized applications that are identified by the TARGET name beginning with the letters **TND**. These are the Message Facility, INFO Mechanism, Internal Command Processor, The Network Center,[5] and Network Administration. They are dealt with by The Network Director just like any other application except that they do not actually represent a VTAM APPL. Thus the TARGET operand for their respective APPLICATION statements has specialized values.

The Network Director recognizes a definition of one of the specialized applications through a specially coded TARGET value. These TARGET values are:

TARGET	Use
TNDMSG	the Message Facility
TNDINFO	the Network Information Mechanism
TNDHELP	a synonym for TNDINFO
TNDADMIN	Network Administration
TNDCMD	the Internal Command Processor
TNDCENTR	The Network Center

Figure 10. Internal Application TARGET Values

TNDMSG - Message Facility

This internal application represents The Network Director's Message Facility. Selecting an APPLICATION with this TARGET will cause The Network Director to present the terminal operator with the primary messages menu, which can be utilized to edit, view, delete, print, or send Network Director messages to one or more other network elements.

TNDINFO/TNDHELP - Network Information File

Selection of an APPLICATION with TNDINFO or TNDHELP as a TARGET causes The Network Director to present the terminal operator with INFO topic 0. The exact INFO topic presented can be controlled by the Network Administrator through appropriate use of the INITIAL-DATA operand of the APPLICATION statement. If present, the text string associated with INITIAL-DATA will be used as an initial INFO command and can cause the first screen presented to differ from INFO topic 0.

TNDHELP differs from TNDINFO only in their uses on the Identification panel. TNDHELP can be selected from the initial panel (for IDENTIFICATION=YES devices)

---

[5] The Network Center is a separately priced software product from North Ridge Software, Inc. providing advanced facilities useful to systems programmers, Network Administrators, and security personnel in maintaining, operating, and managing a ACF/VTAM network.

and TNDINFO cannot be selected. Either is selectable from the Application Selection Panel (presented after the user has logged on).

TNDADMIN - Network Administration

Choosing an APPLICATION with TNDADMIN as a TARGET causes The Network Director to present the terminal operator with the LOG display with the bottom line of the panel containing the most recent LOG entry.

TNDCMD - Internal Command Processor

An APPLICATION with a TARGET of TNDCMD instructs The Network Director to insert the INITIAL-DATA string into an internal command buffer that is normally filled from the Command: line. TNDCMD provides a manner for the Network Administrator to associate a command line command with a PFKEY on an Application Selection Panel.

```
APPLICATION COMMAND,TARGET=TNDCMD,
            INITIAL-DATA=(LOGOFF)
```

will cause The Network Director to act exactly as if the terminal operator had entered the LOGOFF command on the command line.

You should exercise caution when defining TNDCMD APPLICATIONs that could generate recursive calls within The Network Director. Defining an APPLICATION named LOGOFF with INITIAL-DATA of LOGOFF would cause The Network Director to loop if the command were to process continually. The Network Director contains logic to detect recursion, but the function desired may not be accomplished as expected (in our example, the user will not actually be logged off). The Network Director contains logic that will detect and prohibit multiple level uses of TNDCMD. Thus, TNDCMD commands may only be "one level"deep.

Examples

```
APPLICATION INFO,TARGET=TNDINFO,
                 TITLE='Network Assistance',
                 INITIAL-DATA=('HELP SELECT'),
                 UPDATES=NO
```

This defines The Network Director's generalized Information Facility. It is detected by The Network Director because of the specialized value provided on the TARGET operand. The network users that have access to this APPLICATION will not be capable of updating the INFO file. The INITIAL-DATA operand overrides the default placement in the Information File when a terminal operator selects INFO. The HELP SELECT string will be processed as if the operator entered it as a command at the device.

```
APPLICATION NETADMIN,TARGET=TNDADMIN,
                     TITLE='Network Administration',
                     UPDATES=YES
```

This example identifies the Network Administration facility. Any network user that has access to this APPLICATION will be able to exercise the full range of Network Administration capabilities. This includes modifying the logical network, displaying the Primary Messages Menu, and issuing VTAM Modify commands.

Typically, Network Administration with UPDATES=YES specified is restricted to only a few network users. UPDATES=NO provides a facility with which to provide query type Network Administrator capabilities without endangering the integrity of the network.

DEFAULT

This definition provides characteristics that are common to all network users.

Most DEFAULT operands take effect only if there is no USER, GROUP, or TERMINAL statement in effect. The exceptions to this are the APPLICATIONS and the PFKEYS operands. These two will always be in addition to specifications on other Parameter Statements.

The Network Director collects characteristics from the USERS or TERMINALS statement first, then the GROUP statement, and last the DEFAULT statement. The combination of these items make up the actual characteristics that will be assigned to the network element operating within The Network Director. The TERMINALS definition will be utilized (when available) only until a terminal operator has logged on to the device. Once this occurs, the USERS definition will be utilized **instead of** the TERMINALS definition. The only operand currently utilized in a joint fashion (between the TERMINALS and USERS statements) is the APPLICATIONS= operand, which is manipulated as dictated by the SELECTIONS operand of the applicable control statement (see "SELECTIONS" on page 14 for a discussion of how this is done).

The format of the DEFAULT statement is:

```
DEFAULT

  [ ACQUIRE={NO|SELECT} ]
  [ APPLICATIONS=(application name, ...) ]
  [ ATTRIBUTES=({EXTENDED-SEARCH|FORCE-LOGOFF|NO-PATTERNS|
              NON-REPEATING|AUTO-SELECT|UPDATE-DIMMED|
              NEWS-ONLY-ONCE|INQUIRE-DOWN|EXACT-MATCH|
              DIRECTORY|NEWS-ALL-LOGONS|RACFSTAT} ...) ]
  [ AUTHENTICATION={NO|YES|EXT25|INTELLICARD|SNK} ]
  [ AUTOLOGOFF={NO|YES|RETURN|SELECT} ]
  [ COMMANDS={(YES|NO|DISC|DROP|FLASH|LOGON|RESET}, ... ) ]
  [ CONNECT-MAXIMUM={0|numeric value} ]
  [ CUA={NO|YES} ]
  [ DIM={0|numeric value} ]
  [ FORMAT-ID={STANDARD|OPTIONx} ]
  [ IDENTIFICATION={YES|NO } ]
  [ ID-AREA={YES|NO} ]
  [ ID-LOGO=installation logo ]
  [ LOGMODE-EDIT={YES|NO} ]
  [ LOGO=installation logo ]
  [ MESSAGES=({NOTES|MEMOS|BROADCASTS|NONE}, ... ) ]
  [ PASSWORD={password|YES} ]
  [ PFKEYS=({pfkey value|NO}, ... ) ]
  [ PROFILE=(name,{VIEW|CHANGE|NO}) ]
  [ PSWD-OPTIONS=(expiration,generations,minlength,minwait) ]
  [ RECOVERY={LOSTERM20} ]
  [ SELECTIONS=D+(T&U)|{D|T|U}[{+|&}{D|T|U}[{+|&}{D|T|U}]] ]
  [ STATUS-INTERVAL={0|numeric value} ]
  [ TIMEOUT={numeric value|0} ]
  [ TRIES={numeric value|3} ]
  [ WSF={COLOR|NO|YES|KEEP} ]
```

Figure 11. DEFAULT Syntax

ACQUIRE

Identifies whether The Network Director should queue a request (SIMLOGON) for a network element that selects a subsystem

NO no queued SIMLOGON request will be issued

SELECT each time a device is sent to an APPLICATION, The Network Director will issue the appropriate VTAM functions to cause the device to be returned immediately upon terminating the session with the APPLICATION.

ACQUIRE=SELECT is also useful when The Network Director forwarding the device to the subsystem is in a *remote* system to the device owning Network Director (a cross domain Network Director). It will cause the device to return to the "last" Network Director that had control of the device.

APPLICATIONS

identifies the applications previously defined by APPLICATION definitions that are to appear on all Application Selection Panels. This operand is used to remove the requirement for placing general purpose applications like INFO and MESSAGES onto every other APPLICATIONS operand in multiple USER, GROUP, and TERMINAL statements.

Omission of this operand will result in no default applications present on any Application Selection Panels. The Application Selection Panel contents will be determined by the applicable USER, TERMINAL, or GROUP statements (see "SELECTIONS" on page 14 for a discussion of how APPLICATIONS= operands are merged to produce the Application Selection Panel).

ATTRIBUTES

controls specific characteristics and activates specialized logic paths within The Network Director. Valid operands are:

AUTO-SELECT requests that any device that becomes active within The Network Director (either after initial logon for IDENTIFICATION=YES installations or at initial Application Selection Panel for IDENTIFICATION=NO installations) that has only **one** selection on the Application Selection Panel should be automatically sent to the subsystem specified by the selection. The device will not receive the Application Selection Panel, but will be immediately sent to the subsystem.

This has the effect of immediately forwarding AUTO-SELECT eligible devices when The Network Director detects that the single selection has become active (if the device is operational and the subsystem changes to "Active" from the "Down" condition).

DIRECTORY The System Directory is created in virtual storage as terminal users logon to The Network Director during a single execution. This information is then stored into the External File for subsequent usage.

If you would like The Network Director to automatically load the System Directory from the External File during initialization, specify the DIRECTORY ATTRIBUTE. This will cause The Network Director to load the all the System Directory entries from the External File and to save the entire System Directory during STOP QUIESCE processing.

This ATTRIBUTE should be turned on if your installation is relying upon the System Directory to properly represent all the users of your network even if they have not signed on to the current Network Director. This becomes important for Message Facility users that would like to "browse" the System Directory during message creation.

Automatically loading the System Directory costs about 100 bytes of virtual storage for each Directory Entry, which is unnecessary overhead if a full storage directory is not required.[6] If you would like to save the virtual storage, do **not** specify DIRECTORY as one of the ATTRIBUTES.

EXACT-MATCH Requests that Directed logon requests (application names entered on the Command line) match precisely the "first token" entered on the Command line. The first token is the blank delimited set of characters that occur first in the Command line (The Network Director will require one or more blanks after the application name in order to accept it as a request for the application).

EXTENDED-SEARCH normally, The Network Director uses the TERMINAL, then TERMINAL GROUP=, and finally the DEFAULTs to establish characteristics (LOGO=, etc.) for devices that are not logged on and USER, then USER GROUP=, and finally DEFAULTs for devices that are logged on. If you would like The Network Director to continue to factor in the TERMINAL and TERMINAL GROUP= definitions when collecting characteristics, specify EXTENDED-SEARCH.

FORCE-LOGOFF Determines whether a device in violation of the STATUS-INTERVAL or CONNECT-MAXIMUM operands should be queued for logoff or immediately logged off of The Network Director. FORCE-LOGOFF indicates the user will be immediately logged off.

---

[6] This storage is above the 16MB virtual storage line for XA or ESA systems where The Network Director is operating in 31 bit addressing mode.

INQUIRE-DOWN Instructs The Network Director to mark an APPLICATION "Down" when the corresponding INQUIRE APPSTAT does not receive an answer from ACF/VTAM. If INQUIRE-DOWN is not set, The Network Director will mark the APPLICATION "Held", which will require Network Administrator action to reinstate it as available.

NEWS-ALL-LOGONS Normally, the NEWS panel is delivered once each 24 hour period to each user after the user successfully logs on to The Network Director. This ATTRIBUTE requests that the NEWS be scheduled to the user each time a logon is successful.

NEWS-ONLY-ONCE Deliver the NEWS to a user only one time after it has been sent, without regard for how many times signon is completed and without regard for how many days The Network Director executes.

This ATTRIBUTE overrides the System Directory's indication that the NEWS has been delivered.

NON-REPEATING requests that the new password be checked for consecutive, identical characters and that any passwords with two or more consecutive identical characters be rejected.

This applies only to installations that have specified GLOBALS SECURITY=DIRECTOR.[7]

NO-PATTERNS indicates that any new password set by a network user may **not** be contained within the individual's userid or name.

The new password being requested by the terminal user is compared for the length of the requested password against the contiguous characters that make up the userid and name. If this check passes, any numeric digits in the requested password are removed and the NO-PATTERNS check is repeated. If both of these checks succeeds, the password passes the NO-PATTERNS validation.

This applies only to installations that have specified GLOBALS SECURITY=DIRECTOR.

RACFSTAT Indicates that The Network Director should cause RACF to update its statistics indicating that a specific user has logged on when accessing the system via The Network Director's RACROUTE interface logic. If this ATTRIBUTE is not specified, The Network Director will use RACROUTE STAT=NO to invoke RACF.

UPDATE-DIMMED indicates that any device that is dimmed as result of the DIM= operand should be *undimmed* to receive the dynamic status update.

---

[7] This is not the only new password validation that is performed. See NO-PATTERNS and "PSWD-OPTIONS" on page 56 for additional information about new password validation processes when SECURITY=DIRECTOR is in effect.

The dynamic status update will typically occur when The Network Director has an unsolicited message or information destined for the device (a BROADCAST command or an APPLICATION status change). If UPDATE-DIMMED is in effect, The Network Director will schedule a new DFB to the device to refresh the panel (the DIM interval will be restarted). If UPDATE-DIMMED is not in effect, the device will **not** receive notification of the BROADCAST message or APPLICATION status change when it is dimmed.

AUTHENTICATION

controls the characteristics associated with extended user validation (user validation in addition to the basic userid and password combination). Extended authentication also requires that an External File AIB be allocated prior to system access by the user. Please reference the *Network Operator's Guide* (TND-0210) for additional information about adding an AIB utilizing the SHOW processor.

Valid operands are:

EXT25 indicates that an installation exit (EXT25) must approve of any logon attempt prior to The Network Director granting access (providing a Application Selection Panel) to the user covered by this definition. EXT25 is entered as a portion of the LOGON validation routine and may operate in any fashion deemed appropriate by the installation. Terminal input and output is valid within the exit. A sample EXT25 is present on the distribution tape as the member, book, or file named TNDEXT25.

IntelliCARD indicates that the user covered by this definition must utilize IntelliCARD International's IntelliCARD device to obtain access to the system. Please refer to the IntelliCARD Interface manual (TND-0216) for more information.

NO this is the default and indicates that there will be no extended verification required (beyond userid and password).

SNK indicates that the user covered by this definition must utilize Digital Pathway's SecureNet Key device to obtain access to the system. Please refer to the SecureNet Key Interface Reference (TND-0226) for more information.

YES indicates that extended verification is necessary and the algorithm or device process required is defined by the contents of the External File (the AIB defined for the user).

AUTOLOGOFF

instructs The Network Director whether to automatically LOGOFF the User at this terminal when a User selects a subsystem. Valid settings for this operand are:

NO the default value indicates that The Network Director is to remember which user has logged on to the device and to bypass any automatic logoff logic

YES indicates that The Network Director is to logoff the user when the device returns to The Network Director from the subsystem

RETURN is the same as YES

SELECT requests that the terminal user be logged off at the same time as the device is forwarded to the subsystem

This is typically used when you can not be certain that the VTAM LU name will consistently identify the same physical device (as in the case of some protocol convertors, etc).

COMMANDS

controls whether The Network Director's Command Line will be present on the non-CUA Application Selection Panel (it is always present on the CUA Application Selection Panel) and provides some control over what commands can be issued from the Command line. You must specify YES if you would like a Command: line to appear on the Application Selection Panel. It is possible to authorize an extended command (like DROP, etc.) without specifying YES (the operator may issue the DROP command via TNDCMD or a PFKEY setting).

DISC indicates that the terminal operator may issue the DISConnect command to break the session between The Network Director and the terminal.

DROP is the same as DISC, but also generates an internal LOGOFF command for the network element (if it is logged on).

FLASH authorizes usage of the Command: line FLASH command to test the throughput characteristics of the device's connection to the domain operating The Network Director.

LOGON authorizes usage of the Command: line LOGON command as an alternative to modifying the appropriate Identification Area fields (Id: and Password:). If LOGON is not specified, the terminal user will not be able to logon using the keyword syntax and will be required to use the Identification Area.

NO indicates that the device should not have a Command: line on it

RESET applies only when The Network Director is executing in a VM/370 Virtual Machine and is the same as DISC, but includes a CP RESET command to return control of the device to CP.

YES authorizes the device for the Command: line, but does not authorize any of the "privileged" commands

CONNECT-MAXIMUM

specifies the maximum amount of time that a device can be connected to a single subsystem before The Network Director automatically logs of the device (within The Network Director only). This can be utilized to eliminate The Network Director "remembering" who was logged on when a terminal operator powers off his/her device while connected to a subsystem and goes home for the evening.

The Network Director keeps track of when a particular user has selected an application. If the CONNECT-MAXIMUM interval elapses prior to the device returning to The Network Director, it will be queued for autologoff upon return. NRS recommends that this value be set a a relatively large value (E.G. 8H or larger). A specification of zero (the default) disables the CONNECT-MAXIMUM logic.

CUA

The CUA operand indicates whether the network element(s) are to utilize the CUA interface for the initial signon and selection panels or not.

NO indicates to The Network Director that the network element(s) associated with this definition are to utilize the non-CUA Application Selection Panel

YES instructs The Network Director to utilize CUA terminal formatting principles to interact with the terminal user.

DIM

identifies the interval that a device connected to The Network Director **and** at its default panel that will be allowed to elapse prior to The Network Director clearing the screen. This is roughly equivalent to the hardware dim feature available on many of the newer devices and is intended to eliminate "burn in" of the LOGO screens on 3270 type devices.

A zero value (the default) disables the DIM logic. When dimmed, the terminal operator can get the panel restored by pressing any AID key.

Note: Due to the timing of The Network Director's dispatcher, the DIM operation may not occur exactly at the precise number of seconds specified. A delay may be introduced equivalent to the minimum interval specified on the GLOBALS TIMER= operand.

FORMAT-ID

controls the format of the bottom two lines of The Network Director's formatted non-CUA Application Selection Panel (the CUA Application Selection Panel always contains the function keys). Most of the non-CUA samples in this manual presume the default STANDARD format. The following figure identifies which FORMAT-ID contains which fields.

Field	Standard	Option1	Option2	Option3	Option4
LU	Yes	Yes	Yes	Yes	Yes
Id	Yes	Yes	No	Yes	Yes
Time	Yes	Yes	Yes	Yes	Yes
Date	Yes	Yes	Yes	Yes	Yes
Password	Yes	Yes	No	Yes	Yes
New Password	No	Yes	No	Yes	Yes
Extension	Yes	No	No	Yes	No
Account	Yes	No	No	No	Yes
Verify	No	Yes	No	Yes	Yes

Figure 12. Identification Area Format Combinations

The New Password: field is only meaningful when your installation is running one of the available security subsystems (RACF, TOP-SECRET, or ACF2). You also control the presence of the New Password field and Verify: field by the setting of the NEW-PSWD field (for OPTION1, OPTION3, and OPTION4).

IDENTIFICATION

controls the default operation of The Network Director when the terminal operator has not logged on.

NO the APPLICATIONS parameter on the DEFAULT statement or the TERMINAL statement is to be used as a standard default Application Selection Panel instead of the Identification prompt. The device will not be required to sign on first.

YES The terminal operator will have to identify himself prior to further processing.

ID-AREA

establishes whether members of this GROUP should have the ID-AREA displayed on their non-CUA Application Selection Panel (CUA panels do not make use of the ID-AREA).

NO do not include the ID area

YES include the ID area

ID-LOGO

is the operand that provides the simple graphic portrayal of the installation defined identifying information that will be displayed on any device that is **not** logged onto The Network Director **and** there is no specific TERMINAL or GROUP LOGO for the device.

After logon has been successfully accomplished, the LOGO operand will take effect. See the LOGO discussion for more information about the precise handling of the ID-LOGO operand.

LOGMODE-EDIT

controls whether or not a LOGMODE command issued by a terminal operator will be edited (INQUIRE SESSPARM) by The Network Director against the local domain VTAM's MODETAB. Cross domain environments may find that the edit operation will not produce a proper result as a function of the VTAM logic path associated with INQUIRE SESSPARM.

NO do not edit the LOGMODE value entered by the terminal operator

YES the "editing" should be done by The Network Director

LOGO

is the operand that provides the simple graphic portrayal of the installation defined identifying information. This information will be placed at the top of The Network Director's non-CUA Application Selection Panel.

See "LOGO" on page 13 for additional information about the options available to code the LOGO operand.

MESSAGES

identifies the message types that the network users will be authorized to Edit, Send, and Delete. Unless this operand enables one or more of these categories, the terminal user will only be able to View or Print messages sent to him/her.

BROADCASTS authorizes the network element to issue BROADCAST messages. This is typically restricted to authorized Network Administrators and the operator.

MEMOS authorizes the network element to create MEMOS

NONE indicates that this operator will not be authorized for any of the message types.

NOTES authorizes the network element to create NOTES

PASSWORD

is the 1 to 8 byte text string that is used during Network Director sign on to identify the terminal user as an authorized member of this group. As with other passwords, The Network Director will not print this on the output Print file.

YES will invoke the installation's security package to validate the password if GLOBALS SECURITY= was set on. If it was not, the text constant YES will be used as the password. The Wild Character may be used in the PASSWORD field. The password specification may be from 1 to 8 bytes and may contain wild characters. This password will be used when the operator attempting to identify himself does not have a password specification on his GROUP or USER statement. If this parameter is omitted, The Network Director will not require a Password from every operator.

PFKEYS

identifies the Program Function Key value that should be assigned to the DEFAULT APPLICATIONS for non-CUA Application Selection Panels. The first argument within the parends for each operand will be associated together, the second together, etc. If this operand is omitted and APPLICATIONS were defined, The Network Director will dynamically assign the function key values that will be used on the Application Selection Panel. See "PFKEY" on page 33 for additional information about how you can control the pfkey assignment process.

PROFILE

provides the general default for all network operator Profiles and their ability to view or change it. The first argument of this operand is the 1 to 8 byte name of the PROFILE definition that will establish the initial Profile.

The second portion controls whether the operator can VIEW the Profile (by issuing The Network Director's PROFILE command) or CHANGE it. A specification of NO instructs The Network Director to discard any attempt to Change or View the Profile.

PSWD-OPTIONS

When SECURITY=DIRECTOR is in effect, the PSWD-OPTIONS operand (a list of numeric values) controls the numeric specifications associated with The Network Director's internal password maintenance. Each PSWD-OPTION is a positional numeric value with the following meanings:

expiration establishes the maximum duration a password can be utilized without being updated. At the end of this interval, The Network Director will force the user through a password update prior to allowing access to the system. Default value is 30D. A value of zero (0) disables the expiration interval logic.

generations establishes the number of prior passwords that The Network Director will retain to insure that the terminal operator does not select the same password again. 10 (the default) is also the maximum that may be specified. The Network Director will automatically require that the terminal operator enter a new and different password from the prior generations unless this value is set to zero, which disables this validation.

minlength specifies the minimum length that is acceptable for a password. The Network Director will not allow a password that is shorter than this value. Specifying zero indicates that any length password is acceptable. The default is 4.

minwait specifies the minimum amount of time that must expire before The Network Director will allow a new password to be set. This is the minimum interval **between setting new passwords** that is acceptable to The Network Director. Zero (the default) indicates that The Network Director will accept any interval.

Each value can be specified utilizing any valid Network Director numeric specification (30D is "30 days", etc.). As an example:

```
DEFAULT PSWD-OPTIONS=(10D,6,5,2H)
```

This instructs The Network Director to force every user through setting a new password every 10 days, require that the new password does not match any of the last 6 for the user, must be at least 5 characters in length, and that at least 2 hours has elapsed since the last new password was set.

RECOVERY

Controls specific error recovery characteristics associated with individual device sessions within The Network Director. Valid operands are:

LOSTERM20 Indicates that The Network Director should respond to a LOSTERM reason code 20 by queuing a request for a session with the device forwarding the LOSTERM event. If not coded (the default condition), The Network Director will **not** queue a request for the device, which may result in some devices receiving ACF/VTAM's USSMSG10.

When coded, issuing the queued request against certain emulated devices or devices in VTAM error recovery may cause the queued work to stay on the VTAM Pending queue until the device restarts normally. This can create unnecessary VTAM messages and queue depths within ACF/VTAM.

SELECTIONS

establishes the manner in which the APPLICATIONS= specification on the TERMINAL, USER, GROUP, and DEFAULT definitions should be processed. See "SELECTIONS" on page 14 for details.

STATUS-INTERVAL

specifies the interval at which The Network Director will verify that a device forwarded to a subsystem is still in session with that subsystem. A zero value (the default) disables this check. The Network Director accomplishes the check by periodically issuing a D NET,ID=xxxx,E command for each device through the Program Operator interface to interrogate the status of the device. If the device is no longer connected to the subsystem, The Network Director will queue the device for autologoff **within The Network Director** or log the user off immediately (dependent upon ATTRIBUTES FORCE-LOGOFF) and disconnect the user logically from the APPLICATION.

Activation of this operand requires that GLOBALS VTAMOPER=YES is in effect.

There are also performance considerations associated with this operand. If The Network Director is issuing the internal D NET command very often, it is possible that the CPU consumption by both ACF/VTAM and The Network Director will become excessive. NRS recommends that this interval should be set to a value over 15M (15 minutes).

When the response is received from ACF/VTAM, The Network Director compares the connected subsystem name with the APPLICATION TARGET= value **for the number of characters that the TARGET is long**. This provides a mechanism to allow subsystems like TSO to be validated. The actual address space supporting the device will typically be suffixed with an additional qualifier (E.G. TSO00001, etc.).[8]

TIMEOUT

controls the number of seconds that The Network Director will allow an *authorized panel* to remain on the terminal without any activity prior to automatically logging off the operator. Activity is defined as any operator action (pressing a pfkey or entering data).

A value of zero (0) disables the timer. The Network Director will never time the operator out.

---

[8] The ACF/VTAM command used by The Network Director to establish the status will **not** operate as expected if the device and the subsystem are both cross domain resources. Therefore, if your installation makes use of cross domain resources, NRS recommends that you approach this function carefully and with a complete understanding of when the option will operate as expected and when it will not.

TRIES

specifies the number of consecutive erroneous attempts to logon that The Network Director will allow an operator to make before the terminal is placed on the inactive list. Once the terminal is on the inactive list, it will not be available for use within the network until the Network Administrator releases it.

A value of zero (0) disables this check. The Network Director will never place a terminal on the inactive list due to improperly attempting identification.

If your installation uses a system security package and the TRIES value is not zero, a *suspension* or *revocation* of the userid will cause The Network Director to automatically update the TRIES counter associated with the device to the TRIES value. This will cause the device to go inactive at the same time as the userid is held by the system security package.

WSF

This operand specifies whether The Network Director should attempt to utilize the 3270 Write Structured Field command Read Partition Query to interact with the device and collect device specific information (primarily the device's screen size or "usable area").[9]

COLOR indicates that The Network Director should **not** issue the Write Structured Field Read Partition Query, but **should assume** that the device supports the Extended Data Stream if the EDATS bit is on in the Bind image. If you specify EDATS in the BIND and WSF=COLOR for devices that are not capable of supporting the Start Field Extended 3270 order, the device may be susceptible to a variety of PROGnnn related problems.[10]

KEEP instructs The Network Director to retain the response to the Read Partition Query reply received from applicable devices in storage. The response is kept in the MX storage pool (above the 16 MB line in 31 bit capable systems) and is pointed to by the NIBRPQ field in the virtual NIB.

The SHOW NET= Administrator command can be utilized to view the hexadecimal values that were returned from the device during session initialization (select the RPQ Data field). WSF=KEEP is supported for debugging purposes and is not generally recommended for production usage on the entire terminal network.

---

[9] Any device with a X'03' (WSFQ) specified in the Bind image will automatically have the Read Partition Query done, regardless of the WSF setting.

[10] You can use the COLOR Command: line command to selectively determine which devices are capable, if you are unsure of the capabilities of your terminal devices. The COLOR command does not check the EDATS bit in the BIND image.

NO indicates that no Write Structured Field command should be utilized (regardless of the EDATS setting in the BIND image).

YES instructs The Network Director to use the logic if the device has the EDATS bit on in the BIND image that The Network Director retrieves from ACF/VTAM.

This operand is provided to eliminate potential communication errors on devices with the EDATS bit setting on in the BIND, but the device is incapable of responding to the Read Partition Query extended 3270 command. When scanning the definition control blocks, The Network Director will look for a WSF=YES specification on the TERMINALS definition first, then the GROUP definition, and finally the DEFAULT definitions. If WSF=YES is encountered at any point the scan is terminated. To control which specific devices will receive the WSF logic, specify DEFAULT WSF=NO to establish the general default and then WSF=YES on the TERMINAL (or TERMINAL GROUP=name) definition.

Examples

```
DEFAULT APPLICATIONS=(INFO,MESSAGES),
        TIMEOUT=3M,
        LOGO='Corporate Computing Facility'
```

The Network Director's standard INFO and Message Facility will be available to all users. Every authorized panel will be allowed to remain dormant for three minutes prior to being reset by The Network Director. The LOGO will be a simple phrase located on line two of the terminal panels.

Note that this example presumes that the applications named INFO and MESSAGES have been previously defined and are defining The Network Director provided facilities. The Network Director only reserves the special text strings associated with APPLICATION TARGET= operands. Therefore, INFO and/or MESSAGES could be used to define other application subsystems.

```
DEFAULT APPLICATIONS=(MESSAGES),
        PFKEYS=(PF2),
        PASSWORD=YES,
        TRIES=1,
        LOGO=


   **********       ***********       ***********
   ***                  ***               ***
   *****                ***               ***
   ***                  ***               ***
   **********           ***           ***********


LOGO-END
```

There is only a single default application. It appears to be the standard Network Director Message Facility and will be associated with the 3270 PFKEY 2 (if possible). Any operator attempting sign on will be required to provide a password that can be verified against the installation's security facility.

Any operator attempting to logon must provide a proper password on the first attempt or the terminal will be immediately placed on the inactive list.

The LOGO is made up of nine lines that utilize asterisks to graphically spell out the letters **ETI**, which will typically have a symbolic meaning assigned by the Network Administrator.

DIRECTORY

The DIRECTORY statement and its associated operands describe to The Network Director the internal System Directory that represents an individual user of the network. See "The System Directory" on page 242 for additional information about how the System Directory is utilized.

```
DIRECTORY
    userid
  [ DEPARTMENT=alpha-string ]
  [ GROUP=alpha-string ]
  [ INFORMATION=alpha-string ]
  [ NAME=alpha-string ]
  [ PHONE=alpha-string ]
```

Figure 13. The DIRECTORY Statement

The DIRECTORY statement allows the Network Administrator to generate an individual entry for usage in The Network Director's System Directory and can be utilized to provide information about the individuals that utilize the network.

userid

Identifies the specific userid that this directory entry applies to.

DEPARTMENT

Establishes the "department" code that the user belongs to. The DEPARTMENT operand may be from 1 to 8 characters long.

GROUP

Establishes the "group" or "division" that the user belongs to. GROUP may be from 1 to 8 characters long.

INFORMATION

Sets the 1 to 25 characters that are associated with the user and, generally, are used to describe information of significance for your installation. VMSECURE installations can set this field via usage of the *LO entry in the VM Directory.

NAME

Identifies the individual's name that will be using the associated userid (maximum of 20 characters).

PHONE

Establishes the individual's telephone number that uses the associated userid (maximum of 20 characters).

Example

As an example of how this can be coded in the Configuration Parameters, consider the following:

```
DIRECTORY SYS140,NAME='John Everyman',PHONE='(425) 814-9000',
            DEPARTMENT=SYSTEMS,
            INFORMATION='Building 40-A, Room 16'
```

This directory entry describes four elements (name, phone, department, and optional information) that will be held by The Network Director in the System Directory. It will be utilized during normal Network Director processing of subsystem selection, for resolution of system variables, and the information will be available to other users of the system via the DIRECTORY command.

GLOBALS

This definition provides information of a global nature to The Network Director for the purposes of controlling The Network Director's environment.

The format of the GLOBALS statement is:

```
GLOBALS

 [ ACCOUNT-TEXT={Account:|alpha text} ]
 [ ACCOUNTING=({SMR|SAR|TNDSAR}, ... ) ]
 [ ACTIVE-MAXIMUM={200|numeric value} ]
 [ ACTIVE-TEXT={Active|alpha text} ]
 [ APPLID={DIRECTOR|appl name} ]
 [ AUTHORIZATION=(numeric value, ... ) ]
 [ BROADCASTS=({STORAGE|DISK},{value|15M}) ]
 [ COMMAND-CHAR={NO|character} ]
   COLORS=(WD%,WR},WU!,DD ,TD$,TU\,BD+,BR{,GD@,YD¬,PD],RD¢) '
 [ CONSOLE={YES|NO} ]
 [ CP-MSGS={YES|NO} ]
 [ DATE-FORMAT={MM/DD/YY|DD/MM/YY}YY/MM/DD} ]
 [ DATE-TEXT={Date:|alpha text} ]
 [ DOWN-TEXT={Down|alpha text} ]
 [ DUMP={YES|NO|SDUMP} ]
 [ EVENTS=({ADMINCMD|APPLCNTS|APPLSTAT|INFOUPD|
            LOGON|LOGOFF|MSGDEL|MSGPRINT|MSGSEND|
            MSGVIEW|RETURN|SELECT|VTAMERRS}, ...) ]
 [ EXTENSION-TEXT={Extension:|alpha text} ]
 [ EXTERNAL-FILE={YES|NO} ]
 [ FOLD-PFKEYS={YES|NO} ]
 [ HELD-TEXT={Held|alpha text} ]
 [ ID-SIZE=8|numeric value} ]
 [ LINE-COUNT={60|numeric value} ]
 [ LOG={80|level} ]
 [ LOGON-MESSAGE={GENERAL|DETAIL} ]
 [ LOGSIZE={16K|numeric value} ]
 [ MEMOS=({STORAGE|DISK},{numeric value|5D}) ]
```

Figure 14. GLOBALS Statement Syntax (Part one)

```
GLOBALS

 [ MSGID={YES|NO} ]
 [ MSGS={YES|NO} ]
 [ NAME={alpha value|The Network Director} ]
 [ NETWORK-RETRIES={5|numeric value} ]
 [ NETWORK-WAITS=(normal,bid,signal,inquire,simlogon) ]
 [ NEW-PSWD={NO|YES|VERIFY|VALIDATE} ]
 [ NEW-PSWD-TEXT={New Password:|alpha text} ]
 [ NOTES=({STORAGE|DISK},{numeric value|3D}) ]
 [ NSI={YES|NO} ]
 [ OPSYS={VS1|MVS|DOSVSE|VM} ]
 [ PASSWORD=alpha value ]
 [ PASSWORD-TEXT={Password:|alpha text} ]
 [ PRINTERS={RETAIN|RELEASE} ]
 [ REACTIVATE={0|numeric value} ]
 [ RECOVERY={YES|NO} ]
 [ RPL-MAXIMUM={100|numeric value} ]
 [ RPLS={2|numeric value} ]
 [ SECURITY={ACF2|RACF|DIRECTOR|TOPSECRET|VM|NONE} ]
 [ SECURITY-SVC=0|numeric value} ]
 [ SITE=alpha value ]
 [ SMF={0|SMF record number} ]
 [ STORAGE-BALANCE=({50|numeric value}, {50|numeric value}) ]
 [ STORAGE-POOLS=({8K|numeric}, {8K|numeric},24K|numeric)
 [ SWAP={YES|NO} ]
 [ SYNTAX-SCAN={YES|NO} ]
 [ TERMINATE={AUTO|OPERATOR|RETRY} ]
 [ TIME-TEXT={Time:|alpha text} ]
 [ TRANSLATE={LOWER|UPPER} ]
 [ TIMER=({15S|numeric value}, {1M|numeric value}) ]
 [ TRACE={0|numeric value} ]
 [ VERIFY-TEXT={Verify:|alpha text} ]
 [ VMSECURE=alpha value ]
 [ VSAM-PASSWORD=alpha value ]
 [ VTAMOPER={YES|NO} ]
 [ WARN-DAYS={5|numeric value} ]
 [ WTO={0|level} ]
```

Figure 15. GLOBALS Statement Syntax (Part two)

ACCOUNT-TEXT

is the 1 to 8 character constant that will be used to display the title of the Account field in the Identification Area of The Network Director's panels.

ACCOUNTING

specifies the type of account record generation that The Network Director will produce. It is possible to specify more that one type (dependent upon the operating system). The actual events that are recorded is controlled by the EVENTS= keyword. The types and their supported environments are:

SAR requests the SAR format, which are written to SMF in OS systems (SMF= must be specified) or using DIAGNOSE X'4C' in VM/GCS systems (the ACCT option in the VM directory must be specified)

SMR requests the SMR format, which are written to OS SMF (SMF= must be specified)

TNDSAR requests the SAR format, with the output produced out a standard external file definition (OS DD Statement TNDSAR, GCS FILEDEF TNDSAR, or DOS SYSPCH)

The Network Director does not provide any protection for space difficulties. That is the external medium containing the accounting records must be able to hold all the records that may be produced. If it is not, The Network Director may be susceptible to abnormal termination (dependent upon the operating environment and recording media). For this reason, NRS generally recommends that OS systems utilize SMF, GCS systems utilize the VM accounting (DIAGNOSE) option, and DOS system define SYSPCH as a POWER spool file.

ACTIVE-MAXIMUM

The ACTIVE-MAXIMUM operand specifies the number of concurrent DFBs (internal dispatchable elements) that will be allowed to be active prior to entering a Network Director slowdown condition. An active DFB is defined as an attached portion of work that is not in a "long wait" (as an example, a timed terminal wait).

Once the ACTIVE-MAXIMUM is hit, The Network Director will enter the slowdown condition (exactly the same as when RPL-MAXIMUM is encountered) and will eliminate the slowdown when a sufficient number of currently active DFBs terminate to bring the active DFB count below the ACTIVE-MAXIMUM.

This operand is intended to provide an additional "governor" to manage the maximum amount of work that The Network Director can handle during peak periods (in addition to RPL-MAXIMUM). The two MAXIMUMs work independently to determine if slowdown conditions have been encountered. However, once slowdown is entered, the treatment by The Network Director is the same, regardless of which operand triggered the slowdown. In essence, enough work must complete to bring the count below the operand value that caused the slowdown. ACTIVE-MAXIMUM is useful where a large

volume of devices return to The Network Director all at the same time during normal execution (a major subsystem abends, during initialization, etc.).

ACTIVE-TEXT

is the 1 to 6 character constant that will be used to display in the Status area of an individual selection item on a non-CUA Application Selection Panel that is available for selection, but has no or cannot be assigned a PFKEY value.

APPLID

is the 1 to 8 byte name that The Network Director should use to identify itself to VTAM with. This is the APPLID set up within VTAM on the APPL statement for The Network Director to use. If terminals will be LOGAPPLed to The Network Director, this is that name.

If this operand is not provided, The Network Director will attempt to use the text *DIRECTOR* as its APPLID.

AUTHORIZATION

is the numeric coded value that authorizes your installation to execute The Network Director. You may specify up to 5 numeric values, which **must contain** at least one authorization value that enables The Network Director to operate or The Network Director will terminate with an abend code of 142.[11]

BROADCASTS

controls the characteristics of the Message Facility's Broadcast messages. The first argument controls the queueing technique used for Broadcast messages. STORAGE implies that the Broadcast message will be kept in main storage and not on DISK. Any Broadcasts in process during termination (normal or abnormal) will be lost.

The second argument specifies the default expiration interval for Broadcast messages. This interval begins when the message is Sent. After the time interval has elapsed the message will be automatically Deleted by The Network Director.

---

[11] If your installation is using a "CPUID based" AUTHORIZATION value in MVS, The Network Director will have to execute as an APF authorized program.

COLORS

The COLORS operand provides a mechanism to select and set the extended attributes associated with the special characters that have been utilized to implement full color support (see "Color Support" on page 237 for a full discussion of color support).

Each value in the GLOBALS COLORS operand sets the characteristics for one of the special symbols in the format "xys", where "x" is a single letter equating to the **color**, "y" is a single letter equating to the **extended attribute**, and "s" is the **symbol** that will be used to select the color characteristics.

The following letters set the color characteristic for the special symbols (the first character of each COLORS operand):

B Blue
D Default for the device (normally, green)
G Green
N No color setting (the special character will not be utilized as an extended attribute)
P Pink
R Red
T Turquoise
W White
Y Yellow

The following letters set the extended attribute characteristic for the special symbols (the second character of each COLORS operand):

B Blink
D Default (no extended attribute)
R Reverse video
U Underline

The sequence of the COLORS operands match precisely the order of the special symbols as listed in Figure 83 on page 237).

COMMAND-CHAR

identifies the single character that will precede any Network Director commands that will be entered on the Command line of the Application Selection Panel. This option allows installation control over how The Network Director parses the Command Line's input. COMMAND-CHAR can be utilized by the terminal operator to explicitly invoke a Command (such as LOGOFF, DISC, etc). This eliminates any difficulties associated with an installation where the application name and an internal command have the same text value.

NO there will not be any character required to recognize a command.

character the specified character will be required to identify a "command"

CONSOLE

controls whether The Network Director will initiate operator communications via OS QEDIT or DOS PUT.

NO The Network Director will not establish operator communications. All operator commands, etc targeted for The Network Director must then be entered from a valid Network Administrator's terminal.

YES The Network Director will establish operator communications as provided for within the operating system

CP-MSGS

This operand controls whether The Network Director should process incoming IUCV SMSG and/or MSG interrupts as Network Administrator commands or not. This operand may be utilized when The Network Director is operating in a GCS environment.

NO do not service incoming IUCV interrupts as Network Administration commands

YES The Network Director will attach an additional DFB identified as SMSG, which will utilize the appropriate IUCV facilities to intercept SMSG and MSG messages (dependent upon which CP SET operands you utilize).

The Network Director will then deal with incoming messages as if they originated from a Network Administrator's command line. Responses to the incoming command are routed back to the issuing virtual machine by CP MSGNOH as they are placed into the standard LOG.

Incoming messages are identified to The Network Director by the issuing virtual machine name. To determine if the issuing machine is authorized, The Network Director will first look to see if a user with the same id is currently logged on to The Network Director. If he is, then the currently authorized selections are scanned for access to the TNDADMIN application (Network Administration). If present, the command is processed. If TNDADMIN is not present, the request is rejected by the SMSG DFB.

If The Network Director cannot locate a currently logged on user with the same virtual machine name, it will then scan the current TERMINAL definitions for a match (wild characters are valid). If a match is located, the APPLICATIONS= string is checked for access to TNDADMIN. If present, the incoming command is processed. If TNDADMIN is not present, the command is rejected.

To activate the interface, simply code GLOBALS CP-MSGS=YES in The Network Director's parameters and use the appropriate CP facilities to SET SMSG IUCV (SET MSG IUCV may also be utilized). Other authorized virtual machines will then be able to communicate with The Network Director via SMSG. As an example:

```
CP SMSG DIRECTOR DISPLAY NET=T001
```

will cause the command **DISPLAY NET=T001** to be transmitted to the virtual machine named DIRECTOR. If the virtual machine is operating a Network Director with

CP-MSGS=YES specified and the issuing virtual machine has proper authorization for Network Administration, the responses to the DISPLAY command will be returned to the issuing virtual machine.

Normally, The Network Director will also return The Network Director message numbers along with the replies to the query. To enhance the usability of the interface, any responses to The Network Director's VTAM command will have the TND0347G portion eliminated. You may issue **any** valid Network Administration line command (full screen commands are not supported), including the VTAM and VM commands.

DATE-FORMAT

specifies the format that will be utilized to display dates within The Network Director. This includes the lower right hand corner of Network Director panels as well as the display format for any DISPLAY commands.

MM/DD/YY the default format, which is month followed by day followed by year

DD/MM/YY day followed by month followed by year

YY/MM/DD year followed by month followed by day

DATE-TEXT

is the 1 to 5 character constant that will be used to display the Date field title in the Identification area.

DOWN-TEXT

is the 1 to 6 character constant that will be displayed in a Selection Status field on a non-CUA Application Selection Panel when the associated APPLICATION is unavailable.

DUMP

controls whether The Network Director will take a dump during Recovery processing. This is only effective when RECOVERY=YES is in effect.

NO do not take a dump when processing through error recovery

YES allow a dump to be taken prior to continuing processing

SDUMP for MVS or GCS operating environments, The Network Director will utilize the SDUMP SVC to produce a dump of the address space or virtual machine when a DUMP is necessary. The Network Director will require APF Authorization to issue the SDUMP SVC and properly generate the system dump.

The resulting dump will be placed into the MVS defined system dump data sets or the GCS Recovery Machine's reader. It will be capable of being processed by the proper IPCS routines for the applicable operating system.

The dump will receive a title in the form of The Network Director message number 350 in the general form of:

```
S[code] in &JOBNAME &VERS at [csect]+[offset] - PSW [psw value]
```

where:

code is the interrupt code that is associated with the interrupt (S0C4, etc.).

&JOBNAME is the OS Address space name or VM Virtual Machine name of The Network Director's execution environment.

&VERS is the version of The Network Director currently operating.

csect is the internal Network Director CSECT name extracted from the value in R10. This value may not be set correctly if the interrupt occurred with a value in R10 (the normal Network Director base register) that does not properly address a Network Director CSECT.

offset is the computed offset in the CSECT where the interrupt occurred. This may be invalid if R10 was not correct.

psw value is the full 64 bit PSW extracted from the SDWA at entry to the recovery routines.

EVENTS

indicates which SMR (System Measurement Records) or SAR (System Accounting Records) that should be recorded during The Network Director's execution. The recording is an *event recording* process that indicates a particular activity has occurred.

The available operands and their basic contents are:

ADMINCMD a Network Administrator has just issued a command

APPLCNTS the application monitor interval has expired (hourly, at the top of the hour) and the number of network elements in session with each APPLICATION is being recorded

APPLSTAT a defined APPLICATION just changed status

INFOUPD a network user has just modified a portion of the Information Facility

LOGON a network user attempted to logon to The Network Director

LOGOFF a network user has just logged off of The Network Director

MSGDEL a network user just deleted a Network Director message from the Message Facility

MSGPRINT a message facility message was just printed

MSGSEND a network user just sent a message facility message

MSGVIEW a network user just looked at the contents of a Message Facility message that was sent to him

RETURN a network user has just returned from a subsystem

SELECT a network user has just selected a subsystem

VTAMERRS a non zero type return code was received from ACF/VTAM

See "Event Recording" on page 184 for additional information about the contents of the accounting records.

EXTENSION-TEXT

is the 1 to 10 character constant that will be displayed as the title for the Extension field (when used) in the Identification Area of The Network Director's panels.

EXTERNAL-FILE

indicates whether The Network Director should attempt to open the External FIle (YES) or not (NO). This is particularly useful in operating system environments where The Network Director will not receive control back from VSAM in the event of an error (file not allocated, etc.).

FOLD-PFKEYS

indicates if The Network Director should logically "fold" pfkey values on the Application Selection Panel or not.

YES indicates that pfkeys with values greater than 12 will be automatically translated to less than 12 (keys with value less than 12 will have 12 added to them) and selection evaluation will proceed again (presuming there is no selection with a value equal to the higher pfkey value).

NO indicates that the pfkey values will not be translated.

HELD-TEXT

is the 1 to 6 character constant that will be displayed in the status area of a Selection item if the Selection item is in the Held status (a Network Administrator HOLD command).

ID-SIZE

indicates the maximum size userid that will be collected by The Network Director in the Id area of non-CUA panels. The default of 8 is also the maximum value that may be set. This parameter is generally used to cause the Id: data entry field in the Id area to be set smaller to automatically tab to the next field when the last character of the userid has been entered.

LINE-COUNT

is the number of lines on each output page of the Print file. After this number of lines, The Network Director will cause a page eject. This file is typically routed to an OS Sysout class or DOS SYSLST.

LOG

controls the level of message activity that will be available to the Network Administrator for LOG Viewing. Each message within The Network Director is assigned a numeric *class level* If the message has a value equal to or less that the LOG value, it will be collected into the storage LOG queue and will be reproduced onto the output printer LOG. See the Messages and Codes Manual for more explanation of the message levels.

LOGON-MESSAGE

controls the level of detail The Network Director will provide to a terminal operator attempting to logon to The Network Director.

DETAIL indicates that detailed messages be presented to the terminal operator informing him why the logon failed.

GENERAL indicates that The Network Director should **not** give the terminal operator extended information about why a logon attempt has failed.

When GENERAL is in effect, The Network Director will always respond with Message 220 indicating that "Your attempt to logon is not currently valid". This is done regardless of why the logon attempt actually failed. The actual reason for failure is reflected in the LOG for inspection by an authorized Network Administrator. This option is available to provide maximum protection for an installation concerned about intruders. The Network Director will not "help" an intruder by informing him that the ID is correct, but the password is wrong.

However, if you would like additional assistance for the terminal operators during the logon process, specifying DETAIL will provide the terminal operator with more detailed information about why the logon process is failing. For RACF and TOP-SECRET/MVS installations, the return code produced by RACINIT is interpreted by The Network Director. ACF2 shops will receive the actual ACF2 originated messages in the message area. TopSecret/VM installations will receive the actual TopSecret/VM originated messages. VMSECURE installations will receive messages from either VMSECURE or TNDVMS.

LOGSIZE

specifies the amount of main storage that will be used to store The Network Director's LOG for viewing at a Network Administrator's terminal. This storage is managed as a circular queue and will wrap around on itself when it is filled, overlaying the oldest information first.

The LOG messages are maintained within the storage queue in a manner that allows each message to be represented by approximately 60 bytes. This results in each 4K segment containing approximately 70 message entries. The size that should be allocated for this LOG area is dependent upon the amount of messages being logged (the GLOBALS LOG= operand) and the desired number of messages the Network Administrator would like to have available for viewing online.

MEMOS

controls the characteristics of the Message Facility's Memo messages. The first argument controls the queueing technique used for Memo messages. STORAGE implies that the Memo message will be kept in main storage and not on DISK. Any Memos in process during termination (normal or abnormal) will be lost unless DISK queuing is selected.

The second argument specifies the default expiration interval for Memo messages. This interval begins when the message is Sent. After the time interval has elapsed the message will be automatically Deleted by The Network Director.

MSGID

NO excludes the internal identification for which CSECT and DFB issued the message

YES causes The Network Director to include text identifying the DFB issuing the message on the output log (TNDLOG). The MSGID fields are:

DFB Name Columns 101 to 116 of the output line contains the internal name of the DFB that issued the message.

CSECT Columns 118 to 122 contains the right most 5 bytes of the internal Network Director CSECT name that issued the message

Address Columns 124 to 131 contains the hexadecimal address of the virtual storage location that holds the Dispatchable Function Block (DFB) that issued the message

MSGS

NO causes The Network Director's message numbers to be omitted from the text display on the terminal operator's device.

YES indicates that the end user should receive The Network Director's internal message number along with the rest of the message text.

NAME

is the character string that will be used at the top of individual Network Director panels (Message Edit, INFO, etc) in the Title Area to identify The Network Director. It may not exceed 24 characters.

NETWORK-RETRIES

Specifies the number of consecutive attempts (defaults to 5) that The Network Director will try when attempting to place output on a single device or establish a session successfully with a single device. If the device continues to send error responses back, The Network Director will place it onto the Inactive List for *input errors*. The device will be eligible for automatic release when it successfully sends in "input". (Devices placed on the Inactive List for "iteration counter" or "security" reasons are not eligible for automatic release).

NETWORK-WAITS

While processing session traffic between The Network Director and network devices, many ACF/VTAM based operations are initiated. Some of these operations have *timers* associated with them that represent a *timeout* condition within The Network Director. These intervals control how long The Network Director will wait before taking an error recovery action. NETWORK-WAITS allows the installation to control the values associated with these timed waits. This operand is a positionally significant, list type operand with a total of 5 entries in the form:

```
NETWORK-WAITS=(normal,bid,signal,inquire,simlogon)
```

where:

WAIT Type	Default	Meaning
normal	30S	standard wait time interval
bid	30S	wait for BID response
signal	15S	wait for response to SIGNAL
inquire	1M	wait for INQUIRE APPSTAT
simlogon	10S	acquire wait interval (RPLEXIT)

Note: Any operand value that is less than 5S will be forced to 5S (the minimum value acceptable).

NEW-PSWD

specifies how The Network Director should deal with the ability to set a new password This is only active when an installation security package is specified via the SECURITY= operand.

NO indicates that The Network Director is not to allow the terminal operator to set a new password during the logon process. Any attempt to do so will result in an error message. A NO setting will cause the New Password: field to be eliminated from the Identification area.

YES indicates that the setting of new passwords is to be allowed.

VERIFY indicates that the new password set must be also entered into the Verify: field of the Identification area (available when FORMAT-ID=OPTION1, 3, or 4 is in effect). This option allows the terminal operator to enter the new password twice on the same panel and reduces the number of operators that will type the new password incorrectly. If the two "new password" fields do not match exactly, The Network Director will reject the logon attempt with an appropriate message and ask the terminal operator to try it again

VALIDATE indicates that the new password set must be entered again in response to a prompt that will be presented by The Network Director VALIDATE differs from VERIFY in that VERIFY allows the terminal operator to enter the new password twice on the initial panel and with a single ENTER key. VALIDATE will require that the operator key the new password twice and with two separate ENTER keys.

NEW-PSWD-TEXT

is the 1 to 13 character constant that will be displayed in the Identification Area where the New Password field is displayed.

NOTES

controls the characteristics of the Message Facility's Note messages. The first argument controls the queueing technique used for Note messages. STORAGE implies that the Note messages will be kept in main storage and not on DISK. Any Notes in process during termination (normal or abnormal) will be lost unless DISK queuing is selected.

The second argument specifies the default expiration interval for Note messages. This interval begins when the message is Sent. After the time interval has elapsed the message will be automatically Deleted by The Network Director.

NSI

controls whether The Network Director will respond to requests entering via the Network System Interface.

NO NSI originated requests should be rejected

YES NSI originated requests should be accepted (if possible)

OPSYS

is the operating environment that The Network Director will be executing in.

DOSVSE indicates that The Network Director will be operating in a DOS environment (including VCNA under DOS).

MVS indicates an OS/VS2 system, MVS/SP, MVS/XA, or MVS/ESA operating system

VS1 indicates an OS/VS1 system (including VCNA under OS)

VM indicates The Network Director will operate in a VM/GCS virtual machine

PASSWORD

is the 1 to 8 byte alphanumeric string that represents the VTAM password that The Network Director should use when identifying itself to VTAM. This corresponds to the VTAM PRTCT= operand specified on the APPL definition statement. The Network Director recognizes the importance of keeping the PASSWORD secured and will not print its value on any output listing.

PASSWORD-TEXT

is the 1 to 9 character constant that will be displayed in the Identification Area of non-CUA panels where the Password field is entered.

PRINTERS

controls whether The Network Director should stay in session with 3286 type printers when finished printing on them or not. The Network Director will always release the printer when requested by another subsystem that has asked for it via RELREQ procedures.

RELEASE indicates The Network Director should automatically break the session with a printer that was acquired for Printing purposes

RETAIN indicates The Network Director should continue the session with the printer until another subsystem requests it

REACTIVATE

Specifies the numeric value that represents the number of seconds between "automatic releases" of devices placed on the Inactive List for "input errors", "bid failures", or "iteration counter" reasons. Devices that are inactive for security violations, operator HOLD commands, or other internal Network Director reasons will **not** be automatically RELEASEd.

REACTIVATE can aid in the unattended operation of a Network Director node that has periodic "failures" amongst the network (control unit power outage, etc.). When set to a reasonable value, REACTIVATE can be utilized to reduce the number of calls to the Help Desk by automatically retrying inactive devices.

Specifying a value of zero (0) disables the automatic reactivation of inactive devices. Care should be exercised when setting a reactivation interval so that The Network Director is not forced into continual recovery logic on sessions associated with devices that are truly in a non functioning status.

RECOVERY

identifies whether The Network Director will execute with the ability to intercept and recover from internal program checks.

YES indicates that the appropriate STAE, ESTAE, or STXIT is to be issued and any DFB related task suffering a program check should be isolated to the specific terminal creating the abend situation.

NO indicates that the recovery environment is not to be established, which will cause the entire Network Director to abend when a program check is encountered.

RPL-MAXIMUM

indicates the number of active RPLs that The Network Director will allow to become active before slowing down The Network Director's internal dispatching.

This will have the effect of "slowing down" The Network Director, until VTAM has had an opportunity to "catch up". This condition typically arises during The Network Director's initialization. VTAM will begin establishing sessions with The Network Director at a fairly quick rate, but the potential exists for The Network Director to create requests for VTAM at a rate that can create difficulty for the access methods.

RPL-MAXIMUM has the effect of slowing down how many concurrent operations that The Network Director will initiate before giving VTAM time to complete some of the previous work. This can be used to avoid flooding NCPs, etc.

RPLS

is the numeric value representing the number of VTAM RECEIVE-ANY RPLS that The Network Director should attempt to keep active. This will effect the speed with which VTAM can notify The Network Director of a terminal interaction. If unspecified, The Network Director will default to 2.

The RPLS value **must** be smaller than RPL-MAXIMUM. In fact, it should be much smaller. A typical installation should be capable of supporting large amounts of throughput with the default of 2 RECEIVE-ANY RPLS. The Network Director dynamically generates RPLs as necessary to satisfy output (SEND) type operations, etc. RPLS= controls only the number of RECEIVE-ANYs maintained as *active*

SECURITY

identifies the installation's installed standard security package. This controls the manner with which The Network Director will validate individual operator's Passwords for any USER, GROUP, or DEFAULT with a PASSWORD=YES specification.

ACF2 represents The Access Control Facility, a product of Computer Associates. When this option is selected The Network Director will invoke ACF2 through its standard interface or SVC. The password entered by the user will be validated against the ACF2 Password data base. Note that The Network Director will require the ACF2 MUSASS attribute.

DIRECTOR specifies that The Network Director will validate user passwords against a set of rules and procedures identified in "DIRECTOR" on page 210. Essentially, all password maintenance will be performed by The Network Director in conjunction with the terminal user and the Network Administrator. The user will be required to change his/her password on a regular basis (see "PSWD-OPTIONS" on page 56) and it will have to conform to one or more installation selected algorithms (see "ATTRIBUTES" on page 47).

NONE indicates that no system security package will be utilized

RACF The Network Director will invoke the security package via the documented RACROUTE macro. When this option is selected, The Network Director will either have to execute authorized or be defined to RACF as an authorized caller.

TOPSECRET The Network Director will invoke the security package via the documented RACINIT macro. When this option is selected, The Network Director will have to execute authorized and be a defined TOPSECRET facility.

VM instructs The Network Director to utilize DIAGNOSE X'84' to validate the userid and password against the VM Directory

SECURITY-SVC

establishes the SVC number that is to be used to communicate with the installation security package. If SECURITY=ACF2 is in effect, this number should be the TYPE=A SVC number (normally, 221 for OS based systems). This operand is **not** required for ACF2 installations. The Network Director will automatically locate the proper SVC number from the ACCVT. However, if SECURITY-SVC is specified, it will be utilized by The Network Director.

SITE

is the logical name for this Site that is operating The Network Director. This operand is only useful when The Network Director is operating in an environment where multiple Network Director's are interacting with each other via LU-LU communications. A single domain Network Director can set this value, but it will be primarily for comment type purposes.

This value can be symbolically placed into a LOGO by the specification of the LOGO variable &SITE. See "Variables" on page 16 for more information.

If there are any SITES defined, the Editor will enable the Site: field on the Editor panel and any attempt to save a message will require that a corresponding SITE definition be present. You should include in your network definitions a SITE definition for your own installation (this will allow you to control which message targets that are allowable via the NETWORK-ELEMENTS operand of the SITE definition).

SMF

establishes the SMF record number that will be written by The Network Director for recording statistical information. The exact format for the record is discussed on "Event Recording" on page 184. A value of zero (0) indicates that The Network Director should not write any SMF records.

STORAGE-BALANCE

establishes the ratio at which The Network Director will release operating system storage back to the operating system (FREEMAIN or FREEVIS).

The first value specifies the numeric value for The Network Director's MX storage pool and the second value specifies the numeric value for the TP storage pool. The numeric values can be thought of as a percentage of storage that was acquired to handle the *peak processing period*. If the current total allocated pages for the specific storage pool exceeds the percentage of the high water mark achieved since initialization, then unallocated pool elements are released (if available for release).

STORAGE-BALANCE=(50,50) is the default and specifies that The Network Director should retain approximately 50% of the storage that was required to handle the peak processing requirement (normally established during initialization).

Consult the *Internals* manual for a further description of how this storage management algorithm operates.

STORAGE-POOLS

The Network Director divides all dynamically obtained storage into one of three storage pools called the CB, MX, and TP pools. Each pool is further divided into General Storage Elements (GSAs), which are then suballocated as necessary to satisfy internal storage requests. The STORAGE-POOLS operand allows the installation to control the specific size (rounded up to a 4K increment) of the GSA element for each pool.

The first operand specifies the CB pool element size, the second the MX pool element size, and the third the TP pool element size. STORAGE-POOLS=(8K,8K,24K) is the default. The default values and values in effect in an operational Network Director may **not** be reduced, but may be increased.

Additional information about the storage pools, storage concepts, and the impact of modifying the default sizes is available in the Internals manual. For most installations, the default values should be appropriate.

SWAP

instructs The Network Director on how to manage the MVS non-swappable characteristic.

NO indicates The Network Director should issue the SYSEVENT TRANSWAP macro to affect the swappable characteristic and mark itself non-swappable (APF authorization is required to accomplish this function).

YES The Network Director should not issue the SYSEVENT TRANSWAP macro. When YES is in effect, it is still possible to mark The Network Director non-swappable via the standard MVS facilities (IEAPPTxx, etc).

SYNTAX-SCAN

controls whether The Network Director will try to initialize the VTAM interface.

YES after parsing the initialization parameters, The Network Director should simply terminate

NO after parsing the initialization deck, The Network Director should open the VTAM ACB and begin operations

TERMINATE

controls the manner in which The Network Director should terminate when ACF/VTAM is not available or terminates. If VTAM should require The Network Director to CLOSE its ACB, The Network Director will do so. However, if TERMINATE=OPERATOR is in effect, The Network Director will wait until the console operator has issued a command to either STOP or to open the VTAM ACB again (OPEN TAM).

AUTO specifies that The Network Director should terminate immediately if VTAM fails, abends, is not currently active, or simply attempts to exit the system.

OPERATOR specifies that The Network Director should only terminate if the computer operator or Network Administrator has requested it.

RETRY causes The Network Director to retry a failed VTAM OPEN on a timed basis. If RETRY is specified and the VTAM OPEN fails (due to ACF/VTAM not active yet, an improper ACB name, ACF/VTAM abnormal termination, etc.), The Network Director will continue to execute within the operating system.[12] The ACF/VTAM OPEN operation will be rescheduled each dispatch interval (the second value in the GLOBALS TIMER= operand, which defaults to 1 minute).

This option is intended to allow The Network Director and ACF/VTAM's initialization processes to be scheduled without an interrelationship. If

---

[12] With TERMINATE=RETRY specified, the Network Administrator or console operator will be required to issue a STOP command to get The Network Director to terminate (simple VTAM termination will not cause The Network Director to exit the operating system).

ACF/VTAM is fully initialized before The Network Director OPENs the ACB, the OPEN will succeed and The Network Director will begin management of appropriate network devices. If The Network Director initializes before ACF/VTAM, TERMINATE=AUTO causes The Network Director to simply terminate execution. TERMINATE=OPERATOR causes The Network Director to wait for a console generated OPEN TAM request. TERMINATE=RETRY causes The Network Director to **automatically** generate an OPEN TAM request periodically.

TIME-TEXT

is the 1 to 5 character constant that will be displayed in the lower right hand portion of the Identification Area of non-CUA panels as a description of the Time of Day.

TRANSLATE

indicates whether The Network Director should automatically translate the output TNDLOG or SYSLST information to upper case or not. This is provided to aid at those installations without printer support for lower case information.

LOWER generated output should retain the upper **and** lower case default characteristics

UPPER generated output should be translated to all upper case characters

TIMER

controls the wait interval within The Network Director. The second time interval is the maximum time interval The Network Director will wait between interrogation of the current status of the VTAM application subsystems.

The first time interval specifies the minimum number of seconds The Network Director will require before dispatching the internal monitoring function.

The Network Director will enter a long Wait when it has no work to do. The timer interval it will wait for is dependent upon the current DFB mix, but will never be longer that the maximum TIMER value. If The Network Director is dispatched by the operating system (due to terminal input, etc) and the minimum number of seconds has elapsed, The Network Director will dispatch the internal monitor function and reset its timer to the maximum value.

This mechanism reduces the overall swap characteristics in a MVS environment and allows The Network Director to monitor the application environment more often during active periods within the network and less often when the network is idle.

TRACE

controls whether the internal Network Director trace facility is on or off. A zero value specifies that the trace is off. A non zero value turns it on and specifies the amount of storage that will be used to contain trace entries.

VERIFY-TEXT

is the 1 to 7 character constant that will be displayed in the lower line of the Identification Area of non-CUA panels as a field to verify that the new password entered is what was intended. This field will appear only if FORMAT-ID=OPTION1, 3, or 4 and NEW-PSWD=VERIFY is specified.

VMSECURE

allows any installation operating VM Software's VMSECURE to set the name of the virtual machine that The Network Director is to communicate with for validation of VMSECURE based operations that are beyond the capability of DIAGNOSE X'A0'. This includes all the TNDVMS based operations, which are utilized to implement a full function VMSECURE interface.

This operand can be from 1 to 8 characters and is utilized as a value for CP SMSG requests to the VMSECURE machine.

VSAM-PASSWORD

is the value that will be used when opening the External File as the VSAM Password. If not present, The Network Director will assume that there is no security associated with the External File.

VTAMOPER

identifies whether The Network Director's Program Operator facility is to be active or not.

NO The Network Director should not initialize the Program Operator interface (the Network Administrator will not be able to issue VTAM commands and the STATUS-INTERVAL operand and RESET command will not operate).

YES The Network Director should attempt to initialize the Program Operator interface (AUTH=SPO is required on the VTAM APPL definition).

WARN-DAYS

The WARN-DAYS operand provides a mechanism to set the number of days prior to password expiration that a user should receive a warning message indicating that the password will expire. WARN-DAYS defaults to 5, but may be specified as a numeric value up to 32,767.

WARN-DAYS is effective only for installations that also have SECURITY=VMSECURE or SECURITY=DIRECTOR specified and have properly installed TNDVMS. WARN-DAYS causes a Network Director based message to be issued to the terminal operator each time a logon is successful and the password expiration is within the specified number of days.

WTO

controls the level of information that will be written to the operator's console by The Network Director. Any messages that are issued with a value equal to or less than the WTO value will be immediately written to the operator's console. Refer to the *Messages and Codes* manual to establish the meanings for the various message levels.

The Network Director will also always write any messages to the console that are solicited by the console (commands or statements that are entered from the operator's console).

Examples

```
GLOBALS APPLID=NRSTND,
        NOTES=(STORAGE,1H),
        TIMER=(30S,2M),
        SECURITY-SVC=222,
        SECURITY=ACF2
```

The Network Director will use the text string NRSTND in its VTAM ACB to identify itself to VTAM. Application status will be checked every 2 minutes (or more often if a terminal user in the network is active). The security package named ACF2 will be utilized to validate any User id/Password combination and it can be communicated with via SVC 222.

The Message Facility will queue all Notes in main storage and will automatically Delete the Notes after 1 hour.

```
GLOBALS  PASSWORD=SECRET,
         LINE-COUNT=48,
         NAME='Seattle Data Center',
         NSI=NO,
         WTO=40,
         RPLS=6
```

The Network Director should continue to use its default of DIRECTOR for a VTAM APPLID and it should use the password SECRET when attempting to OPEN its ACB. The Network Director's output Print file will receive a page eject sequence every 48 output lines. There will be six VTAM Receive Any RPLS active during normal Network Director processing. The Title Area will contain the text *Seattle Data Center* in appropriate locations instead of *The Network Director*.

The Network System Interface has been disabled. Any attempt to use it will be rejected with a *NSI is Disallowed* response.

The operator's console will receive any message assigned Message Class 40 or lower, which includes any internal errors or operator reply type messages.

GROUP

This definition identifies the characteristics of a single logical grouping of users. It defines the attributes associated with a collection of individuals that will be referenced to this definition via the GROUP= operand on another statement (TERMINAL or USER).

The format of the GROUP statement is:

```
GROUP

    group-name
    [ ACQUIRE={NO|SELECT} ]
    [ APPLICATIONS=(application name, ...) ]
    [ ATTRIBUTES=({NEWS-CREATION,NO-NEWS,NEWS-ALL-LOGON,
                   NEWS-ONLY-ONCE}, ... )
    [ AUTHENTICATION={NO|YES|EXT25|INTELLICARD|SNK} ]
    [ AUTOLOGOFF={NO|YES|RETURN|SELECT} ]
    [ COMMANDS={(YES|NO|DISC|DROP|FLASH|LOGON|RESET}, ... ) ]
    [ CONFIDENTIAL={YES|NO} ]
    [ CUA={NO|YES} ]
    [ DAYS=(day specification, ...) ]
    [ DIM={0|numeric value} ]
    [ FORMAT-ID={STANDARD|OPTIONx} ]
    [ IDENTIFICATION={NO|YES} ]
    [ ID-AREA={YES|NO} ]
    [ LOGO=group logo ]
    [ MAXIMUM=numeric value ]
    [ MESSAGES=({NOTES|MEMOS|BROADCASTS|NONE} )]
    [ NETWORK-ELEMENTS=(alpha value, ... ) ]
    [ PASSWORD={alpha text|YES} ]
    [ PFKEYS=(application 1, ...) ]
    [ PROFILE=(profile name,{VIEW|CHANGE|NO}) ]
    [ PSWD-OPTIONS=(expiration,generations,minlength,minwait) ]
    [ SELECTIONS=D+(T&U)|{D|T|U}[{+|&}{D|T|U}[{+|&}{D|T|U}]]
    [ STATUS-INTERVAL={0|numeric value} ]
    [ TERMINALS=(terminal name, ...) ]
    [ TRIES={0|numeric value} ]
    [ TIMES=(time specification, ...) ]
    [ TIMEOUT={0|numeric value} ]
    [ WSF={COLOR|NO|YES|KEEP} ]
```

Figure 16. GROUP Syntax

group name

establishes the name of the GROUP (wild characters are acceptable). This name will be utilized later as the value on one or more GROUP= operands on TERMINAL or USER definition statements. This group name can also be utilized to Send messages to.

ACQUIRE

Identifies whether The Network Director should queue a request (SIMLOGON) for a network element that selects a subsystem

NO no queued SIMLOGON request will be issued

SELECT each time a device is sent to an APPLICATION, The Network Director will issue the appropriate VTAM functions to cause the device to be returned immediately upon terminating the session with the APPLICATION.

ACQUIRE=SELECT is also useful when The Network Director forwarding the device to the subsystem is in a *remote* system to the device owning Network Director (a cross domain Network Director). It will cause the device to return to the "last" Network Director that had control of the device.

APPLICATIONS

identifies the set of logical applications that this GROUP will have placed upon its Application Selection Panel. Each of the applications must have been previously defined via a Network Director APPLICATION statement. If the APPLICATIONS operand is omitted, the GROUP will have only the DEFAULT APPLICATIONS available to it.

ATTRIBUTES

The ATTRIBUTES operand indicates specific processing characteristics associated with a network element that is associated with the corresponding definition element. The Network Director will utilize the ATTRIBUTES operand that is related to the "most detailed" definition element that applies to the network element.

Valid settings are:

NEWS-ALL-LOGONS the NEWS panel should be delivered to the applicable network elements every time a user logs on to the system

NEWS-CREATION the related network elements are authorized to create the NEWS message

NEWS-ONLY-ONCE the NEWS panel will be delivered to each unique user only one time (this requires the presence of the External File for tracking across executions of The Network Director)

If you set this ATTRIBUTE on a GROUP definition, it must be the default GROUP for the network element (TERMINAL or USER) or the NEWS characteristic will not operate.

NO-NEWS the NEWS message is not to be delivered to a network element associated with the definition

AUTHENTICATION

controls the characteristics associated with extended user validation (user validation in addition to the basic userid and password combination). Extended authentication also requires that an External File AIB be allocated prior to system access by the user. Please reference the *Network Operator's Guide* (TND-0210) for additional information about adding an AIB utilizing the SHOW processor.

Valid operands are:

EXT25 indicates that an installation exit (EXT25) must approve of any logon attempt prior to The Network Director granting access (providing a Application Selection Panel) to the user covered by this definition.

IntelliCARD indicates that the user covered by this definition must utilize IntelliCARD International's IntelliCARD device to obtain access to the system. Please refer to the *IntelliCARD Interface* manual (TND-0216) for more information.

NO this is the default and indicates that there will be no extended verification required (beyond userid and password).

SNK indicates that the user covered by this definition must utilize Digital Pathway's SecureNet Key device to obtain access to the system. Please refer to the SecureNet Key Interface Reference (TND-0226) for more information.

YES indicates that extended verification is necessary and the algorithm or device process required is defined by the contents of the External File (the AIB defined for the user).

AUTOLOGOFF

instructs The Network Director whether to automatically LOGOFF the User at this terminal when a User selects a subsystem Valid setting for this operand are:

NO the default value indicates that The Network Director is to remember which user has logged on to the device and to bypass any automatic logoff logic

YES indicates that The Network Director is to logoff the user when the device returns to The Network Director from the subsystem

RETURN is the same as YES

SELECT requests that the terminal user be logged off at the same time as the device is forwarded to the subsystem

This is typically used when you can not be certain that the VTAM LU name will consistently identify the same physical device (as in the case of some protocol convertors, etc).

COMMANDS

controls whether or not this Group will have the Command Line present on its Application Selection Panel (non-CUA users only). YES specifies that it will and NO indicates that it should not be present. DROP, DISC, LOGON, and RESET authorize the activities associated with those commands. See "COMMANDS" on page 51 for more information.

CONFIDENTIAL

For TERMINALS connected to this GROUP, indicates whether the transmissions are to be confidential or not.

NO will allow the VTAM trace to contain the data that is sent on the session between the device and The Network Director.

YES will cause trace entries for the session to have the data suppressed

CUA

The CUA operand indicates whether members of this GROUP are to utilize the CUA interface for the initial signon and selection panels or not.

NO indicates to The Network Director that the GROUP members are to utilize the non-CUA Application Selection Panel

YES instructs The Network Director to utilize CUA terminal formatting principles to interact with the terminal user.

DAYS

describes the days of the week that the GROUP is allowed to be active within The Network Director. See the DAY description under "Day Specification" on page 6 for more information. The default is for the GROUP to be always authorized for access to The Network Director.

DIM

specifies the interval after which The Network Director will automatically clear the device's screen. The DIM interval applies only to devices in their default condition (not logged on). A value of zero indicates that no DIM logic will be utilized.

FORMAT-ID

controls the format of the bottom two lines of The Network Director's formatted non-CUA Application Selection Panels. Additional information about specific options is available in "FORMAT-ID" on page 53.

IDENTIFICATION

controls whether the usage of devices connected to this GROUP will require a signon or not

NO a user at the device is not required to signon to utilize the system

YES devices will be prompted with the Identification panel. The terminal operator will have to identify himself prior to further processing.

ID-AREA

establishes whether members of this GROUP should have the ID-AREA displayed on their Network Director non-CUA panels.

NO do not include the ID area

YES include the ID area

If The Network Director encounters an ID-AREA=YES specification at a TERMINAL or USER level first, it will take precedence over the GROUP specification.

LOGO

is the operand that provides the simple graphic portrayal of the installation defined identifying information. This information will be placed at the top of The Network Director's non-CUA Application Selection Panel for members of this Group.

See "LOGO" on page 13 for additional information about the options available to code the LOGO operand.

MAXIMUM

establishes the maximum number of times an individual user that is connected to this GROUP may logon to The Network Director.

MESSAGES

controls the type of messages this GROUP may Edit, Send, and Delete within the Message Facility. NONE indicates that this operator will not be authorized for any of the message types.

NETWORK-ELEMENTS

establishes a list of network element patterns that can be considered as members of this GROUP. Messages sent to this GROUP will be individually delivered by The Network Director to each network element whose identifier matches at least one of the NETWORK-ELEMENT patterns.

PASSWORD

is the 1 to 8 byte text string that is used during Network Director sign on to identify the terminal user as an authorized member of this group. As with other passwords, The Network Director will not print this on the output Print file.

YES will invoke the installation's security package to validate the password if GLOBALS SECURITY= was set on. If it was not, the text constant YES will be used as the password. The Wild Character may be used in the PASSWORD field.

PFKEYS

are the program function key values that should be associated with the APPLICATION selections. The Network Director will automatically assign values if the PFKEYS parameter is left out. The keyword NO may be used to prohibit PFKEY assignment. See "PFKEY" on page 33 for additional information about how you can control the pfkey assignment process.

PROFILE

identifies this GROUP's default Profile. The profile name is the text name for the PROFILE statement that sets the Profile's values. The second argument controls the level at which this GROUP can change its Profile.

PSWD-OPTIONS

When SECURITY=DIRECTOR is in effect, the PSWD-OPTIONS operand (a list of numeric values) controls the numeric specifications associated with The Network Director's internal password maintenance. Each PSWD-OPTION is a positional numeric value with the following meanings:

expiration establishes the maximum duration a password can be utilized without being updated. At the end of this interval, The Network Director will force the user through a password update prior to allowing access to the system. Default value is 30D.

generations establishes the number of prior passwords that The Network Director will retain to insure that the terminal operator does not select the same password again. 10 (the default) is also the maximum that may be specified. The Network Director will automatically require that the terminal operator enter a new and different password from the prior generations unless this value is set to zero, which disables this validation.

minlength specifies the minimum length that is acceptable for a password. The Network Director will not allow a password that is shorter than this value. Specifying zero indicates that any length password is acceptable. The default is 4.

minwait specifies the minimum amount of time that must expire before The Network Director will allow a new password to be set. This is the minimum interval **between setting new passwords** that is acceptable to The Network Director. Zero (the default) indicates that The Network Director will accept any interval.

SELECTIONS

establishes the manner in which the APPLICATIONS= specification on the TERMINAL, USER, GROUP, and DEFAULT definitions should be processed. See "SELECTIONS" on page 14 for details.

STATUS-INTERVAL

specifies the interval at which The Network Director will verify that a device forwarded to a subsystem is still in session with that subsystem. See "STATUS-INTERVAL" on page 58 for more information.

TERMINALS

identifies the physical terminals that a user defined as a member of this GROUP may be entered from. Each entry in the list may be specified using the Wild Character.

TIMES

is the time of day specification that this GROUP is allowed access to The Network Director. See the discussion under the TIME parameter for the APPLICATION statement for more specifics on how to specify the TIME. If omitted, the GROUP is always allowed access based upon the time of day check. The time specification format is discussed in detail under "Time Specification" on page 5.

TRIES

specifies the number of consecutive, erroneous attempts to logon that The Network Director will allow a terminal operator to make before the device is placed on the Inactive List for security violations. See "TRIES" on page 59 for additional information.

TIMEOUT

is the number of seconds that a terminal logged on as a member of this GROUP will have to operate on an authorized Network Director panel before it is reset to its default condition.

WSF

controls whether The Network Director will use the 3270 Read Partition Query command to establish the characteristics of the device. See "WSF" on page 59 for more information about how this operates.

Examples

```
GROUP     PAYROLL,APPLICATIONS=(PAYABLE,PERSON,PAYROLL),
                  PASSWORD=ADMIN+++,
                  DAYS=(MONDAY-FRIDAY)
```

Members of this GROUP will have on its Application Selection Panel at least three application subsystems (PAYABLE, PERSON, and PAYROLL). The Network Director will assign the program function keys. Access to The Network Director from this GROUP may only be accomplished on the normal week days and the terminal user will have to know that the password must start with ADMIN before being presented with a Application Selection Panel.

```
GROUP    WAREHSE,APPLICATIONS=(WARES,STOCK),
                 PASSWORD=YES,
                 TERMINALS=(INV+++++,SPAD0),
                 PROFILE=(INV,NO)
```

The GROUP named WAREHSE has access to two application systems. The password used will be validated by the installation security package. This GROUP's operators must utilize the terminals whose names begin with the characters INV or from the single terminal SPAD0. The GROUP's Profile is assigned defaults according to the INV PROFILE statement and it can not be modified or viewed by the GROUP.

```
GROUP    MGRS,NETWORK-ELEMENTS=(TS++++++,SYSTEMS)
```

Any message (BROADCAST, MEMO, or NOTE) sent to the GROUP MGRS will be individually delivered to the userid SYSTEMS or any device or user whose id begins with the letters *TS*.

KEYS

LU1 devices utilize a great variety of key sequences to indicate particular 3270 functions to the host. The Network Director recognizes that each device may be different and has provided a KEYS definition statement to allow each installation (and each device user) control over which key sequences represent what activity.

The KEYS definitions may also be SAVEd, RELOADed, and processed via the SHOW command. The KEYS definitions described in the following figure are distributed on the standard External File under the name of NRSKEYS and can be RELOADed for use by issuing a RELOAD KEYS,NAME=NRSKEYS either from Network Administration or in the Configuration Parameters.

The KEYS definition is associated with a particular TERMINAL or USER in the PROFILE operand and has the following format:

```
KEYS

    name
  [ BACKSPACE=alpha value ]
  [ BKSPACE=alpha value ]
  [ CLEAR=alpha value ]
  [ CLRSCRN=alpha value ]
  [ CONTROL=alpha value ]
  [ ENTER=alpha value ]
  [ ESCAPE=alpha value ]
  [ PAn=alpha value ]
  [ PFnn=alpha value ]
```

Figure 17. KEYS Statement Format

name

is the 1 to 8 character "name" associated with the KEYS definitions that follow

BACKSPACE

establishes the character that represents a backspace operation (the backspace key on the keyboard)

BKSPACE

establishes the character that, when preceded by an ESCAPE character, represents a backspace operation

CLEAR

identifies the character received by The Network Director when a CLEAR key has been struck

CLRSCRN

identifies the string that, when preceded by an ESCAPE character, indicates that a CLEAR function has been done

CONTROL

is the control character used by some devices as an alternate to the ESCAPE character

ENTER

identifies the character that represents the ENTER key

ESCAPE

establishes the escape character

PAn

identifies the sequence that, when prefixed with ESCAPE, indicates that a particular PA key was struck (PA1, PA2, and PA3 are valid operands)

Standard KEYS Definitions

The following standard key definitions are provided as samples:

Device	IBM3101	IBM3161	VT100	VT52	VT220	ADDS	HAZEL	HAZ1500	BEEHIVE	DGD210	HP2621B
CLEAR	03		03	03	03	03	03	03	03	0C	03
BACKSPACE	02	16	16	16	02	3D	16	16	16	19	16
BKSPACE	C4	C4	C4	C4	C4						C4
CLRSCRN	D3	D3					1C	1C			
ENTER	0D	0D	0D	0D	0D	0D	0D	0D	0D	25	0D
ESCAPE	27	27	27	27	27	27	27	27	27	27	27
PA1	A4	94	6B	6B		6B	6B	6B	40	6B	6B
PA2	A5	95	4B	4B		4B	4B	4B	4F	4B	4B
PA3	A6	96	61	61		61	61	61	7F	61	61
PF01	81	F1	F1	F1	98	F1	F1	F1	97	98	97
PF02	82	F2	F2	F2	99	F2	F2	F2	98	99	98
PF03	83	F3	F3	F3	A2	F3	F3	F3	99	A2	99
PF04	84	F4	F4	F4	A3	F4	F4	F4	A2	A3	A2
PF05	85	F5	F5	F5	A4	F5	F5	F5	A3	A4	A3
PF06	86	F6	F6	F6	A5	F6	F6	F6	A4	A5	A4
PF07	87	F7	F7	F7	A6	F7	F7	F7	A5	A6	A5
PF08	88	F8	F8	F8	A7	F8	F8	F8	A6	A7	A6
PF09	89	F9	F9	F9	A8	F9	F9	F9	A7	A8	F9
PF10	91	F0	F0	F0	D7	F0	F0	F0	A8	A9	F0
PF11	60	60	60	60	D8	60	60	60	A9	C0	60
PF12	7E	7E	7E	7E	D9	7E	7E	5F	C0	6A	7E
PF13	7F	81	4F	4F		4F	4F	4F	6A	D0	4F
PF14	7C	82	7C	7C		7C	7C	7F	D0	A1	7C
PF15	7B	83	7B	7B		7B	7B	7B	A1	97	7B
PF16	5B	84	5B	5B		5B	5B	5B	07	81	5B
PF17	6C	85	6C	6C		6C	6C	6C	87	82	6C
PF18	5F	86	5F	5F		5F	5F	50	7E	83	5F
PF19	50	87	50	50		50	50	7D	F4	84	50
PF20	5C	88	5C	5C		5C	5C	4D	F5	85	5C
PF21	4D	89	4D	4D		4D	4D	5D	F6	86	4D

Device	IBM3101	IBM3161	VT100	VT52	VT220	ADDS	HAZEL	HAZ1500	BEEHIVE	DGD210	HP2621B
PF22	5D	91	5D	5D		5D	5D	6A	F7	87	5D
PF23	6D	92	6D	6D		6D	6D	7E	50	88	6D
PF24	4E	93	4E	4E		4E	4E	25	F0	89	4E

Figure 18. Standard LU1 Key Definitions

PROFILE

This definition establishes default values for a Profile or the CUA user's initial Options settings that can be referenced by multiple USERS and/or TERMINALS. It defines the attributes associated with processing within The Network Director. If authorized through proper use of the PROFILE Operand on other Statements, the terminal operator can modify the contents of this Profile for individual use.

The Network Director will always maintain a separate Profile for each unique entity within the network. If multiple Users are referenced to the same PROFILE definition as each modifies the Profile, The Network Director will automatically replicate it for the user prior to any modification.

The format of the PROFILE statement is:

```
PROFILE

   profile name
   [ ACCOUNT=alpha value ]
   [ ALARM={YES|NO} ]
   [ CMDLINE={BOTTOM|TOP) ]
   [ COLOR={COLOR|MONOCHROME) ]
   [ EDIT-KEYS=(pfkey value, ... ) ]
   [ FKEYS={LONG|SHORT) ]
   [ KEYS=alpha value ]
   [ MSGID={OFF|ON) ]
   [ PANELID={OFF|ON) ]
   [ PA1={PROFILE|PA1 value} ]
   [ PA2={PA2 value} ]
   [ PA3={PA3 value} ]
   [ PARMS=(alpha value, ... ) ]
   [ PRINTER=alpha value ]
   [ ROOM=alpha value ]
```

Figure 19. PROFILE Syntax

profile name

is the 1 to 8 character identifier for this Profile. This is the name that will be used in PROFILE= operands on the other definition statements.

ACCOUNT

sets the default value for the ACCOUNT field in the Identification Area. If ACCOUNT=ACF2 is in effect for this profile, the actual account value will be set as discussed under "Account Code Validation" on page 209.

ALARM

establishes the initial condition for the Profile user's 3270 alarm feature. The Network Director will attempt to activate the ALARM when a Broadcast Message is sent or an application on the Application Selection Panel changes status.

NO indicates that The Network Director should not attempt to activate the alarm

YES indicates that The Network Director should continue to attempt to activate the alarm

CMDLINE

The CMDLINE operand controls where the Command ===> prompt appears on the various Network Director CUA based panels.

TOP requests that The Network Director position the Command line after the panel title line and before the panel body

BOTTOM indicates that the Command line will appear near the bottom of each Network Director panel, immediately before the function key area.

COLOR

The COLOR operand controls whether The Network Director will produce extended colors on properly equipped devices in CUA mode or not.

COLOR requests that The Network Director attempt to use the 3270 Start Field Extended orders to display and set the field characteristics on Network Director output panels.

MONOCHROME indicates that The Network Director should use only the basic 3270 Start Field and corresponding attributes to construct output panels.

This operand cannot enable COLOR support for devices that are not properly configured to respond to the Read Partition Query properly. It only sets the desired characteristic associated with the session.

EDIT-KEYS

initializes The Network Director's Program Function Key values. The pfkey values are positional within this operand and each must be specified up to the highest valued key that you would like to assign (up to and including PF12).

FKEYS

The FKEYS operand indicates to The Network Director the format that the CUA function key area will be displayed in.

LONG requests that The Network Director display as many basic function key settings as possible that apply to the current panel

SHORT instructs The Network Director to display in the function key area only the "primary" functions that are available on the panel

KEYS

specifies the 1 to 8 character name of the KEYS definition statement that will be used for any network elements that connect to this PROFILE with an LU1 type device (non-3270 data stream device).

MSGID

The MSGID operand controls whether The Network Director internal message number should be displayed in error messages.

OFF requests that only the text portion of The Network Director's messages be displayed to the terminal operator.

ON indicates that The Network Director should include the TNDnnnn message number prefix on all output messages.

PANELID

The PANELID operand controls whether The Network Director's internal panel identification is to be displayed in the title line on CUA panels.

OFF instructs The Network Director to suppress the panel identifier and to place the installation name on the panels where the panelid would appear.

ON requests that The Network Director include the internal panel identification on each output panel generated by The Network Director. This is useful when attempting to isolate problems and communicate to others the panel you are currently using.

PA1

sets a command to be associated with the PA1 key, that will be executed when the key is struck by the terminal operator.

PA2

sets a command to be associated with the PA2 key, that will be executed when the key is struck by the terminal operator.

PA3

sets a command to be associated with the PA3 key, that will be executed when the key is struck by the terminal operator.

PARMS

establishes values to be utilized as optional parameters to be associated with the network users connected to this profile. These items can be utilized as additional parameters to be passed to the APPLICATIONs, or other uses as determined by your local requirements. As an example, at least one installation has defined the first PARM as the location for entering the network operators full name, which is then passed to a Electronic Mail system for processing (when that selection is made).

PRINTER

sets the value for the VTAM terminal that will receive Messages for this Profile that are Printed via the Message Facility's Print Action Code.

ROOM

is used to set the default value for the 8 byte alphanumeric value that will be used by the Message Facility to identify messages that have been Printed. This field can be used to route the hardcopy results of a Print Action Code within your organization.

Examples

```
PROFILE      TEST,PRINTER=INVPRT01,
                  ROOM=I405
```

This Profile has accepted all the defaults for the Message Editor's PFKEYS. It has also directed the Message Facility to route all Printed Messages for this Profile's users to the printer named INVPRT01 and label them with the "Room number" of I405.

```
PROFILE      SAMPLE,PA1=LOGOFF,PA2=MONITOR,
             EDIT-KEYS=(HELP,SPLIT,END,QUIT,LOCATE,CHANGE,
                        UP,DOWN,FORMAT,PREFIX,RESET,RETRIEVE),
                  PARMS='HELP COMPANY SCHEDULE'
```

This Profile has set the PA1 key to simulate the LOGOFF command, the PA2 key to issue the Network Administrator's command MONITOR, redefines the basic function keys, and has set the first optional parameter at a value that could be provided to the INFO facility to automatically place the terminal operator at a location in INFO that could display the computer schedule.

The resulting individual PROFILE panel would look like the following figure.

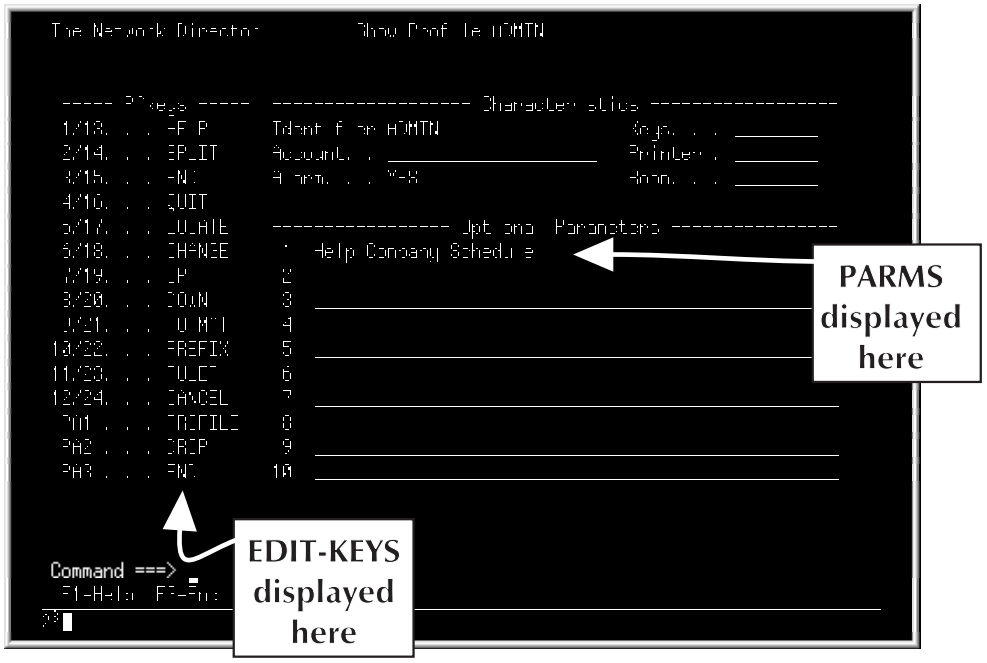


Figure 20. Sample PROFILE Panel

RESOURCE

The **RESOURCE** statement provides a general purpose mechanism to define "formats" or definition elements for use within The Network Director's environment.

```
RESOURCE

   resource-name
   DATA=
 [ TITLE=resource description ]
```

Figure 21. The RESOURCE Statement

where:

resource-name

establishes the 1 to 8 character identifier that will be associated with this "resource". This is the name that is used in other locations within The Network Director to make reference to the following DATA.

DATA

provides the character string that will be identified within The Network Director by the defined resource name.

TITLE

Identifies the 1 to 30 character description of the RESOURCE being defined. It is simply a manner to use an extended description for the RESOURCE to simplify subsequent RESOURCE management via the SHOW processor.

Example

The RESOURCE statement provides a generalized mechanism that can be used to reduce repetitive tasks and provide external definitions for the configuration of The Network Director.

The Network Director can make use of the RESOURCE statement as an alternative for identifying the LOGO definition. As an example, assume the following Configuration Parameters:

```
DEFAULT  IDENTIFICATION=NO
GROUP    SYSTEMS,APPLICATIONS=(TSO,CMS,CICS)
TERMINAL T01+++,AUTOLOGOFF=YES,LOGO=
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
*                                                                         *
*                    Sample LOGO                                          *
*                                                                         *
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
USERS    TECH++,GROUP=SYSTEMS,LOGO=
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
*                                                                         *
*                    Sample LOGO                                          *
*                                                                         *
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
```

The Network Director allows the LOGO to be specified in a GROUP and then reference the TERMINAL and USER definitions to the GROUP (in order to eliminate the requirement to repeat the LOGO). An example of this is:

```
DEFAULT  IDENTIFICATION=NO
GROUP    SYSTEMS,APPLICATIONS=(TSO,CMS,CICS),LOGO=
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
*                                                                         *
*                    Sample LOGO                                          *
*                                                                         *
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
TERMINAL T01+++,AUTOLOGOFF=YES,GROUP=SYSTEMS
USERS    TECH++,GROUP=SYSTEMS
```

This works well for some locations, but can create a problem in others. As with our example, this may authorize APPLICATIONS TSO, etc. for a TERMINAL that should not receive it.

The RESOURCE statement provides a mechanism within the Configuration Parameters to specify a RESOURCE name in the LOGO= operand. This allows the Network Administrator to have a single LOGO, but without requiring that the TERMINAL definition pick up the other characteristics associated with the GROUP definition. Our example would now look like this:

```
DEFAULT  IDENTIFICATION=NO
RESOURCE MAINLOGO,DATA=
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
*                                                                         *
*                    Sample LOGO                                          *
*                                                                         *
* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - *
DATA-END
GROUP    SYSTEMS,APPLICATIONS=(TSO,CMS,CICS)
TERMINAL T01+++,AUTOLOGOFF=YES,LOGO=MAINLOGO
USERS    TECH++,GROUP=SYSTEMS,LOGO=MAINLOGO
```

Generalized RESOURCEs

The Network Director contains multiple RESOURCEs that can be used to locally customize various aspects of The Network Director. Each of the elements is defined and manipulated via the RESOURCE definition, either in the Configuration Parameters or online via SHOW RESOURCE.

The elements typically affect a single portion of The Network Director's panels or operations. As an example, the following Application Selection Panel has two areas that can be set via the RESOURCE definition process.

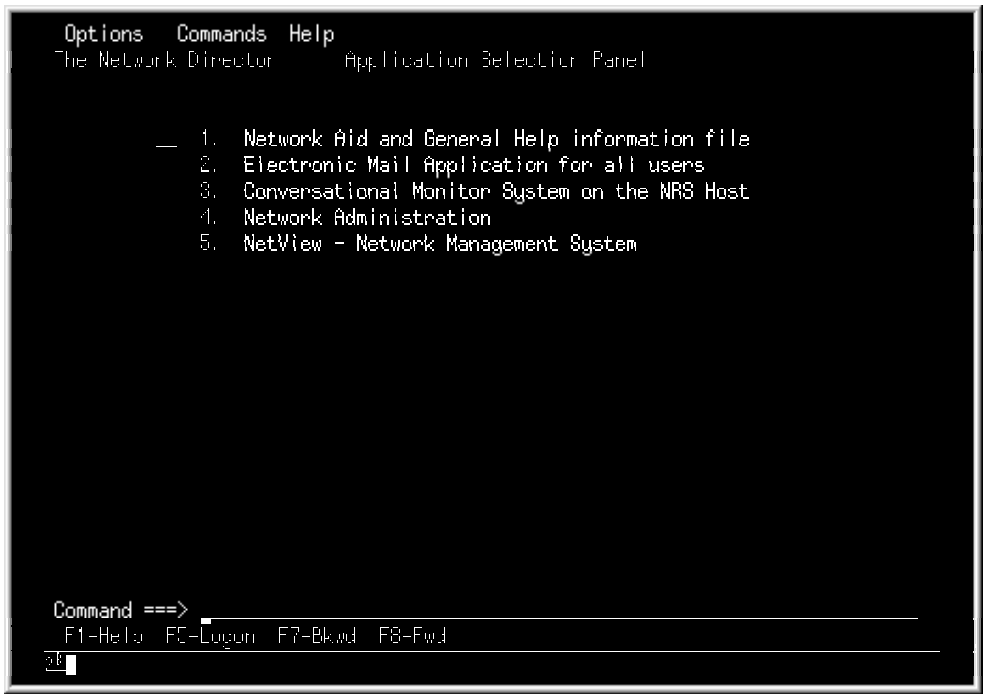


Figure 22. Generalized RESOURCE Usage

Thus, to supply an alternative for a customizable element (as discussed in the following sections), simply define a RESOURCE by the same name as identified.

The default values for all the following RESOURCEs are identified in the examples listed after each item using Configuration Parameters syntax.

CUAASP

The **CUAASP** resource defines the 1 to 30 character string that will be used as the title for the CUA Application Selection Panel. The default is:

```
RESOURCE CUAASP,DATA='Application Selection Panel'
```

CUAIDP

The **CUAIDP** resource defines the 1 to 30 character string that will be used as the title for the CUA based Identification Panel. This is the panel that is presented to a CUA=YES based device prior to signon for IDENTIFICATION=YES installations.

```
RESOURCE CUAIDP,DATA='Identification Panel'
```

KEYSADMN

The **KEYSADMN** resource defines the function key area contents for the Network Administration panel (TNDADMIN). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSADMN,TITLE='Network Administration Function Keys',DATA=
F1=Help  F3=End  F5=Locate  F7=Bkwd  F8=Fwd  F10=Prefix  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSEDIT

The **KEYSEDIT** resource defines the function key area contents for The Network Director's general purpose Editor (Message Facility and Info Editor). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSEDIT,TITLE='Editor Function Keys',DATA=
F1=Help  F2=Split  F3=End  F5=Locate  F6=Change  F7=Bkwd  F8=Fwd  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSINFO

The **KEYSINFO** resource defines the function key area contents for the Info or Help panels (TNDINFO). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSINFO,TITLE='Information Panel Function Keys',DATA=
F1=Help  F3=End  F7=Bkwd  F8=Fwd  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSMSG

The **KEYSMSG** resource defines the function key area contents for the Primary Messages Menu (TNDMSG). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSMSG,TITLE='Primary Messages Function Keys',DATA=
F1=Help  F3=End  F7=Bkwd  F8=Fwd  F9=Create F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSPROF

The **KEYSPROF** resource defines the function key area contents for the Profile display panel (TNDSHPDE). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSPROF,TITLE='Profile Function Keys',DATA=
F1=Help  F3=End  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSSCOL

The **KEYSSCOL** resource defines the function key area contents for the SHOW Element processor panel (TNDSHCOL). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSSCOL,TITLE='Show Subprocessor Function Keys',DATA=
F1=Help  F3=End  F7=Bkwd  F8=Fwd  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSSCRN

The **KEYSSCRN** resource defines the function key area contents that is used if no other function arrangement is in effect. Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSSCRN,TITLE='Default Function Keys',DATA=
F1=Help  F3=End  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSSEL

The **KEYSSEL** resource defines the function key area contents for the Application Selection Panel when the device is in CUA mode (CUA=YES). Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSSEL,TITLE='CUA Selection Panel Function Keys',DATA=
F1=Help  F5=Logon  F7=Bkwd  F8=Fwd
F1=Help  F5=Logon
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

KEYSSHOW

The **KEYSSHOW** resource defines the function key area contents for most of the SHOW processor and associated panels. Both the long and the short form can be defined (the short form is only used when CUA=YES is in effect and the terminal user has selected it via the Options action).

```
RESOURCE KEYSSHOW,TITLE='SHOW Function Keys',DATA=
F1=Help  F3=End  F5=Locate  F7=Bkwd  F8=Fwd  F12=Cancel
F1=Help  F3=End  F12=Cancel
DATA-END
```

The first line (80 characters) defines the primary or long form of the function keys and the second line the short form.

SHOWANE

The **SHOWANE** resource defines the format that the SHOW Network-elements panel will be in.

```
RESOURCE showane,TITLE='Show Network Elements format',DATA=
Terminal    User     Status        Name             Telephone
&TERM   &NAME   &ANESTAT &USER-NAME(a)       &USER-PHONE(a)
DATA-END
```

The first line (80 characters) defines the "title" line for the panel. The second line provides the actual data that will be inserted in each line (one line for each Network Element processed).

SHOWDIR

The **SHOWDIR** resource defines the specific format that the SHOW DIRECTORY panel will contain.

```
RESOURCE SHOWDIR,TITLE='Show Director format',DATA=
     User    Group    Status        Name         Telephone          News
&DIRGRP. &DIRSTAT &USER-NAME(a)    &USER-PHONE(a)  &NWS
DATA-END
```

The first line (80 characters) defines the "title" line for the panel. The second line provides the actual data that will be inserted in each line (one line for each Directory entry). If you change the variables that are used, make sure that you select items that are available from the individual DIR entry.

SITE

This definition identifies the characteristics of a network node that is operating as a single installation (for the purposes of networking). Typically, a SITE definition is provided for each ACF/VTAM Domain that is operating a Network Director. The SITE definition provides a name for, and a path to the other domain.

The SITE definition is utilized to define a path between multiple Network Director's. Each Network Director can then communicate with the other via the defined path. This is used for several purposes. An example would be the transmission of a message created via the Message Facility intended for a network user located at a different "site" within the computer network.

The SITE definition should also be utilized to improve security amongst multiple nodes by causing The Network Director to guarantee that a user transferring from one node to another is still attending the terminal when it returns to the initial node. This is accomplished by proper use of the ACQUIRE=SELECT and ATTRIBUTES=NO-ACQUIRE definition statements and the terminal operator's RETURN command. See "RETURN Command" on page 256 for additional information.

The format of the SITE statement is:

```
SITE

    site name
  [ NETWORK-ELEMENTS=(alpha pattern, ... ) ]
    TARGET=alpha value
```

Figure 23. SITE Syntax

site name

is the 1 to 8 character identifier for the SITE being defined. This will be used externally to refer to the SITE and is the name that will be entered on the Message Editor's panel to indicate where a particular message should be sent.

NETWORK-ELEMENTS

identifies the network element values (typically, USERS or TERMINALS definitions that are located at the SITE being defined. This operand provides a mechanism to cause The Network Director to enforce "naming standards" for what destinations are located at the SITE. The value entered by a Message Editor user into the To: field must match at least one of the operands present on this operand or it will be rejected. Wild characters are valid.

If the "site name" matches the GLOBALS SITE= value, then The Network Director will assume that the SITE you are defining is itself. In this case, the NETWORK-ELEMENTS operand controls which destinations in this Network Director can receive messages (although actual Sent messages will not go through the LU-LU type logic).

TARGET

is the VTAM APPLID that can be utilized in LU-LU operations for this Network Director to contact the other Network Director.

Examples

```
SITE    SEATTLE,TARGET=DIRECTOR,
        NETWORK-ELEMENTS=(Z+++++++,LU++++++)
```

This SITE definition establishes that the SEATTLE data center has The Network Director operating under the ACF/VTAM APPLID of DIRECTOR and the valid destinations at that data center for messages must have a User Id or LU Name starting with a Z or a LU character string.

TERMINALS

This definition identifies Network Director characteristics that should be assigned to a particular terminal or set of terminals regardless of who is at the device.

The format of the TERMINAL statement is:

```
TERMINALS

      terminal pattern
    [ ACQUIRE={NO|SELECT|YES} ]
    [ APPLICATIONS=(application name, ...) ]
    [ ATTRIBUTES=({NEWS-CREATION,NO-NEWS,NEWS-ALL-LOGON,
                   NEWS-ONLY-ONCE}, ... )
    [ AUTHENTICATION={NO|YES|EXT25|INTELLICARD|SNK} ]
    [ AUTHORIZATION=(statement identifier, ...) ]
    [ AUTOLOGOFF={NO|YES|RETURN|SELECT} ]
    [ COMMANDS={(YES|NO|DISC|DROP|FLASH|LOGON|RESET}, ... ) ]
    [ CUA={NO|YES} ]
    [ DAYS=(day specification, ...) ]
    [ DIM={0|numeric value} ]
    [ EXTENSION={+++++++++|alpha value} ]
    [ FORMAT-ID={STANDARD|OPTIONx} ]
    [ IDENTIFICATION={NO|YES} ]
    [ ID-AREA={NO|YES} ]
    [ GROUPS=(alpha-value, ... ) ]
    [ LOGO=terminal logo ]
    [ LOGMODE=alpha value ]
    [ MESSAGES=({NOTES|MEMOS|BROADCASTS|NONE}) ]
    [ MODE={LINE|SCREEN|COMPRESS}  ]
    [ NETID={++++++++|alpha pattern ]
    [ PFKEYS=(application 1, ...) ]
    [ PROFILE=(profile name,{VIEW|CHANGE|NO}) ]
    [ RECOVERY={LOSTERM20} ]
    [ REJECT={YES|NO} ]
    [ STATUS-INTERVAL={0|numeric value} ]
    [ SUBAREAS=(numeric value, ... ) ]
```

Figure 24. TERMINALS Syntax (Part One)

```
TERMINALS

    [ TIMES=(time specification, ...) ]
    [ TIMEOUT={0|,numeric value ]
    [ TRIES={0|numeric value} ]
    [ USER={user id|NO} ]
    [ USERS=(id 1,id 2, ... ) ]
    [ WSF={COLOR|NO|YES|KEEP} ]
```

Figure 25. TERMINALS Syntax (Part Two)

terminal pattern

specifies the LU pattern that should be used to identify terminals that will be covered by this TERMINALS definition. The Wild Character is allowed in the terminal pattern.

ACQUIRE

Identifies whether The Network Director should queue a request (SIMLOGON) for a device that matches the terminal pattern

NO do not issue a SIMLOGON to acquire the device at initialization (The Network Director is assuming that LOGAPPL has been utilized at the VTAM definition level)

SELECT issue a SIMLOGON to acquire the device only after the device has chosen an application (do not issue a SIMLOGON during initialization processes). This has a variety of uses in conjunction with other functions (see APPLICATION ATTRIBUTE=NO-ACQUIRE).

YES issue a SIMLOGON to obtain control over the device. When a device selects an application, YES also causes The Network Director to queue a request for the device to get the device back when the session is complete.

Normally, the VTAM PU or LU will have been directed to The Network Director via the LOGAPPL parameter. ACQUIRE=YES is an alternative to this method and instructs The Network Director to acquire the device via SIMLOGON. This operand is not valid if the terminal name includes a wild character.

Do **not** specify ACQUIRE=YES and LOGAPPL for the same LU or ACQUIRE=YES in two Network Directors. This creates many difficulties within the ACF/VTAM environment that can result in VTAM CIDs being reassigned inappropriately (producing incorrect LU names in the ID-AREA) or can cause the device to enter session with the wrong Network Director (in cross domain environments).

APPLICATIONS

identifies the set of logical applications that this TERMINAL will have placed upon its Application Selection Panel. Each of the applications must have been previously defined via a Network Director APPLICATION statement. If the APPLICATIONS operand is omitted, the TERMINAL will have only the DEFAULT APPLICATIONS available to it (assuming no GROUP definition is involved).

ATTRIBUTES

The ATTRIBUTES operand indicates specific processing characteristics associated with a network element that is associated with the corresponding definition element. The Network Director will utilize the ATTRIBUTES operand that is related to the "most detailed" definition element that applies to the network element.

Valid settings are:

NEWS-ALL-LOGONS the NEWS panel should be delivered to the applicable network elements every time a user logs on to the system

NEWS-CREATION the related network elements are authorized to create the NEWS message

NEWS-ONLY-ONCE the NEWS panel will be delivered to each unique user only one time (this requires the presence of the External File for tracking across executions of The Network Director)

If you set this ATTRIBUTE on a GROUP definition, it must be the default GROUP for the network element (TERMINAL or USER) or the NEWS characteristic will not operate.

NO-NEWS the NEWS message is not to be delivered to a network element associated with the definition

AUTHENTICATION

controls the characteristics associated with extended user validation (user validation in addition to the basic userid and password combination). Extended authentication also requires that an External File AIB be allocated prior to system access by the user. Please reference the *Network Operator's Guide* (TND-0210) for additional information about adding an AIB utilizing the SHOW processor.

Valid operands are:

EXT25 indicates that an installation exit (EXT25) must approve of any logon attempt prior to The Network Director granting access (providing a Application Selection Panel) to the user covered by this definition.

IntelliCARD indicates that the user covered by this definition must utilize IntelliCARD International's IntelliCARD device to obtain access to the system. Please refer to the *IntelliCARD Interface* manual (TND-0216) for more information.

NO this is the default and indicates that there will be no extended verification required (beyond userid and password).

SNK indicates that the user covered by this definition must utilize Digital Pathway's SecureNet Key device to obtain access to the system. Please refer to the SecureNet Key Interface Reference (TND-0226) for more information.

YES indicates that extended verification is necessary and the algorithm or device process required is defined by the contents of the External File (the AIB defined for the user).

AUTHORIZATION

establishes The Network Director statements that may be issued from this terminal when the terminal selects Network Administration (if it is authorized). The default is for all statements to be allowed. Coding any value on the AUTHORIZATION operand authorizes only the coded statements. Other unauthorized statements will be ignored and considered a security violation. As an example, AUTHORIZATION=(DISPLAY,VTAM,USER) allows the device to issue only the three listed commands when connected to Network Administration.

AUTOLOGOFF

instructs The Network Director whether to automatically LOGOFF the User at this terminal when a User selects a subsystem Valid setting for this operand are:

NO the default value indicates that The Network Director is to remember which user has logged on to the device and to bypass any automatic logoff logic

YES indicates that The Network Director is to logoff the user when the device returns to The Network Director from the subsystem

RETURN is the same as YES

SELECT requests that the terminal user be logged off at the same time as the device is forwarded to the subsystem

This is typically used when you can not be certain that the VTAM LU name will consistently identify the same physical device (as in the case of some protocol convertors, etc).

COMMANDS

controls whether this terminal will have The Network Director's Command Line present on its non-CUA Application Selection Panel. DROP, DISC, LOGON, and RESET imply YES and authorize the defined element access to those functions. See "COMMANDS" on page 51 for more information.

CONFIDENTIAL

Indicates whether the session traffic between The Network Director and the device are to be confidential or not.

NO will allow the VTAM trace to contain the data that is sent on the session between the device and The Network Director.

YES will cause trace entries for the session to have the data suppressed

CUA

The CUA operand indicates whether terminals defined by this definition are to utilize the CUA interface for the initial signon and selection panels or not.

NO indicates to The Network Director that the devices associated with this definition are to utilize the non-CUA Application Selection Panel and associated processes.

YES instructs The Network Director to utilize CUA terminal formatting principles to interact with the terminal user.

DAYS

describes the days of the week that the TERMINAL is allowed to be active within The Network Director. See the DAYS discussion under "Day Specification" on page 6 for more information. The default is for the TERMINAL to be always authorized for access to The Network Director.

DIM

specifies the interval after which The Network Director will automatically clear the device's screen. The DIM interval applies only to devices in their default condition (not logged on). A value of zero indicates that no DIM logic will be utilized.

EXTENSION

sets the value for the extended TERMINAL characteristic that will allow an identification of the TERMINAL beyond that provided simply by the terminal name. This operand will be utilized to establish uniqueness between multiple TERMINAL statements with the same terminal name. To receive the characteristics of this TERMINAL definition, the operator must provide the proper Extension from the proper terminal.

FORMAT-ID

controls the format of the bottom two lines of The Network Director's formatted non-CUA panels. See "FORMAT-ID" on page 53 for additional information.

GROUPS

establishes one or more Network Director GROUPs that devices connected to this definition will have access to. The network element is automatically connected to the first GROUP specified (if present) and can change the operational characteristics of the device by making use of the GROUP command.

See "Terminal User Controlled GROUPing" on page 155 for a discussion of the possible uses for the GROUPS= operand.

IDENTIFICATION

controls whether the usage of devices connected to this TERMINALS definition require a signon or not

NO a user at the device is not required to signon to utilize the system

YES devices will be prompted with the Identification panel. The terminal operator will have to identify himself prior to further processing.

ID-AREA

establishes whether this TERMINAL should receive the ID area or not (for non-CUA Application Selection Panels). The terminal operator can reverse this setting by issuing the Command Line's ID command, if the Command Line is present.

NO the device should not receive the ID area

YES the device should receive the ID area

LOGO

is the operand that provides the simple graphic portrayal of the installation defined identifying information. This information will be placed at the top of The Network Director's non-CUA Application Selection Panel for devices matched by this definition.

See "LOGO" on page 13 for additional information about the options available to code the LOGO operand.

LOGMODE

specifies the 1 to 8 character name of the VTAM BIND image that should be utilized to establish a session with the device. If the LOGMODE is invalid, you will receive sense codes indicating the problem in the LOG display.

This LOGMODE value **overrides** the value specified in VTAMLST or by the terminal operator for sessions with The Network Director. The presence of the LOGMODE operand also disables The Network Director's BIND "refresh and compare" logic associated with responding to physical device reconfiguration procedures (3180s, etc.).

NRS recommends that you allow the ACF/VTAM LOGMODE to control The Network Director's interactions with the device.

MESSAGES

controls the type of Message Facility messages this TERMINAL may Edit, Send, and Delete. NONE indicates that this operator will not be authorized for any of the message types.

MODE

Establishes special processing characteristics for devices associated with the definition. MODE can be set at:

COMPRESS indicates that LU1 devices will receive an abbreviated output transmission of the full 3270 panel (COMPRESS is exactly like SCREEN mode, except that completely blank lines are suppressed).

For non-LU1 devices (3270 type devices), The Network Director will "compress" all output streams sent to the 3270 device by replacing 5 or more blanks (X'40'), underscores (X'6D'), dashes (X'60'), plus signs (X'4E'), equal signs (X'7E'), periods (X'4B'), or asterisks (X'5C') with a 3270 Repeat to Address order. Compression will only be beneficial if you use one or more of the identified characters in consecutive positions in an output transmission (LOGOs, Info panels, selection titles, etc.).

LINE indicates that The Network Director will operate in a "line at a time" mode for all interactions with LU1 type devices. The Network Director will prompt only with "Command ===>" for input from the device.

SCREEN requests that The Network Director simulate the output display of a 3270 panel on a LU1 device. The Network Director will transmit the appropriate information to the LU1 device to approximate the physical appearance of the full 3270 panel on the LU1 device.

The LU1 terminal operator may modify the initial setting via usage of the operational commands (*L, *S, or *C), which are entered on the Command line.

The non-LU1 compression routine uses optimized instructions to scan the output transmissions to keep CPU consumption as low as possible, but you should recognize that activation of the COMPRESS option will cause CPU usage to increase. As a result, NRS recommends that you activate the compression logic only on TERMINAL devices that will actually benefit from the compression (i.e. remote devices on relatively slow lines, devices that receive LOGOs containing one or more of the designated characters in a repeating pattern, etc.).

NETID

The NETID operand identifies which devices in the entire ACF/VTAM network should match the TERMINALS or USERS definition (wild characters are valid).

When a device enters a session with The Network Director, the NETID associated with the device is collected from the queued CINIT and stored in a Network Director control block associated with the device (the Active Network Element or ANE). This value is then utilized in all searches associated with searching the TERMINALS or USERS definitions.

The operand provides a mechanism to specify specific characteristics (like APPLICATIONS=) that should be associated with devices that originate in specifically identifiable networks.[13]

PFKEYS

are the program function key values that should be associated with the APPLICATIONS selections The Network Director (for non-CUA Application Selection Panels). will automatically assign values if the PFKEYS parameter is left out. Specifying NO prohibits The Network Director from assigning a PFKEY value. See "PFKEY" on page 33 for additional information about how you can control the pfkey assignment process.

PROFILE

assigns this TERMINAL's default Profile. The profile name identifies the PROFILE statement containing this TERMINAL's default specifications. The second argument controls whether this TERMINAL may modify or view its own Profile.

RECOVERY

Controls specific error recovery characteristics associated with individual device sessions within The Network Director that are associated with the current TERMINAL definition. Valid operands are:

LOSTERM20 Indicates that The Network Director should respond to a LOSTERM reason code 20 by queuing a request for a session with the device forwarding the LOSTERM event. If not coded (the default condition), The Network Director will **not** queue a request for the device, which may result in some devices receiving ACF/VTAM's USSMSG10.

When coded, issuing the queued request against certain emulated devices or devices in VTAM error recovery may cause the queued work to stay on the VTAM Pending queue until the device restarts normally. This can create unnecessary VTAM messages and queue depths within ACF/VTAM.

---

[13] The collection of the NETID value is associated with RUs that are present in ACF/VTAM 3.1.1 and higher releases and will be not available on older ACF/VTAM releases.

REJECT

indicates whether The Network Director should accept sessions from the defined devices or if it should automatically CLSDST the defined LU(s).

NO The Network Director should accept sessions from devices that match this TERMINAL definition

YES The Network Director should immediately reject session from a device that matches this definition

STATUS-INTERVAL

specifies the interval at which The Network Director will verify that a device forwarded to a subsystem is still in session with that subsystem. See "STATUS-INTERVAL" on page 58 for more information.

SUBAREAS

The Network Director collects during session initialization the origin ACF/VTAM subarea that is associated with the device and it can be utilized to match TERMINALS and USERS definitions.

SUBAREAS is a list of numeric value subarea specifications (maximum of 60) that are considered valid for the particular definition to be considered a "match" for a specific network element. This operand allows the Network Administrator to associate definition characteristics with device from a particular subarea within the ACF/VTAM network.

TIMES

is the time of day specification that this TERMINAL is allowed access to The Network Director. See the discussion under "Time Specification" on page 5 for more specifics on how to specify the TIME. If omitted, the TERMINAL is always allowed access based upon the time of day check.

TIMEOUT

is the time interval this TERMINAL has before an authorized panel is automatically replaced with the default. A specification of zero (0) disables this timer.

TRIES

specifies the number of consecutive erroneous attempts to logon that The Network Director will allow a terminal operator to make before the device is placed on the Inactive List for security violations. See "TRIES" on page 59 for additional information.

USER

is The Network Director User id that this TERMINAL should be automatically associated with. The TERMINAL will take on all the attributes of the designated User, but without the requirement to identify himself. The appropriate USER definition must have been previously defined to The Network Director.

A specification of NO indicates to The Network Director that the identified terminal is not eligible for being logged on as a USER.

USERS

provides a list of User ids that are authorized to utilize this terminal. The Network Director will reject any attempt to logon by an operator not contained in the list. If this operand is not present, any operator may utilize the terminal. Wild Characters are allowable in the list.

WSF

controls whether The Network Director will use the 3270 Read Partition Query command to establish the characteristics of the device. See "WSF" on page 59 for more information about how this operates.

Examples

```
TERMINAL SPD093,APPLICATIONS=(PAYROLL,CODING),
                PFKEYS=(PF6),
                TIME=(08:00-18:00)
```

This terminal (terminal name SPD093) has access every day of the week between 8 am and 6 pm to the PAYROLL and CODING applications. PF6 will be associated with the PAYROLL selection and the CODING selection will be assigned a program function key by The Network Director.

```
TERMINAL   TM03,GROUP=PAYROLL
```

This terminal (terminal name TM03) will automatically become a portion of the PAYROLL GROUP. This will be the default for the terminal unless a terminal user modifies the attributes of the terminal by signing on as a USER.

```
TERMINALS   ABC++D++,USERS=(TSG+++++),
                    APPLICATIONS=(ABCTEST),
                    PROFILE=(ABC,VIEW)
```

The terminals whose names consist of **ABC** in the first 3 bytes and **D** the 6th byte will receive a single application named ABCTEST. If any terminal operator attempts to logon at the terminals, they must provide a User id that begins with TSG. Additionally, the terminal operators at these terminals may look at their Profile, but not change it.

USERS

This definition provides the characteristics for a single user or set of users of The Network Director's facilities. It defines those items that will be available to the terminal that the defined user signs on to.

The format of the USERS statement is:

```
USERS

      user id pattern
    [ ACQUIRE={NO|SELECT} ]
    [ APPLICATIONS=(application name, ...) ]
    [ ATTRIBUTES=({NEWS-CREATION,NO-NEWS,NEWS-ALL-LOGON,
                   NEWS-ONLY-ONCE}, ... )
    [ AUTHENTICATION={NO|YES|EXT25|INTELLICARD|SNK} ]
    [ AUTHORIZATION=(statement identifier, ...) ]
    [ AUTOLOGOFF={NO|YES|RETURN|SELECT} ]
    [ COMMANDS={(YES|NO|DISC|DROP|FLASH|LOGON|RESET}, ... ) ]
    [ CUA={NO|YES} ]
    [ DAYS=(day specification, ...) ]
    [ EXTENSION={+++++++++|alpha value} ]
    [ FORMAT-ID={STANDARD|OPTIONx} ]
    [ LOGO=user logo ]
    [ GROUPS=(alpha-value, ... ) ]
    [ ID-AREA={YES|NO} ]
    [ MAXIMUM={0|numeric value} ]
    [ MESSAGES=({NOTES|MEMOS|BROADCASTS|NONE}) ]
    [ NETID={++++++++|alpha pattern ]
    [ PASSWORD=password ]
    [ PFKEYS=(application 1, ...) ]
    [ PROFILE=(profile name,{VIEW|CHANGE|NO}) ]
    [ PSWD-OPTIONS=(expiration,generations,minlength,minwait) ]
    [ SELECTIONS=D+(T&U)|{D|T|U}[{+|&}{D|T|U}[{+|&}{D|T|U}]]
    [ SUBAREAS=(numeric value, ... ) ]
    [ STATUS-INTERVAL={0|numeric value} ]
    [ TERMINALS=(terminal name, ...) ]
    [ TIMES=(time specification, ...) ]
    [ TIMEOUT={0|numeric value ]
```

Figure 26. USERS Syntax

user id pattern

represents the 1 to 8 characters that will be entered into the Id: field to establish the terminal operator as a User of the network. This user id may contain wild characters and therefore may define multiple users.

ACQUIRE

Identifies whether The Network Director should queue a request (SIMLOGON) for a network element that selects a subsystem

NO no queued SIMLOGON request will be issued

SELECT each time a device is sent to an APPLICATION, The Network Director will issue the appropriate VTAM functions to cause the device to be returned immediately upon terminating the session with the APPLICATION.

ACQUIRE=SELECT is also useful when The Network Director forwarding the device to the subsystem is in a *remote* system to the device owning Network Director (a cross domain Network Director). It will cause the device to return to the "last" Network Director that had control of the device.

APPLICATIONS

identifies the set of logical applications that this USER will have placed upon his Application Selection Panel. Each of the applications must have been previously defined via a Network Director APPLICATION statement. If the APPLICATIONS operand is omitted, the USER will have only the DEFAULT APPLICATIONS available to it (presuming no GROUP definition is involved).

ATTRIBUTES

The ATTRIBUTES operand indicates specific processing characteristics associated with a network element that is associated with the corresponding definition element. The Network Director will utilize the ATTRIBUTES operand that is related to the "most detailed" definition element that applies to the network element.

Valid settings are:

NEWS-ALL-LOGONS the NEWS panel should be delivered to the applicable network elements every time a user logs on to the system

NEWS-CREATION the related network elements are authorized to create the NEWS message

NEWS-ONLY-ONCE the NEWS panel will be delivered to each unique user only one time (this requires the presence of the External File for tracking across executions of The Network Director)

If you set this ATTRIBUTE on a GROUP definition, it must be the default GROUP for the network element (TERMINAL or USER) or the NEWS characteristic will not operate.

NO-NEWS the NEWS message is not to be delivered to a network element associated with the definition

AUTHENTICATION

controls the characteristics associated with extended user validation (user validation in addition to the basic userid and password combination). Extended authentication also requires that an External File AIB be allocated prior to system access by the user. Please reference the *Network Operator's Guide* (TND-0210) for additional information about adding an AIB utilizing the SHOW processor.

Valid operands are:

EXT25 indicates that an installation exit (EXT25) must approve of any logon attempt prior to The Network Director granting access (providing a Application Selection Panel) to the user covered by this definition.

IntelliCARD indicates that the user covered by this definition must utilize IntelliCARD International's IntelliCARD device to obtain access to the system. Please refer to the *IntelliCARD Interface* manual (TND-0216) for more information.

NO this is the default and indicates that there will be no extended verification required (beyond userid and password).

SNK indicates that the user covered by this definition must utilize Digital Pathway's SecureNet Key device to obtain access to the system. Please refer to the SecureNet Key Interface Reference (TND-0226) for more information.

YES indicates that extended verification is necessary and the algorithm or device process required is defined by the contents of the External File (the AIB defined for the user).

AUTHORIZATION

establishes The Network Director statements that may be issued by this User when he selects Network Administration (if it is authorized). The default is for all statements to be allowed. Coding any value on the AUTHORIZATION operand authorizes only the coded statements. Other unauthorized statements will be ignored and considered a security violation.

As an example, AUTHORIZATION=(VTAM,VM,STOP) will restrict the user to issuing only VTAM and VM commands and shutting down The Network Director.

AUTOLOGOFF

instructs The Network Director whether to automatically LOGOFF the User at this terminal when a User selects a subsystem Valid setting for this operand are:

NO the default value indicates that The Network Director is to remember which user has logged on to the device and to bypass any automatic logoff logic

YES indicates that The Network Director is to logoff the user when the device returns to The Network Director from the subsystem

RETURN is the same as YES

SELECT requests that the terminal user be logged off at the same time as the device is forwarded to the subsystem

This is typically used when you can not be certain that the VTAM LU name will consistently identify the same physical device (as in the case of some protocol convertors, etc).

COMMANDS

controls whether or not this User is authorized to have the Command Line present on the non-CUA Application Selection Panel (it is always present on CUA Application Selection Panels). DROP, DISC, LOGON, and RESET imply YES and authorize access to the implied facilities. See "COMMANDS" on page 51 for more information.

CUA

The CUA operand indicates whether the users associated with this definition are to utilize the CUA interface for the initial signon and selection panels or not.

NO indicates to The Network Director that the users associated with this definition are to utilize the non-CUA Application Selection Panel and associated processes.

YES instructs The Network Director to utilize CUA terminal formatting principles to interact with the terminal user.

DAYS

describes the days of the week that the USER is allowed to be active within The Network Director. See the DAY discussion under "Day Specification" on page 6 for more information. The default is for the USER to be always authorized for access to The Network Director.

EXTENSION

sets the value for the extended USER characteristic that will allow an identification of the USER beyond that provided simply by the User id. This operand will be utilized to establish uniqueness between multiple USER statements with the same User id. Any operator desiring the characteristics of this USER must provide both the proper User id and Extension.

The default of all wild characters indicates that the terminal operator may enter anything into the Extension field.

For RACF installations, specifying EXTENSION=RACF causes The Network Director to present the data entered into the Extension: field to RACF as the "requested" RACF connect group. If invalid, the logon attempt will be rejected. If valid, the RACF Connect Group specified in the Extension: field can be utilized for GROUP=RACF processing or can be passed to an eligible subsystem via the INITIAL-DATA operand.

If you elect to activate this option, consider changing the ID area field text value to something more meaningful to its use (E.G., GLOBALS EXTENSION-TEXT='Group:').

FORMAT-ID

controls the format of the bottom two lines of The Network Director's formatted non-CUA panels. See "FORMAT-ID" on page 53 for additional information.

ID-AREA

establishes whether this User will have the ID area present on his/her non-CUA panels or not. If the User is authorized the Command Line, this setting can be altered by entering the ID command.

NO the device should not receive the ID area

YES the device should receive the ID area

LOGO

is the operand that provides the simple graphic portrayal of the installation defined identifying information. This information will be placed at the top of The Network Director's non-CUA Application Selection Panel for devices matched by this definition.

See "LOGO" on page 13 for additional information about the options available to code the LOGO operand.

GROUPS

establishes one or more Network Director GROUPs that devices connected to this definition will have access to. The network element is automatically connected to the first GROUP specified (if present) and can change the operational characteristics of the device by making use of the GROUP command.

See "Terminal User Controlled GROUPing" on page 155 for a discussion of the possible uses for the GROUPS= operand.

If the effective operand is set to the constant **RACF** and the terminal operator is susceptible to RACF checking (GLOBALS SECURITY=RACF and PASSWORD=YES), The Network Director will retrieve the RACF connect group from the ACEE (ACEEGRPN) and will attempt to connect this user to a Network Director GROUP statement with the same name. If there is no GROUP with the same name, The Network Director will attempt to connect to the GROUP with the literal RACF as a name.

If this operand is set to the constant **ACF2** and the terminal operator is susceptible to ACF2 checking (GLOBALS SECURITY=ACF2 and PASSWORD=YES), The Network Director will retrieve the first 8 bytes of the ACF2 UID string and will attempt to connect this user to a Network Director GROUP statement with the same name. If there is no GROUP with the same name, The Network Director will attempt to connect to the GROUP with the literal ACF2 as a name.[14]

If this operand is set to the constant **TSSDIV** or **TSSDEPT** and the terminal operator is susceptible to TopSecret/VM or TopSecret/MVS checking (GLOBALS SECURITY=TOPSECRET and PASSWORD=YES), The Network Director will retrieve the DEPARTMENT or DIVISION from TopSecret/VM or TopSecret/MVS and will attempt to connect this user to a Network Director GROUP statement with the same name. If there is no GROUP with the same name, The Network Director will attempt to connect to the GROUP with the literal TSSDIV or TSSDEPT.

---

[14] Recognizing that the first 8 bytes of the UID string may not be optimal for your installation, you can also utilize Exit 19 to set an alternative based on any values present in the UID string, the ACMCB, or the LIDREC. See the Internals manual for more information about the exit.

MAXIMUM

establishes the number of users that can be logged on with this User id at one time within The Network Director. The default of zero indicates that The Network Director will obtain the MAXIMUM value from the GROUP definition (if present). If no GROUP definition is applicable, then a value of one will be utilized as a default.

MESSAGES

specifies the types of Messages that this USER may Edit, Send, and Delete when utilizing the Message Facility. NONE indicates that this operator will not be authorized for any of the message types.

NETID

identifies which devices in the entire ACF/VTAM network should match the TERMINALS or USERS definition (wild characters are valid).

When a device enters a session with The Network Director, the NETID associated with the device is collected from the queued CINIT and stored in a Network Director control block associated with the device (the Active Network Element or ANE). This value is then utilized in all searches associated with searching the TERMINALS or USERS definitions.

The operand provides a mechanism to specify specific characteristics (like APPLICATIONS=) that should be associated with devices that originate in specifically identifiable networks.[15]

PASSWORD

is the 1 to 8 byte text string that is used during Network Director sign on to identify the terminal user as the USER identified by this definition. As with other passwords, The Network Director will not print this on the output Print file. The Wild Character is valid.

PFKEYS

are the program function key values that should be associated with the APPLICATION selections on non-CUA Application Selection Panels. The Network Director will automatically assign values if the PFKEYS parameter is left out. NO indicates that no PFKEY value should be assigned. See "PFKEY" on page 33 for additional information about how you can control the pfkey assignment process.

---

[15] The collection of the NETID value is associated with RUs that are present in ACF/VTAM 3.1.1 and higher releases and will be not available on older ACF/VTAM releases.

PROFILE

identifies the Profile this USER will be assigned. Profile name identifies the PROFILE definition that contains the specifications. The second operand assigns the Profile characteristics to the USER.

PSWD-OPTIONS

When SECURITY=DIRECTOR is in effect, the PSWD-OPTIONS operand (a list of numeric values) controls the numeric specifications associated with The Network Director's internal password maintenance. Each PSWD-OPTION is a positional numeric value with the following meanings:

expiration establishes the maximum duration a password can be utilized without being updated. At the end of this interval, The Network Director will force the user through a password update prior to allowing access to the system. Default value is 30D.

generations establishes the number of prior passwords that The Network Director will retain to insure that the terminal operator does not select the same password again. 10 (the default) is also the maximum that may be specified. The Network Director will automatically require that the terminal operator enter a new and different password from the prior generations unless this value is set to zero, which disables this validation.

minlength specifies the minimum length that is acceptable for a password. The Network Director will not allow a password that is shorter than this value. Specifying zero indicates that any length password is acceptable. The default is 4.

minwait specifies the minimum amount of time that must expire before The Network Director will allow a new password to be set. This is the minimum interval **between setting new passwords** that is acceptable to The Network Director. Zero (the default) indicates that The Network Director will accept any interval.

SELECTIONS

establishes the manner in which the APPLICATIONS= specification on the TERMINAL, USER, GROUP, and DEFAULT definitions should be processed. See "SELECTIONS" on page 14 for details.

STATUS-INTERVAL

specifies the interval at which The Network Director will verify that a device forwarded to a subsystem is still in session with that subsystem. See "STATUS-INTERVAL" on page 58 for additional information.

SUBAREAS

The Network Director collects during session initialization the ACF/VTAM subarea that is associated with the device and it can be utilized to match TERMINALS and USERS definitions.

SUBAREAS is a list of numeric value subarea specifications (maximum of 60) that are considered valid for the particular definition to be considered a *match* for a specific network element. This operand allows the Network Administrator to associate definition characteristics with device from a particular subarea within the ACF/VTAM network.

TERMINALS

provides a list of physical terminals that this User id is valid from. The Network Director will reject any attempt to logon from another device in the network. If this operand is not present, the USER may sign on to any terminal (as long as the terminal is not prohibited from USER session - TERMINAL USER=NO). The Wild Character is valid on this operand.

TIMES

is the time of day specification that this USER is allowed access to The Network Director. See the discussion under "Time Specification" on page 5 for more specifics on how to specify the TIME. If omitted, the USER is always allowed access based upon the time of day check.

TIMEOUT

specifies the time interval that an authorized panel will be allowed to remain on the terminal with this USER logged on. A specification of zero (0) will disable the timer.

Examples

```
USER    SYSTEMS,APPLICATIONS=(NETADMIN,CICSTEST),
                  PASSWORD=SSHHH
```

This USER will have available to it the applications named NETADMIN and CICSTEST. The Network Director will assign the program function keys. Access to The Network Director from this USER can occur whenever The Network Director is executing. In order to receive this USER's Application Selection Panel the terminal user will have to know the PASSWORD SSHHH.

```
USERS SP++,APPLICATIONS=(CODING),
           PASSWORD=++++++++,
           TIMEOUT=2M,
           TERMINALS=(SP++++++),
           DAYS=(MONDAY-FRIDAY)
```

Any User with a four character Id that begins with the letters **SP** can identify herself/himself as a USER to The Network Director. A Password must be provided, but it can be any value. The User will have only CODING available. Additionally, the Users must logon from a terminal whose name begins with a **SP** and will only be allowed access on weekdays. Whenever these Users are logged on, their authorized panels will be allowed to reside on the terminal only two minutes before The Network Director restores the terminal to its default condition.

Network Administration

As terminal based systems expand, the requirement for adequate control has become an important factor. The Network Director is a software subsystem that provides multiple facilities to assist in the administration of the network. Network Administration is the process of managing, monitoring, and planning the growth of the terminal network.

The Network Administrator

This section of the manual is addressed to the individual(s) responsible for the network. The title used here is the Network Administrator, but it is the function of network management that is important.

The Network Director considers the terminal network a valuable resource that should be treated as such. It is the end user's most visible contact point with the computing facility. Terminal availability, reliability, and usability are of major importance. It is the Network Administrator's responsibility to insure that the terminal network resource is available to authorized individuals in a predictable and timely manner.

Overview

This section of the manual provides the information necessary for the Network Administrator to utilize the facilities of The Network Director to provide optimum usage of the terminal network. Note that The Network Director can only provide the mechanisms to enable a knowledgeable individual to manage the network. It is important that the function of Network Administration be an active one.

Network Administration (and this section) begins with a discussion of the planning necessary for the initial implementation of The Network Director. This identifies the types of areas that the Network Administrator will require information about, to adequately define the network through The Network Director's Configuration Parameters.

We will then discuss the mechanism provided by The Network Director for the online viewing and modification of the network definitions.

The Network Director also provides a LOG file of all activities that go on within the logical networks. This LOG file may be viewed by the Network Administrator to resolve difficulties that may have occurred within the network. This section will identify the information present in the LOG file and how to utilize it.

Next, the discussion will focus upon how to utilize The Network Director's Program Operator facility. This subject identifies how the Network Administrator can use The Network Director to interact with VTAM itself.

Finally, this section will provide a broad discussion of the types of information (reports, etc.) that are available to the Network Administrator for the monitoring of the terminal network. Various facilities, online and batch, are provided and can be used for a variety of purposes (Trend analysis, etc.).

Obviously, each Network Administrator will develop his (or her) own combination of facilities that best meet individual site requirements. It is this section's task to present a general overview of the available facilities to the Network Administrator.

From this point on in this section of the manual, a reference to *you* or *your* is a reference to the individual or individuals responsible for Network Administration.

Sample Configuration Parameters

The following Configuration Parameters present a basic approach when constructing Network Director Configuration Parameters.

```
*---------------------------------------------------------------*
*                                                               *
*     First, define all the APPLICATIONS in use                 *
*                                                               *
*---------------------------------------------------------------*
APPLICATION  PERSON,TARGET=CICS1,
                    TITLE='General Personnel System'
APPLICATION  PAYABLE,TIMES=(08:00-12:00,13:00-17:00),
                    TARGET=CICS2,
                    TITLE='Accounts Payable Inquiry'
APPLICATION  NETADMIN,TARGET=NETADMIN,
                    TITLE='Network Administration'
APPLICATION  INFO,TARGET=TNDINFO,PFKEY=PF1,
                    TITLE='Network Director Assistance'
APPLICATION  MESSAGES,TARGET=TNDMSG,PFKEY=PF12,
                    TITLE='Messages'
APPLICATION  CODING,TITLE='Program Development',TARGET=TSO
*---------------------------------------------------------------*
*                                                               *
*     Second, set the PROFILE and DEFAULTs                      *
*                                                               *
*---------------------------------------------------------------*
PROFILE      GENERAL,PRINTER=SPPRT01,
                    ACCOUNT='2094-G63'
           DEFAULT  APPLICATIONS=(INFO,MESSAGES),
                    PROFILE=(GENERAL),
                    LOGO=
              *******        ********          ********
             ***   ***       ***   ***        ***    ***
             ***   ***       ***    ***      ***
             *********       ***    ***      ***
             ***   ***       ***   ***        ***    ***
             ***   ***       ********          ********
LOGO-END
*---------------------------------------------------------------*
*                                                               *
*     Third, identify the GROUPs                                *
*                                                               *
*---------------------------------------------------------------*
GROUP     PAYROLL,APPLICATIONS=(PAYABLE,PERSON),
                  PASSWORD=ADMIN,DAYS=(MONDAY-FRIDAY),
                  TIMEOUT=4M
GROUP       PROG,APPLICATIONS=(CODING)
*---------------------------------------------------------------*
*                                                               *
*     Last, list the TERMINALS and USERs                        *
*                                                               *
*---------------------------------------------------------------*
TERMINAL   TM03,APPLICATIONS=(PERSON,PAYABLE,CODING),
                    TIME=(08:00-17:00)
TERMINALS  PY++++++,GROUP=PAYROLL
*
USER       SYSTEMS,PASSWORD=SECRET,
                  APPLICATIONS=(CODING,NETADMIN)
TERMINALS  SPD++TS,USER=SYSTEMS
```

Figure 27. Sample Configuration Parameters

Implementation Planning

Once The Network Director is installed (see the *Installation* manual), you may begin the implementation of the logical network. Of course, this implies that the implementation you would like to use is already identified. The following discussion is intended to assist you in preparing the Implementation Plan.

The Implementation Plan is simply the process of identifying your logical definition of the terminal network and migrating terminals and the user community to it. Migration may occur all at once or a portion at a time, depending upon the complexity of your physical network and the logical networks.

Implementation Planning will cover the following major topics:

1. VTAM Definition Activities
2. Network Director network definitions
3. Security package considerations
4. Migration Approach

Each of these major planning topics require differing approaches. The following sections will identify the objective for each topic and immediately discuss the points that require attention to adequately accomplish the objective of the specific planning topic.

VTAM Definition Activities

The Network Director's use of the terminal network must be synchronized with the definitions in use within VTAM. This portion of the planning effort identifies the VTAM parameters that may require attention.

Objectives

This planning activity, when completed, should provide you with the information necessary to modify VTAM definitions to be in concert with your logical network's requirements. The Network Director must be defined (along with its authorized functions) as a valid application program to VTAM. Terminals that will be managed by The Network Director may also require some attention.

The APPL Definition

The Network Director executes as a normal VTAM subsystem and will require a definition within the VTAM Application Program Major Node. This is accomplished by placing the VTAM APPL definition statement in the appropriate VTAM library member or source book.

The system generation process will have prepared a sample APPL statement on its Stage One Listing based upon the installation parameters. You should insure that it matches the criteria that you wish based upon the following discussion.

Note: The VTAM definition statements present in this manual are only presented here to emphasize the parameters that may have to be set to enable The Network Director to function in the manner you have selected. For a complete list of VTAM definition parameters, you should reference the appropriate VTAM manual.

The basic format for The Network Director related APPL definition statement is:

```
applname    APPL  AUTH=(PASS,NVPACE{,ACQ}{,SPO})
                  ,PRTCT=password
```

Figure 28. Network Director APPL Definition

applname

is the 1 to 8 byte ACB APPLID id that The Network Director will use to identify itself to VTAM. This is equivalent to the VTAMAPL parameter in the Stage One deck.

```
AUTH=(PASS,NVPACE{,ACQ}{,SPO})
```

provides the VTAM facilities that The Network Director is allowed to utilize.

PASS is required and allows The Network Director to forward ownership (CLSDST PASS) of a terminal to another ACF/VTAM application subsystem This facility is used by The Network Director when the terminal operator has made a selection from a Application Selection Panel that is not one of the internal Network Director facilities.

The Network Director always (as far as VTAM is concerned) sends single element messages to terminals that are in session with it. Specifying NVPACE informs VTAM of this characteristic.

ACQ is required if The Network Director will be dynamically acquiring terminals (ACQUIRE=YES on the TERMINAL definition via SIMLOGON commands, or for Message Printing) or if you would like to use the RELEASE command. You should always provide this option to The Network Director unless you have a specific reason it cannot be provided, in which case you should contact North Ridge Software, Inc. for additional information.

SPO is required if you have elected to utilize The Network Director's Program Operator facility. This is the mechanism that will allow you to issue VTAM commands from an authorized Network Administrator terminal.

PRTCT=password

is the 1 to 8 byte password that The Network Director will use to insure that it is the proper *applname* user. This should be the same as the VTAMPAS parameter in the Stage One deck.

VTAM NSI APPL Definition

If your installation has elected to make use of the documented Network System Interface for batch programs, you will also require another VTAM APPL definition for the NSI.

The Network System Interface is technically accomplished via a LU-LU session (LU0 or LU6.2, depending upon which routine you use) between The Network Director and NSI in the calling address space/partition. This will require one of the following definitions:

```
TNDNSI   APPL AUTH=(NVPACE)
TNDNSI62 APPL AUTH=(NVPACE),APPC=YES,MODETAB=TNDINCLM
```

Additional information about the NSI is available in the *Network User's Guide* and the *Internals* Manual.

The LU, PU, or LOCAL Definition

The basic format for The Network Director related LU, PU, or LOCAL statement is:

```
name       PU|LU|LOCAL   LOGAPPL=applid
```

where:

name is the symbolic name for the terminal (the VTAM minor node name for the device).

LU|PU|LOCAL is the VTAMLST type of logical unit being defined.

LOGAPPL=applid is the 1 to 8 byte name (applname on the APPL definition statement) that this terminal should be automatically connected to when VTAM initializes or the device is not queued to any other application.

VTAM Definition Summary

The VTAM APPL definition statement is required before The Network Director may execute. The characteristics present on the APPL statement control the VTAM facilities that The Network Director may make use of. The Stage One Listing produced during installation will contain a recommended APPL statement.

You may also wish to include a definition for the Network System Interface in the event that your installation decides to make use of the interface.

You may have to modify the LU, PU, or LOCAL definitions for the terminals that you wish The Network Director to manage. The LOGAPPL parameter will direct specified terminals to The Network Director.

This concludes the entries necessary within the VTAM definition members, files, or books. Once the appropriate entries are made, The Network Director can initialize and begin operation.

It should be emphasized that you are not required to make any PU, LU, LOCAL, or NSI related entries. These mechanisms can be activated after initial experimentation and the network migration plan is in place. To proceed with testing, only the APPL definition for The Network Director itself is required.

TNDINTAB

The Network Director typically relies upon the LOGAPPL definition operation to obtain control of the devices in the network. To further insure that a device cannot select an application subsystem without being subject to The Network Director and the associated security package checks, it is possible to restrict the device to The Network Director. This is accomplished via the use of an "interpret table", which can be used to convert any input entered from a device and passed to SSCP into a session request for The Network Director.

A sample interpret table is present on the distribution tape called TNDINTAB. Simply assemble this and place it into an appropriate library; then associate it with the desired devices by proper usage of the LOGTAB operand on the LU or PU definition statements.

ASYDE

ACF/VTAM Version 3.2 and up contains a start option that controls what occurs on an active session when a local non-SNA device is powered off. ASYDE=TERM is the default and causes the session to be terminated between the device and the application subsystem. You should set the option to ASYDE=KEEP to cause the session to be retained and the power on/off to be reflected to the application.

ASYDE=KEEP allows The Network Director to retain control over devices that have been powered off and thereby continue to actively monitor their usage.

Network Definitions

The logical network that The Network Director manages is described to The Network Director via the Network Definitions (Configuration Parameter entries or RELOADed definitions from the External File). The Network Definitions describe the various logical components of your network and instruct The Network Director on how to manage it.

Objectives

This planning activity, when completed, should provide you with a tailored Network Director configuration. Each of the definition statements is described as it applies to the planning of the logical network. The approach discussed here is not the only approach that can be used to successfully configure The Network Director, but this approach should produce a generalized definition of your terminal network.

The Philosophy

Generally, The Network Director as a software subsystem is attempting to make the physical terminal network and associated VTAM major nodes a set of *logical networks*. This implies that individual users and/or terminals are not necessarily knowledgeable about where a particular processing function is within the general computing facility.

The designation of these *logical* identities makes the computing facility easier to utilize for the non data processing individual and enhances the Network Administrator's ability to "move" application subsystems from one processing environment to another. As an example, if the end user is always asking to connect his terminal to the INVENTORY application and not the "production CICS" system, then the INVENTORY application can be moved to another "production CICS" system without requiring the end user to be made aware of a different logon technique.

Additionally, the end user(s) can also be managed as though there are logical groupings of users. This allows the matching of end user with the application totally at a logical level. This logical grouping of users also allows The Network Director to deal with more than a single user at a time. It is possible to allow (or disallow) access by GROUP (disabling/enabling more than a single end user) and to send a message to the GROUP.

Identifying Logical Entities

As a result of the *logical network* definition, your first task is to identify the entities within your computing environment that require their own logical identity. Look for combinations of programs, transactions, processes, and users that are interrelated.

Usually, the majority of these combinations are easy to spot. Most installations have already broken the total work load into manageable subsystems. However, do not automatically assume that the use of each subsystem is independent of any other. Also, do not assume that each end user's utilization of the system is exactly like anyone else.

Each of the network definitions is generally explored in the following discussion. You should remember that this discussion is only intended to point out major decision points that you should address. Once you have arrived at a major definition point, you should evaluate each operand of the specific definition for applicability to your specific definition.

In the following discussion and in the subsequent sections of this manual, references to a *network element* or *network entity* are references to a specific element or individual within the network. You may have a specific individual at a specific terminal whose definitions (USER and TERMINAL) are both "wild character" type definitions. The "network element" is not the USER or TERMINAL definition, but rather the unique User id and/or unique LU name associated with the specific user and terminal.

This identification of a *network element* will continue to be utilized throughout The Network Director, including specific reporting and display operations.

APPLICATION

Each unique combination of programs and/or transactions that make up a single logical entity should be defined as a Network Director APPLICATION. Examples of applications are: PAYROLL, PERSONNEL, INVENTORY, ACCOUNTING, CLAIMS, NCCF, UCC7, etc..

The Network Director's APPLICATION statement will identify a logical application that The Network Director can manipulate independently of any others. An APPLICATION can be made available to a USER, GROUP, or TERMINAL for selection. It can be HELD by the Network Administrator and various Network Director reports and queries can produce statistics about it. It is also possible to Send a Message (Broadcast) to all network elements that are authorized to access a particular APPLICATION.

Each application should be then assigned a Network Director "name" and each subparameter on the APPLICATION statement should be reviewed for applicability. Does the application have any special requirements about time of day availability? Or day of week? What general descriptive phrase should The Network Director use on the Application Selection Panels to describe the application?

Do not forget to define The Network Director's standard facilities that you intend to use (INFO, Message Switching, or Network Administration). If they are not defined as APPLICATIONs, you will not be able to access them.

Each of these application definitions will be authorized for each terminal, user, and group that may have access. The key task at this point is to properly identify all the applications. Actual use assignments will occur later.

GROUP

Each major grouping of network users should also be identified. When there are multiple individuals that will be running multiple terminals and processing with the same or similar characteristics, you may wish to identify a GROUP to The Network Director to simplify the network definition coding requirements.

The GROUP designation will allow the Network Administrator to manipulate the status of multiple operators with a single Network Director operator command. Messages can be sent to the entire GROUP with a single Send command.

The GROUP designation can be obtained from your security system (if you have one installed), which can significantly reduce the number of Network Director definitions that are required.

If specific operator identification is required to maintain system integrity, consider a USER definition utilizing the Wild Character to provide similar facilities.

Terminal User Controlled GROUPing

The Network Director's **GROUP** command permits the terminal user to dynamically change The Network Director GROUP he/she is a member of without affecting the logon status of the network element.

The Network Director permits the terminal operator to invoke the GROUP command to change the current GROUP assignment. The command syntax is:

```
GROUP {desired-group}
```

The "desired-group" may be any group name listed in the applicable USER or TERMINAL GROUPS= operand. If the terminal operator enters an authorized GROUP name, the Application Selection Panel will be reconstructed utilizing the characteristics of the new GROUP and message TND0833 is written to the LOG and the affected device.

If the terminal operator requests a GROUP that is not authorized via the applicable GROUPS= operand, TND0832 is issued and the current GROUP remains unaffected.

The terminal operator may request that The Network Director return to the default GROUP by simply entering the GROUP command with no operand value.

To illustrate how the new GROUPS logic and GROUP command may be useful, consider the following Configuration Parameters:

```
APPLICATION CICS1,TARGET=CICS001,TITLE='CICS One'
APPLICATION CICS2,TARGET=CICS002,TITLE='CICS Two'
APPLICATION CICS3,TARGET=CICS003,TITLE='CICS Three'
APPLICATION TOCICS,TARGET=TOCICS,TITLE='To CICS Menu',
         INITIAL-DATA=('GROUP CICS')
*
APPLICATION IMS1,TARGET=IMS001,TITLE='IMS One'
APPLICATION IMS2,TARGET=IMS002,TITLE='IMS Two'
APPLICATION IMS3,TARGET=IMS003,TITLE='IMS Three'
APPLICATION TOIMS,TARGET=TOIMS,TITLE='To IMS Menu',
         INITIAL-DATA=('GROUP IMS')
*
GROUP IMS,APPLICATIONS=(IMS1,IMS2,IMS3,TOCICS)
GROUP CICS,APPLICATIONS=(CICS1,CICS2,CICS3,TOIMS)
GROUP USERS,APPLICATIONS=(CICS1,IMS1,TOCICS,TOIMS)
*
USERS ++++++++,GROUPS=(USERS,IMS,CICS)
```

When an individual signs on that is successfully pattern matched with the USERS definition (in this example, everyone will match), they are immediately assigned to the default GROUP of USERS (the first GROUP in the list of GROUPS operands).

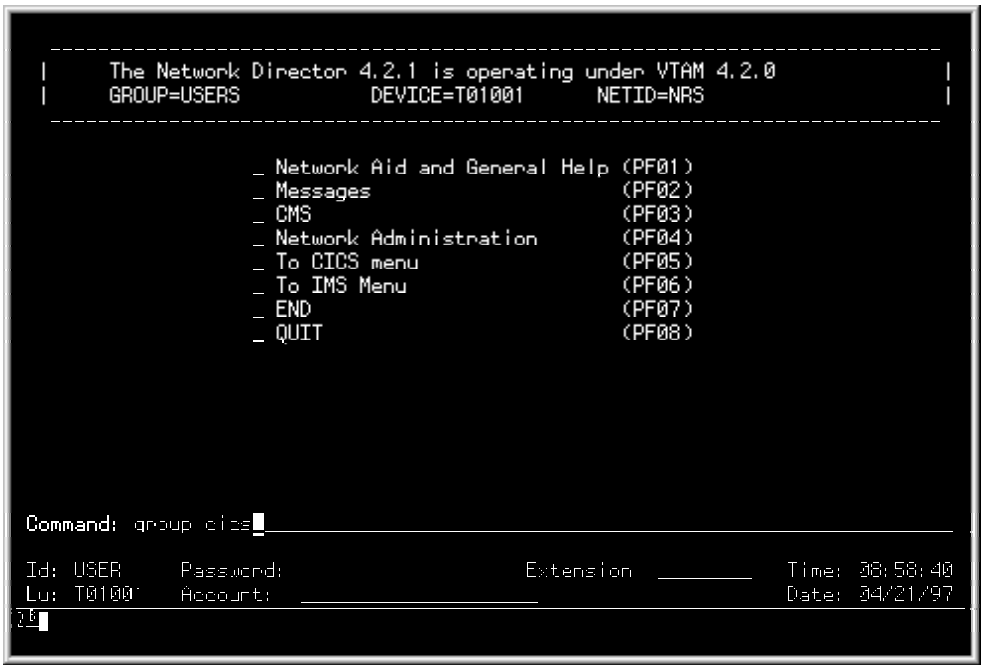


Figure 29. USERS GROUP Application Selection Panel

The terminal user can change to a menu consisting of only CICS applications by entering the command "GROUP CICS" or pressing the function key associated with the TOCICS choice on the Application Selection Panel. The CICS GROUP includes the three defined CICS systems, as well as a choice to select a menu of IMS applications.

Figure 30. CICS GROUP Application Selection Panel

With a little planning, this mechanism can be used to divide your logical applications into a variety of collections (GROUPS) that can make your network much easier to utilize.

USERS

Operators with specific authorization needs (designated Network Administrators) or installations with specific authorization requirements should uniquely identify the operators with the USER definition statement. Individual operators (USERs) and their characteristics require definition in order for The Network Director to provide proper authorization checking for authorized individuals.

Each operator that has specific requirements should be designated a USER. Note that some generality can be achieved through proper utilization of the Wild Character. Additionally, a USER can automatically become a member of a GROUP. This can allow each GROUP member to be identified by a separate User id/Password combination, but the total GROUP can still be dealt with as a single entity.

Remember that a USER can move from one terminal to the next unless restricted via the TERMINALS= parameter. Note also that the USERS definition provides only a "pattern" to use for a specific set of users within the network. Each network element will extract individual characteristics as it becomes active within The Network Director.

TERMINALS

You should define specific terminals to The Network Director whenever a physical terminal is to be authorized immediately for access and requires more applications than is defined on the DEFAULT statement. Any operator that has access to the physical terminal will be allowed access to the terminal's selections. This is typically used for terminals that are in a secure location and all the individuals in the terminal's proximity are authorized to use it.

Devices that have no matching TERMINALS definition will still be presented with the DEFAULT APPLICATIONS= if the DEFAULT IDENTIFICATION=NO operand is in effect. If IDENTIFICATION=YES is active then the terminal will receive the User id Identification panel. This characteristic implies that you **do not** have to define each terminal that will utilize The Network Director. In this case, simply providing the VTAM LOGAPPL operand is enough to cause The Network Director to manage the terminal.

You may want to consider eliminating the terminal's ability to identify itself as a USER. This prohibits the terminal from becoming assigned to a different logical area and then being left. This can be accomplished via the USER=NO operand or ID-AREA=NO and COMMANDS=NO.

Terminals are typically routed to The Network Director through utilization of VTAMs PU or LU LOGAPPL operand. As an alternative, you may specify ACQUIRE=YES to instruct The Network Director to dynamically obtain the terminal. The parameter for terminal acquisition will have to be present in either VTAM's or The Network Director's definitions. In general, North Ridge Software, Inc. recommends the LOGAPPL approach, but either parameter will achieve the same effect.

The ACQUIRE=YES operand prohibits the use of Wild Characters, which will typically increase the number of TERMINAL definitions. However, it may be an alternative you would like to utilize. ACQUIRE=YES is particularly convenient during early testing and prior to actually making the necessary changes in VTAM's definition library. Make sure that you remove the ACQUIRE option when you begin utilizing the LOGAPPL approach to eliminate any potential confusion on the part of ACF/VTAM.

Similar to the USERS statement, the TERMINALS statement defines a pattern (remember the wild characters) that will be used to associated actual network elements with the TERMINALS definition.

DEFAULT

The DEFAULT statement contains parameters that are common to all the GROUPs, USERS, and TERMINALS that are active within The Network Director. Its most common use is to extend the availability of general applications to all current sessions (reference the following discussion on APPLICATIONS=). It is also the location that the default LOGO for your installation is defined.

Typically, the common Network Director facilities (Message Switching and INFO) are defined as default APPLICATIONS for all operators. You should keep in mind that the applications specified on the DEFAULT statement are in addition to any other applications the operator qualifies for.

The TIMEOUT parameter is especially important to set properly. The Network Director considers terminal panels "secure" if they are on a terminal that currently has a USER session active (an operator has identified himself to The Network Director). These secure panels will be allowed to remain on the terminal for TIMEOUT seconds before the panel will be reset to the physical terminal's default. The USER session will be automatically terminated (forced LOGOFF).

The TIMEOUT facility has been provided to protect the terminal network from the accidental abandonment of a physical terminal that has been presented with an authorized panel. It can also be controlled at the USERS, GROUP, and TERMINALS level. It is important to set the parameter to an appropriate value. If it is not present, the DEFAULT is no TIMEOUT at all. This means that an authorized panel will never be removed from a terminal by The Network Director.

The DEFAULT statement is also where you will want to set the general "mode" of operation (CUA or not). CUA (Common User Access) is a set of definition and operating processes that specifies how panels are to be presented to the user. This specification is intended to provide a similar "look and feel" across different applications in your system. If you would like the CUA principles to apply, set CUA=YES. CUA=NO (the default) provides panels that are a bit more flexible, contain more information, but do not conform to CUA.

NRS recommends that you experiment a little with both modes of operation and then establish a standard for your installation.

GLOBALS

The GLOBALS statement controls the systems environment portion of The Network Director and does not have any impact on the logical network implementation. Refer to the GLOBALS statement description under "GLOBALS" on page 65 for more information.

APPLICATIONS

The subparameter is present on the USER, GROUP, TERMINAL, and DEFAULT parameter statements. It is the mechanism that provides the logical connection between the APPLICATION definitions and the individual operators. The operands of this subparameter will dictate which selections the operator will have on the Application Selection Panel.

The Network Director will always use the "most detailed" identity to establish the selections for a specific operator. Thus, if the operator is sitting at a terminal defined with the TERMINAL statement, the Application Selection Panel will contain APPLICATIONS from the TERMINAL and DEFAULT statements. If the operator identifies himself as a USER, the Application Selection Panel will contain APPLICATIONS from the USER, TERMINAL and DEFAULT statements as controlled by the SELECTIONS= operand.

If the operator is currently logged on as a USER and chooses to identify himself as a different USER, The Network Director will process a logical logoff of the first USER from the terminal immediately prior to processing the logon of the "new" USER.

Multiple Page Application Selection Panels

The Network Director has no maximum of allowable APPLICATIONS. You can define as many as required for the particular USER, TERMINAL, or GROUP. The Network Director will fill the Application Selection Panel with as many as can fit on the panel. If the non-CUA network user still has applications available, they can be viewed by simply striking the ENTER key. The PFKEYs may be used also, provided that F7 and F8 are not also assigned to APPLICATION selections. The terminal operator will have to exercise some care when using PFKEYs. They will be generally reassigned for each "page" of selections.

The CUA terminal user can also use the Bkwd (F7) and Fwd (F8) commands to page through the selection menu. This *paging* operation will continue until the operator has exhausted the authorized APPLICATIONS, at which point the Application Selection Panel will return to the first panel again.

Whether the APPLICATION is displayed or not, the terminal operator can select the APPLICATION by typing the APPLICATION NAME. Dynamic status updates for APPLICATIONs not currently displayed will cause no activity on the panel.

PROFILE

The PROFILE statement[16] allows you to assign basic operational characteristics to a particular USER, GROUP, or TERMINAL. The primary decision that must be made during the definition process is whether the network users will be allowed to modify their Profile or not. If they will be allowed to modify it, the Network Administrator will not be required to set the Profile contents exactly.

However, if the network users will not be allowed to change their Profile contents. The network definitions must contain the proper settings for each USER, GROUP, and TERMINAL.

Summary

The Network Director's network definitions provides you with a wide variety of definitions with which to define your logical terminal network. The construction of the network definitions should follow the logical process discussed previously.

The network definitions are likely to require changes as your terminal network grows. For this reason, you should carefully plan the relationships represented by the definitions.

Except for a few of the GLOBALS subparameters, all of the parameters and subparameters present in the network definitions are modifiable during The Network Director's execution. However, these changes will not be saved to the next execution unless you specifically SAVE them.

---

[16] Known as the Options for CUA mode users.

To summarize the Configuration Parameter planning tasks:

1. Identify logical applications and define each with an APPLICATION definition
2. Establish the network default applications and identify them with a single DEFAULT definition
3. Identify logical groupings of terminal operators and define each with a GROUP definition
4. Authorize access for specific individuals or sets of individuals through the USER definition
5. Establish specific terminal requirements and define them through a TERMINAL definition

Figure 31. Implementation Planning Tasks

Remember that the USERS and TERMINALS definitions provide a pattern for defining USERs and TERMINALs. If the definition contains no Wild Characters, it defines a pattern that will be used by only one network element at a time, but it is still a pattern to be merged with the DEFAULT and GROUP statements. When a new network element is encountered by The Network Director the network element's characteristics are drawn from the most detailed definitions (USERS and TERMINALS) first, the GROUP definition second, and finally, the DEFAULT definition.

Migration Approach

Once the VTAM Definition and The Network Director network definition planning activities are complete, you can begin implementation of the logical networks. This portion of the planning effort discussion offers some general comments on the alternatives available to you to accomplish the migration.

Objectives

This portion of the planning discussion should provide you with some ideas on how you can implement The Network Director and its concepts in your environment. This discussion is, of necessity, general in nature and should be adjusted according to the specific needs of your environment.

Definition

For the purposes of this discussion, *migration* is the term used to indicate those activities that a Network Administrator has to go through to convert terminals from the existing method of computing facility access to The Network Director's general philosophy.

Migration is typically a gradual process. Portions of an existing network are usually migrated individually. This allows a minimum of disruption in the event of an unanticipated error.

The Network Definitions

Generally, it is a good policy to initialize The Network Director with your entire logical network definition. The network definitions often have many internal relationships and any attempt on your part to "split" the network definitions at various migration points may inadvertently affect the relationships.

Initializing The Network Director with the fully defined network allows you to concentrate on the effect of the migration on the terminal operators and the full computing facility without the constant need to update the Configuration Parameters. However, do not hesitate to modify the Configuration Parameters to better serve your needs as migration proceeds.

New Network Additions

Terminals and their corresponding users that are just being introduced to the computing facility are excellent candidates for immediate conversion. In fact, since they are totally new, the term *conversion* is really inappropriate.

If the entire network is new or under significant expansion, the effort to convert or migrate is greatly simplified. Remember to make the proper documentation available to the terminal operators for the facilities they will be using. The selection process within The Network Director is relatively simple to use, but if the operator will be using INFO or the Message Facility extensively, the *Network User's Guide* should be available.

Existing Networks

It is more likely that you have an existing terminal network and will be interested in identifying specific portions to migrate. Usually there will be one or more specific user groupings that have the most urgent need for the new facilities. Obviously, they are good candidates for migration. They are more likely to be willing to assist in the refinement of the network definitions for improved usage characteristics.

It is also usual that one or more GROUPs of individual operators will stand out as likely early migration candidates. The data processing staff itself can be dealt with as such a group. Perhaps only particular subsets like a particular development group, or possibly systems programming are likely candidates.

The logical network's definitions must be validated as early during migration as possible. The ideal situation is that as individuals and groups are migrated, the logical network they are migrating into is stable (in terms of their view of the network). The Network Director is about improving the end user's interface to the computing facility. If the logical definitions do not match the end user's needs, then this goal is sacrificed.

Testing Techniques

When you have decided to migrate a particular group of users or terminals, you will typically be assigning ownership of the terminals to The Network Director in one of two manners. Either the VTAM LOGAPPL definition or The Network Director's ACQUIRE=YES parameter will be necessary for The Network Director to manage the terminal (do **not** use both techniques at the same time on the same device).

To test the network definition for a particular terminal, you can leave both of these parameters off. To activate The Network Director simply issue the standard VTAM USS commands from the terminal to LOGON to The Network Director. This presumes that the appropriate entries have been made for The Network Director in VTAM's USS tables. A functioning Network Administrator terminal may also issue The Network Director's SIMLOGON operator command to duplicate this activity from within The Network Director.

These techniques will enable you to test the Application Selection Panel for the terminal and to utilize any authorized Network Director facilities. However, when you cause The Network Director to transfer your terminal to a target subsystem (via the Application Selection Panel), The Network Director will release your terminal and will not recover it once your session with the target subsystem is complete.

As an alternative, you can modify a particular terminal's characteristics within The Network Director by issuing a Network Administrator TERMINAL ACQUIRE=YES command for the target terminal. This will cause The Network Director to modify the specified terminal's internal control block to indicate that The Network Director should issue the VTAM SIMLOGON function for the device. To actually acquire the device the first time, you should issue the Network Administrator's SIMLOGON command. Thereafter, The Network Director will manage the device exactly as if you had initialized The Network Director with the ACQUIRE option specified.

The preceding techniques will allow you to test a logical definition on an experimental basis. Full migration on a production basis will not take effect until you actually modify the network definitions.

Summary

Migration to The Network Director is primarily one of accepting the logical network concepts. This can be achieved using many different approaches. The following list represents one of the approaches.

1. Completely define the logical network first.
2. Identify portions of the logical network that can be migrated individually.
3. Test specific definitions for each migration group before actual migration.
4. Be responsive to requests for extended definitions to enhance the usability of the computing facility.

The Network Administration Panel

The Network Administration panel is the basic panel that an authorized operator will use to access the Network Administrator defined functions. It is reached from the Application Selection Panel and is authorized exactly like any other "application" in the network definitions.

The following information discusses in detail each of the Network Administrator's available functions. The Network Administrator panel can be portrayed as:

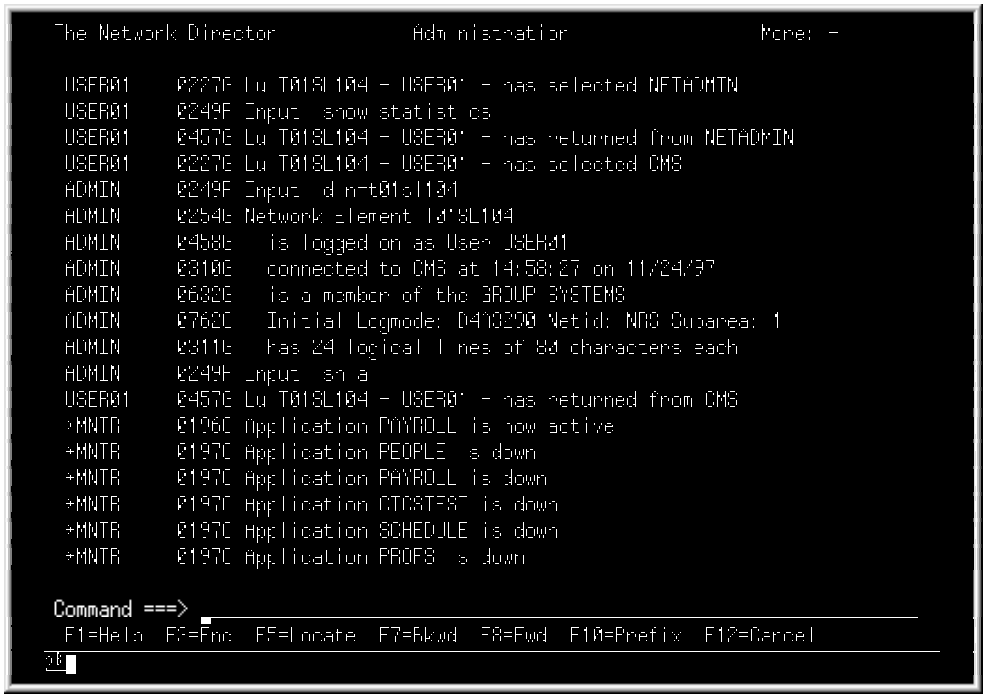


Figure 32. Network Administration Panel

The Network Administrator can return to the Application Selection Panel by striking the CLEAR key, typing the Primary Commands END or CANCEL, or pressing a PFKEY that has been assigned one of these values. To utilize one of the Network Administrator functions, simply enter text commands on the Primary Command line or utilize the standard Network Director Program Function Keys.

The information to be displayed can be controlled via use of the PREFIX command (see "The PREFIX Command" on page 170). The data in the LOG can be searched sequentially via usage of the LOCATE command (see "The LOCATE Command" on page 171).

Network LOG Display

The Network Administrator's panel will automatically display the most recent contents of The Network Director's LOG file. You can manipulate this file display by entering the Bkwd or Fwd commands (default PF07 and PF08) or the ALL command.

The Pfkeys can be used to move the display forward or backward in the LOG. This mechanism allows the Network Administrator to diagnose problems occurring within the logical network or to simply monitor activity.

The Network Director's online LOG file is a circular storage queue. The buffer size is controlled via the LOGSIZE operand on the GLOBALS statement. If the LOG buffer is small, you may want to restrict entries in the LOG to those that you consider important. The LOG operand of the GLOBALS statement allows the Network Administrator to manage the class of messages that are logged into the buffer. The message classes are described in further detail in the Message and Codes manual.

A Network Administrator can also place the Network Administration panel into an *automatic update* mode by entering the Primary Command MONITOR. This will cause the Network Administration panel to be automatically updated whenever a non trace message is placed into the LOG by any activity within The Network Director. Monitor Mode can be terminated by striking any AID key other than ENTER or issuing the RESET primary command.

The left portion of the Network Administrator panel contains either the time of day or a network element name associated with the LOG entry. The Network Administrator can alternate between the standard display of this area and all "times" by issuing the PREFIX command (default PF10).

ALL Command

The Network Director contains a general purpose command intended to allow the Network Administrator to selectively choose elements from a list for display. The **ALL** command allows the terminal operator (normally, a Network Administrator) to use one or more operands (delimited by any character desired) combined via boolean logical operations to select items.

Each argument must be delimited by a character, which is specified as the first and last character of the string.[17]

The general syntax of ALL is:[18]

```
ALL arg1 [ {AND|OR} {NOT} arg2 ] ...
```

Figure 33. ALL Command Syntax

Thus, specific messages associated with a particular device could be selected from the LOG display by issuing:

```
ALL "T01005"
```

The double quotes are the delimiters that cause ALL to create a display of any messages that has the string T01005 associated with it.

You can utilize multiple operands by adding the appropriate keyword operators between arguments, as provided for in the ALL syntax. Entering ALL with no operands resets the current ALL criteria to the null condition (all elements will be included again).

When viewing the Network Administration log,[19] the Network Administrator may issue the ALL command to select a portion of the LOG for viewing. This alternative to the PREFIX command is more general purpose and allows the specification of multiple criteria (PREFIX allows only pattern matching to select elements).

The Administrator's ALL command searches the LOG for messages that contain the specified criteria and presents them for display to the Network Administrator. ALL and PREFIX are mutually exclusive for selecting messages for display (PREFIX can still be used to control the format of the prefix area).

---

[17] The first character of the first argument in the ALL command is accepted as the delimiter for all the arguments in a single ALL command.

[18] The ALL command is not case sensitive.

[19] The ALL command can also be used on SHOW list type panels to "subset" the list of elements.

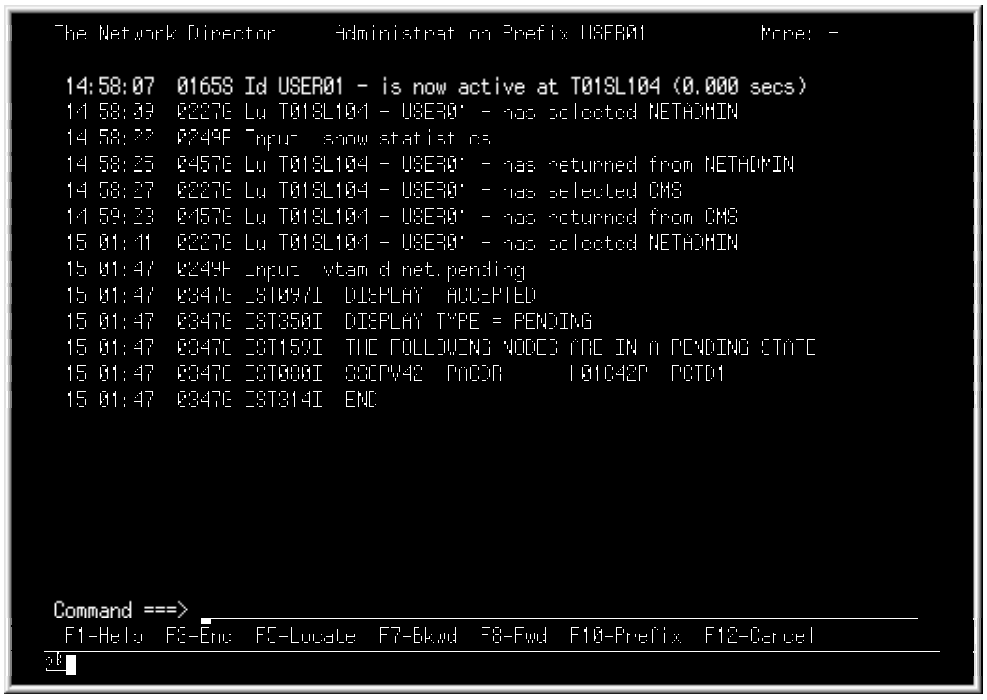


Figure 34. Network Administration LOG Display All Command

ALL scans each Log Buffer Entry (LBE) in storage and, as a result, can be utilized to select any message for a specific device or userid. However, the LBE does not contain the time, date, or message number in EBCDIC form and ALL cannot locate messages using these values.

The PREFIX Command

The PREFIX command offers the following options:

```
PREFIX {pattern|STANDARD|TIMES|LUNAMES|DATES|NONE|#nnnn}
```

Figure 35. PREFIX Command Syntax

Operand	*Meaning*
DATES	displays only the date in the prefix area
LUNAMES	displays only the lu names associated with the messages
NONE	eliminates the prefix area completely from the panel, which provides more area for viewing long messages (like the VTAM Program Operator responses, etc.)
no operand	alternates the TIMES and STANDARD formats or reset the current PREFIX pattern
pattern	selects LOG entries associated with the entered pattern (wild characters are valid)
STANDARD	displays either the User Id, LU Name, or Time (in that order) if it is associated with the message
TIMES	displays only the time in the prefix area
#nnnn	selects only LOG entries whose Network Director numeric message number matches the "nnnn" pattern (wild characters valid)

When a PREFIX pattern is in effect, the upper right hand corner of the Network Administration panel will contain the pattern in effect instead of **Network Administration**. An example of the PREFIX command usage is in the Network Operator's Guide under "Isolating Activity".

The LOCATE Command

The LOCATE command is also active and will search forward in the LOG display for a character string. You can issue the LOCATE command by entering LOCATE, SEARCH, or FIND as a primary command on the command line and following it with the character string you are searching for. Alternatively, the CMS LOCATE syntax of a single slash "/" will also function as a LOCATE command.

```
===> /datastring/
```

The search will proceed forward from the current position in the LOG and will stop at the first data line that contains the specified character string of "datastring". The LOCATE pfkey (default PF5) will repeat the last LOCATE function.

Control the Logical Network

The Network Director provides a mechanism to control and monitor the logical and physical network. There are a variety of keyword commands that can be used to interrogate the status of an existing portion of the defined network (the Configuration Parameter definitions), dynamically allocated items and the current status (see "Network Reporting" on page 173), and to operate on portions of the system (RELEASE, HOLD, DELETE, etc.)

The commands can be issued from the primary command line of the Network Administration panel and are documented in their entirety in the *Network Operator's Guide*.

You may also enter the GLOBALS command from the command line (other Configuration Parameter definitions are manipulated via the SHOW command) or the operating system console (OS Stop/Modify, GCS WTOR, DOS MSG). The ability to enter the GLOBALS command allows you to set key operating system level elements while attempting to recover from unusual situations that may arise in your system.

Issue VTAM Commands

If The Network Director has been authorized to operate as a VTAM Program Operator (APPL AUTH=SPO and GLOBALS VTAMOPER=YES), then the Network Administrator can issue any valid VTAM command from the Primary Command line. All such commands must be prefixed with the text string **VTAM** in order for The Network Director to recognize it as a VTAM operator command.

The result of the command will be displayed in the Display Area exactly as would any other Network Director message. The message "reply" is susceptible to message class controls exactly as any other message would be.

RETRIEVE

The last input entered by the Network Administrator can be restored to the LOG display's command line by execution of the RETRIEVE command. This provides a mechanism to quickly correct any data entry that has had a slight error.

The RETRIEVE command is most useful when associated with a PFKEY or PAKEY in the individual Network Administrator's Profile (use the PROFILE command to select the PFKEY).

Network Reporting

The Network Administrator can also request multiple reports and displays that provide information about the status and make up of the network. This reporting facility is intended to aid the Network Administrator in understanding the characteristics of the logical network while the network is active.

DISPLAY Syntax

The reporting facility is provided through The Network Director's DISPLAY command. Its general format is:

```
DISPLAY

   [ ACTIVE ]
   [ APPLICATIONS [ =application name ] ]
   [ AUTOLOGOFF ]
   [ BROADCASTS ]
   [ CHAINS ]
   [ COUNTS ]
   [ DEFAULTS ]
   [ DFBS ]
   [ ERRORS ]
   [ EXITS ]
   [ FILE-IO ]
   [ GLOBALS ]
   [ GROUPS [ =group name ] ]
   [ HELD ]
   [ INACTIVE ]
   [ INTERVAL ]
   [ ITERATION ]
   [ MEMOS ]
   [ MESSAGES ]
   [ MODULES ]
   [ NETID={++++++++|alpha pattern} ]
   [ NETWORK-ELEMENTS [=network element name ] ]
   [ NOAUTOLOGOFF ]
   [ NOTES ]
   [ PROFILES [ =profile name ] ]
   [ PTFS ]
   [ REJECT ]
   [ SAVED [ =(setname,version) ] ]
   [ SECURITY ]
   [ SITES [ =site name ] ]
   [ STORAGE ]
   [ SUBAREA=numeric value ]
   [ TERMINALS [ =terminal name ] ]
   [ USERS [ =user name ] ]
   [ ZAPS ]
```

Figure 36. DISPLAY Command Syntax

any of the =xxx operands may be specified with Wild Characters.

When an operand is specified as a positional value, you will receive an Overview of the specific area you have request a display on. E.G. DISPLAY APPLICATIONS will produce a single line for each defined APPLICATION and its current status.

When an operand is specified as a keyword (operand=value), you will receive a specific display for the network entity you are displaying. The format will be similar to the syntax required in the Configuration Parameters to define the entity. To conserve space in the LOG display queue, operands will generally only be displayed if their setting is something other than the default.

Operand	***Meaning***
ACTIVE	requests a display of all network elements that are logged onto The Network Director and have not selected a subsystem.
APPLICATIONS =pattern	requests information about one or more Network Director APPLICATIONS.
AUTOLOGOFF	requests a display of all network elements that are queued for a logoff function. AUTOLOGOFF may be queued by AUTOLOGOFF=RETURN, exceeding CONNECT-MAXIMUM or violation of the STATUS-INTERVAL check. This DISPLAY operand may also be used in conjunction with APPLICATION=, TERMINALS=, USERS=, or NETWORK-ELEMENTS= to qualify the display further. Contrast this with NOAUTOLOGOFF.
BROADCASTS	requests a one line display for each Broadcast Message currently within the Message Facility.
CHAINS	requests a single line display for each major control block chain within The Network Director. The basic number allocated and currently is use is reported.
COUNTS	is the general request for demographic information associated with the logical network. This will provide overview numeric values associated with the number of network elements currently connected to the various applications.
DEFAULTS	produces a list of the current values that are provided via the DEFAULT statement.
DFBS	produces a list of the current Dispatchable Function Blocks. This represents individual work elements that The Network Director has underway. See the Internals Manual for a detailed description of the DFB.
ERRORS	produces a subset of devices on the INACTIVE list which are inactive because of consecutive errors within a single session. These devices are eligible for *automatic release* if the device is capable of sending a "successful input" to

	The Network Director (SNA devices may have to use the ATTN key).
EXITS	produces a list of installation exits that are active within the operating Network Director nucleus.[20]
FILE-IO	This DISPLAY operand produces a single line identifying the number of logical External File operations that The Network Director has initiated. This is **not** a count of the number of I/O operations actually performed by the Access Method, but rather the number of internal, logical operations performed (i.e. a single PUT requires a GET for UPDATE followed by a UPDATE call).
GLOBALS	provides a display of the global values currently in effect within The Network Director.
GROUPS =pattern	produces information about one or more GROUP definitions.
HELD	produces a subset of devices on the INACTIVE list which are inactive because of operator HOLD commands
INACTIVE	produces a single line for each device that is on the Inactive List
INTERVAL	produces a subset of devices on the INACTIVE list which are inactive because of TIME or DAY specifications
ITERATION	produces a subset of devices on the INACTIVE list which are inactive because of consecutive session failure activities
MEMOS	requests a one line display for each Memo Message currently within the Message Facility.
MESSAGES	displays overview information associated with each message within the Message Facility.
MODULES	produces a list of each internal Network Director CSECT and when it was assembled for inclusion in the current Network Director nucleus.
NETID	establishes the alpha pattern to be utilized to qualify network elements for inclusion in the results of the DISPLAY. This operand only **qualifies** which items to include in the DISPLAY. You must use another DISPLAY operand to indicate what items to display.

[20] This operation will produce proper output only if the exits were assembled utilizing the TNDSTART macro.

NOAUTOLOGOFF requests a display of all network elements that are **not** queued for a logoff function.

This DISPLAY operand may also be used in conjunction with APPLICATION=, TERMINALS=, USERS=, or NETWORK-ELEMENTS= to qualify the display further. Contrast this with AUTOLOGOFF.

NOTES requests a one line display for each Note Message currently within the Message Facility.

NETWORK-ELEMENTS =pattern requests a display of basic information associated with a currently active network element within the network. The network element name can be either the LU name or the User id of the network element.

PROFILES =pattern produces the values that were assigned with one or more PROFILE statements.

PTFS produces a list of PTFs (ZAPS) that have been applied to the operating Network Director nucleus (this is the same as DISPLAY ZAPS).

REJECT produces a subset of devices on the INACTIVE list which are inactive because of BID failures. These devices are eligible for *automatic release*.

SAVED DISPLAYs information associated with the definitions that have been stored in the External File via the SAVE command. See "Displaying SAVED Definitions" on page 179 for examples of the DISPLAY SAVED command and its variations.

SECURITY produces a subset of devices on the INACTIVE list which are inactive because of security violations

SITES =pattern produces the values that were assigned with one or more SITE statements.

STORAGE displays the current virtual storage allocations being managed by The Network Director's storage management routines.

SUBAREA establishes the subarea number to be utilized to qualify network elements for inclusion in the results of the DISPLAY. This operand only **qualifies** which items to include in the DISPLAY. You must use another DISPLAY operand to indicate what items to display.

TERMINALS =pattern requests information about one or more specific TERMINALS within the logical network.

USERS =pattern display information associated with one or more specific USERS.

ZAPS produces a list of ZAPS (PTFs) that have been applied to the operating Network Director nucleus (same as DISPLAY PTFS).

The inactive list operands (ERRORS, HELD, INTERVAL, ITERATION, REJECT, and SECURITY) may be specified individually or in any combination.

```
DISPLAY SECURITY,HELD,ITERATION
```

shows all devices that are on the Inactive List that are not eligible for automatic release because of security violations, operator HOLD commands, or consecutive session failures.

```
TND0249G Input: DISPLAY NETWORK,SUBAREA=1,NETID=NRS+++
TND0764G T01001 - active from Subarea: 1 Netid: NRS
TND0764G T01005 - USER1 active from Subarea: 1 Netid: NRS
TND0764G T01015 - USER3 active from Subarea: 1 Netid: NRS
```

Note: Internal network elements (OPERATOR, OPERSMSG, etc.) are automatically assigned to the local Netid and a Subarea of 0. They are not actual devices in the network, but are logical elements of the processing system.

Displaying SAVED Definitions

The DISPLAY SAVED command produces a single line for each stored record on the External File that meets the criteria specified in the SAVED operand. DISPLAY SAVED displays one line for each complete set of saved definitions (definitions saved as a unit with a single SAVE command). As an example:

```
TND0249G Input: display saved
TND0728G SAVED Control Block Records
TND0729G     Name=DIRECTOR,Version=0
TND0729G     Name=DIRECTOR,Version=1
TND0729G     Name=DIRECTOR,Version=2
TND0729G     Name=DIRECTOR,Version=4
TND0729G     Name=TEST ,Version=0
```

Specifying the saved name displays a single line for each definition within the identified set (without regard for version). Using the version portion of the SAVED= operand causes only definitions from the specified version to be displayed.

```
TND0249G Input: display saved=test
TND0728G SAVED Control Block Records TEST
TND0730G     USER TEST ++++++++
TND0730G     USER TEST2 ++++++++

TND0249G Input: display saved=(director,2)
TND0728G SAVED Control Block Records DIRECTOR 2
TND0730G     APPLICATION ADMIN
TND0730G     TERMINAL OPERATOR ++++++++
TND0730G     USER ++++++++ ++++++++
```

This information can also be obtained by using the TNDUTIL batch program as discussed in "External File Maintenance (DISPLAY/DELETE)" on page 260.

Overview Displays

The DISPLAY command has three basic types of requests. They are called Overview, Specific, and Combined Displays. The Network Director will categorize your report request based upon the number of DISPLAY operands you have used.

The first request type is called an Overview Display and will address general requests of The Network Director. This request will have only a single operand and the operand will have no supplied argument value.

Figure 37. Overview Display Example 1

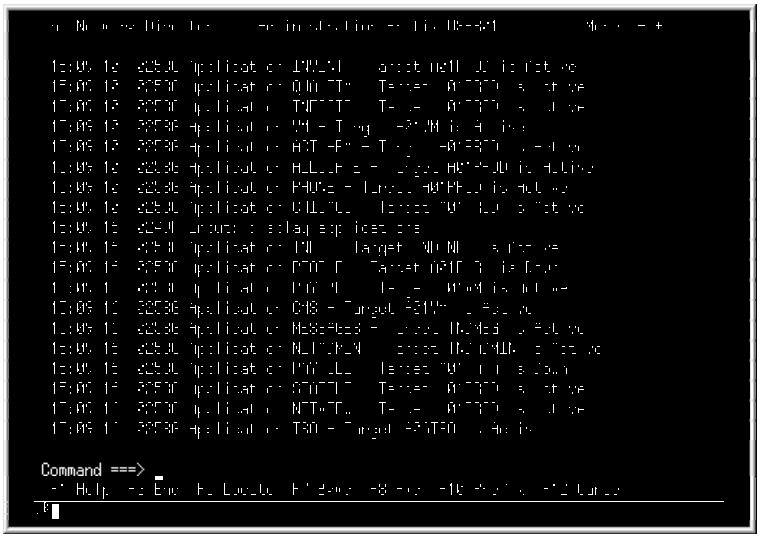


Figure 38. Overview Display Example 2

Specific Displays

The second type is called a Specific Display and will produce displays showing the single dimensional values present in a Network Director control block. The control block values are typically set via network definition efforts. Thus, the Network Administrator can use Specific Displays to query the attributes associated with a particular network entity. The Network Director's Wild Character is valid.

Figure 39. Specific Display Example 1

The following example is a command typically used by an installation HELP desk to interrogate details associated with a device. This would be used where the user's id is known and the HELP desk personnel are interested in more information about what device the user is on and what status it is in.

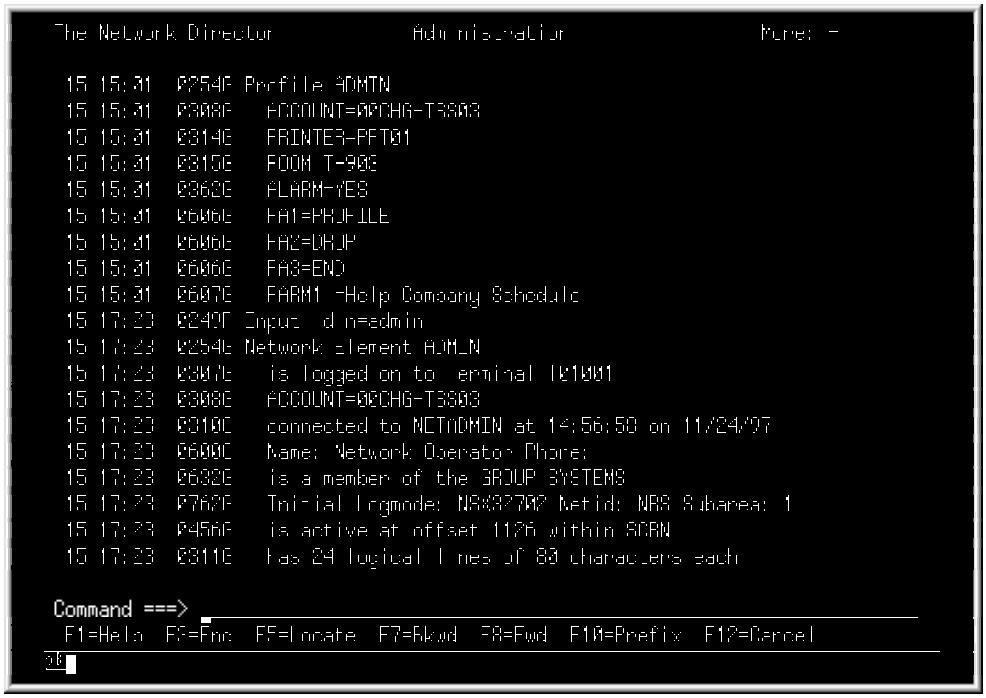


Figure 40. Specific Display Example 2

Combined Displays

The third type of Display Type is called a Combined Display. It will have two or more valid Display operands and will produce differing reports depending upon the combination.

Figure 41. Combined Display Example

Consult the *Network Operator's Guide (TND-0210)* for additional information and examples.

Event Recording

The Network Director can also provide data associated with events occurring within its partition/address space. This is termed **Event Recording**. To activate this, specify the GLOBALS EVENTS= operand with the appropriate values to cause The Network Director to produce the SMRs (System Measurement Record) for OS systems and the SARs (System Accounting Record) for DOS, GCS, or OS systems. The exact medium used to record the events is dependent upon the operating environment that The Network Director is executing in. Reference the Installation Guide under *Supported Accounting Operands* for the specific operating system The Network Director is operating in for additional information.

The following descriptions are intended to provide additional information about the contents of the SMRs and SARs. Any additional overhead introduced by the operating environment is **in addition to** the SMR or SAR fields (e.g., OS SMF Header, etc.).

SARs are 80 character accounting records that are operating system independent. That is, the SAR from a Network Director in DOS can be merged with SARs from GCS and/or OS systems to produce a single file that can be processed on the system accomplishing the merge process. SMRs are variable length and can be effectively recorded only in an OS SMF environment. Because of the general characteristic of operating system portability, NRS recommends use of the SAR format. However, both the SMR and SAR formats are discussed in this section.

```
SMR      DSECT                          Director's SMR Record
*
*        The Network Director's SMR Header Record Description
*
SMRTYPE  DS    H                 Director SMR Record Type
SMRPUSER EQU   0                   Reserved for installation
SMRPRET  EQU   4                   EVENT=RETURN
SMRPLOGN EQU   8                   EVENT=LOGON
SMRPLOGF EQU   12                  EVENT=LOGOFF
SMRPAPPL EQU   16                  EVENT=APPLSTAT
SMRPVTAM EQU   20                  EVENT=VTAMERRS
SMRPIUPD EQU   24                  EVENT=INFOUPD
SMRPACNT EQU   28                  EVENT=APPLCNTS
SMRPMSND EQU   32                  EVENT=MSGSEND
SMRPMDEL EQU   36                  EVENT=MSGDEL
SMRPMPRT EQU   40                  EVENT=MSGPRINT
SMRPMVIW EQU   44                  EVENT=MSGVIEW
SMRPACMD EQU   48                  EVENT=ADMINCMD
SMRPSLCT EQU   52                  EVENT=SELECT
*
*        Demographics
*
SMRPID   DS    CL8                 Id of the user (if present)
SMRPLU   DS    CL8                 VTAM LU Name (from NIB)
SMRPDATE DS    PL4                 Calendar Date
SMRPTIME DS    Pl4                 Time EVENT Occurred
SMRPDIR  DS    CL8                 Director's APPLID
SMRPVRS  DS    CL3                 Director Version Number
         DS    CL13                reserved
SMRPVAR  EQU   *                   variable portion start
```

Figure 42. SMR Header DSECT

```
SAR      DSECT                Director's SAR Record
*
*        The Network Director's SAR Header Record Description
*
SARPNAME DS    CL8              Director'S IDENTIFIER
SARPTYPE DS    H                Director SAR Record Type
SARPUSER EQU   0                   Reserved for installation
SARPRET  EQU   4                   EVENT=RETURN
SARPLOGN EQU   8                   EVENT=LOGON
SARPLOGF EQU   12                  EVENT=LOGOFF
SARPAPPL EQU   16                  EVENT=APPLSTAT
SARPVTAM EQU   20                  EVENT=VTAMERRS
SARPIUPD EQU   24                  EVENT=INFOUPD
SARPACNT EQU   28                  EVENT=APPLCNTS
SARPMSND EQU   32                  EVENT=MSGSEND
SARPMDEL EQU   36                  EVENT=MSGDEL
SARPMPRT EQU   40                  EVENT=MSGPRINT
SARPMVIW EQU   44                  EVENT=MSGVIEW
SARPACMD EQU   48                  EVENT=ADMINCMD
SARPSLCT EQU   52                  EVENT=SELECT
*
SARPVRS  DS    XL1               Director Version Number
SARPV230 EQU   23                  2.3.0
         DS    XL1               RESERVED
SARPID   DS    CL8               Id of the user (if present)
SARPLU   DS    CL8               VTAM LU Name (from NIB)
SARPDATE DS    PL4               Calendar Date
SARPTIME DS    PL4               Time EVENT Occurred
SARPVAR  EQU   *                 variable portion start
```

Figure 43. SAR Header DSECT

This information is present in the front of every event type produced by The Network Director. Information in the SMR or SAR past the header is dependent upon the EVENT type being produced.

The full DSECT is available on The Network Director's Source Library via the ASSEMBLER Macro TNDSMR or TNDSAR. The Network Director does not currently provide any manner with which to further reduce the data represented by the SMF record.

SMR or SAR header fields can be further defined as follows (where the first three bytes of the field can be SMR or SAR to identify the record where they reside).

Field	*Purpose*
PTYPE	represents the logical processing point at which The Network Director is writing the event.
PID	contains the Id field from the Identification Area. This will be the USER name of the terminal operator. It may be blank if no user has logged onto the device.
PLU	is the VTAM LU name extracted from the VTAM NIB and displayed after LU: in the Identification Area.
PDATE	is the calendar date (in 0YYMMDD+ format) the event occurred.
PTIME	is the time of day that the event occurred.
PDIR	is the APPLID being utilized by The Network Director to identify itself to ACF/VTAM. This can be utilized to differentiate between Network Director's when you are executing more than one within your network.
PVAR	represents the location where variable information begins in the event.

ADMINCMD

The ADMINCMD Event is recorded whenever a Network Administrator has issued a command via Network Administration.

The SMRPVAR layout is:

```
SMRMCMD  DS    CL11              Command being issued
SMRMOBJ  DS    H                 DUMP object
SMRMADB  DS    CL8               APPLICATION
SMRMUDB  DS    CL8               USERS
SMRMTDB  DS    CL8               TERMINALS
SMRMGDB  DS    CL8               GROUP
SMRMNEL  DS    CL8               NETWORK-ELEMENTS
SMRMSDB  DS    CL8               SITE
SMRMPDE  DS    CL8               PROFILE
SMRMEXT  DS    CL8               EXTENSION
SMRMDFB  DS    CL16              DFB
SMRMTEXT DS    CL72              Command Text
SMRMSIZE EQU   *-SMRHSIZE        Size of ADMINCMD format
```

Figure 44. SMR ADMINCMD Event DSECT

The SARPVAR layout is:

```
SARMCMD  DS    CL11               Command being issued
SARMOBJ  DS    H                  DUMP object
SARMTEXT DS    CL27               Command Text
SARMSIZE EQU   *-SMRPSTRT         Size of ADMINCMD format
```

Figure 45. SAR ADMINCMD Event DSECT

Each of the ADMINCMD Fields can be further defined as follows:

Field	*Purpose*
MCMD	is The Network Director's Statement Identifier for the command.
MOBJ	contains the object of the DUMP command (See the DSECT for the PPE to interpret the contents further).
MADB	contains the APPLICATION name when the administrator command contained the APPLICATION= operand.
MUDB	contains the USERS name when the administrator command contained the USERS= operand.
MTDB	contains the TERMINALS name when the administrator command contained the TERMINALS= operand.
MGDB	contains the GROUP name when the administrator command contained the GROUP= operand.
MNEL	contains the NETWORK-ELEMENTS name when the administrator command contained the NETWORK-ELEMENTS= operand.
MSDB	contains the SITE name when the administrator command contained the SITE= operand.
MPDE	contains the PROFILE name when the administrator command contained the PROFILE= operand.
MEXT	contains the EXTENSION value when the administrator command contained the EXTENSION= operand.
MDFB	contains the DFB value when the administrator command contained the DFB= operand.
MTEXT	the text associated with the last input buffer from the Network Administrator. This contains the entire text for a VM or VTAM command.
MSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

APPLCNTS

The APPLCNTS Event is recorded once an hour for each defined APPLICATION that has at least one network element connected to it.

The SMRPVAR layout is:

```
SMRCAPPL DS    CL8               APPLICATION Name
SMRCTRGT DS    CL8               VTAM APPLID
SMRCUSER DS    F                 Number of USERS connected
SMRCTERM DS    F                 Number of TERMINALS connected
SMRCMAX  DS    F                 MAXIMUM=
SMRCSIZE EQU   *-SMRHSIZE        Size of APPLCNTS format
```

Figure 46. SMR APPLCNTS Event DSECT

The SARPVAR layout is:

```
SARCAPPL DS    CL8               APPLICATION Name
SARCTRGT DS    CL8               VTAM APPLID
SARCUSER DS    F                 Number of USERS connected
SARCTERM DS    F                 Number of TERMINALS connected
SARCMAX  DS    F                 MAXIMUM=
SARCSIZE EQU   *-SMRPSTRT        Size of APPLCNTS format
```

Figure 47. SAR APPLCNTS Event DSECT

Each of the APPLCNTS Fields can be further defined as follows:

Field	*Purpose*
CAPPL	is the name of the APPLICATION.
CTRGT	the VTAM APPLID the APPLICATION is known by (TARGET=).
CUSER	a binary count of the number of network elements logged onto The Network Director that have chosen this APPLICATION.
CTERM	a binary count of the number of terminals that have chosen this APPLICATION.
CMAX	the MAXIMUM= value associated with the APPLICATION.
CSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

APPLSTAT

The APPLSTAT Event is recorded each time a defined APPLICATION changes status.

The SMRPVAR layout is:

```
SMRASTAT DS    H                New status
SMRAHELD EQU   4                   Held
SMRAWAIT EQU   8                   Wait
SMRAACT  EQU   12                  Active
SMRADOWN EQU   16                  Down
SMRANAME DS    CL8               APPLICATION Name
SMRATRGT DS    CL8               VTAM APPLID
SMRASIZE EQU   *-SMRHSIZE        Size of APPLSTAT format
```

Figure 48. SMR APPLSTAT Event DSECT

The SARPVAR layout is:

```
SARASTAT DS    H                 New status
SARAHELD EQU   4                   Held
SARAWAIT EQU   8                   Wait
SARAACT  EQU   12                  Active
SARADOWN EQU   16                  Down
SARANAME DS    CL8               APPLICATION Name
SARATRGT DS    CL8               VTAM APPLID
SARASIZE EQU   *-SMRPSTRT        Size of APPLSTAT format
```

Figure 49. SAR APPLSTAT Event DSECT

Each of the APPLSTAT fields can be further defined as follows:

Field	***Purpose***
ASTAT	contains the new status of the APPLICATION.
ANAME	contains the defined Network Director name for the APPLICATION.
ATRGT	is the 8 characters used to identify this APPLICATION to ACF/VTAM.
FSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

INFOUPD

The INFOUPD Event is recorded each time a network user updates a Information file record (either a INFO topic or an Index record).

The SMRPVAR layout is:

```
SMRUFLAG DS    H                 Update Type
SMRUHDE  EQU   4                   INFO Screen
SMRUHIX  EQU   8                   INFO Index
SMRUSCRN DS    CL5               Screen or Index level updated
SMRUSIZE EQU   *-SMRHSIZE        Size of INFOUPD format
```

Figure 50. SMR INFOUPD Event DSECT

The SARPVAR layout is:

```
SARUFLAG DS    H                 Update Type
SARUHDE  EQU   4                   INFO Screen
SARUHIX  EQU   8                   INFO Index
SARUSCRN DS    CL5               Screen or Index level updated
SARUSIZE EQU   *-SMRPSTRT        Size of INFOUPD format
```

Figure 51. SAR INFOUPD Event DSECT

Each of the INFOUPD fields can be further defined as follows:

Field	*Purpose*
UFLAG	indicates whether a INFO topic or an Index has been updated.
USCRN	is the 5 byte numeric value associated with the INFO topic or the Index
USIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

LOGOFF

The LOGOFF Event is recorded each time a network user is logged off of The Network Director.

The SMRPVAR layout is:

```
SMRFFLAG DS    H                LOGOFF Event type
SMRFCMD  EQU   4                  Terminal User initiated
SMRFTIME EQU   8                  USER timed out
SMRFOP   EQU   12                 Administrator forced LOGOFF
SMRFAUTO EQU   16                 AUTOLOGOFF occurred
SMRFDROP EQU   20                 Terminal user issued DROP
SMRFSSI  EQU   24                 SSI caused LOGOFF
SMRFACCT DS    CL8              Account code
SMRFEXT  DS    CL8              Extension value
SMRFSIZE EQU   *-SMRHSIZE       Size of LOGOFF format
```

Figure 52. SMR LOGOFF Event DSECT

The SARPVAR layout is:

```
SARFFLAG DS    H                LOGOFF Event type
SARFCMD  EQU   4                  Terminal User initiated
SARFTIME EQU   8                  USER timed out
SARFOP   EQU   12                 Administrator forced LOGOFF
SARFAUTO EQU   16                 AUTOLOGOFF occurred
SARFDROP EQU   20                 Terminal user issued DROP
SARFSSI  EQU   24                 SSI caused LOGOFF
SARFACCT DS    CL8              Account code
SARFEXT  DS    CL8              Extension value
SARFSIZE EQU   *-SMRPSTRT       Size of LOGOFF format
```

Figure 53. SAR LOGOFF Event DSECT

Each of the LOGOFF fields can be further defined as follows:

Field	***Purpose***
FFLAG	contains an indication of what caused the LOGOFF.
FACCT	contains the Account: field from the ID area, when used.
FEXTN	contains the 8 byte Extension: field from the ID area.
FSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

LOGON

The LOGON Event is recorded each time a terminal user attempts to identify himself (whether successful or not).

The SMRPVAR layout is:

```
SMRNFLAG DS    H                LOGON Event type
SMRNOK   EQU   4                  Successful LOGON
SMRNPSWD EQU   8                  Password not matched
SMRNSEC  EQU   12                 Security System rejected
SMRNAIE  EQU   16                 Outside TIME or DAY
SMRNHELD EQU   20                 Network Element HELD
SMRNATE  EQU   24                 At the wrong TERMINAL
SMRNMAX  EQU   28                 MAXIMUM= exceeded
SMRNVPSW EQU   32                 VERIFY didn't work
SMRNNPSW EQU   36                 NEW-PSWD attempt
SMRNAUTH EQU   40                 AUTHENTICATION failed
SMRNTRY  DS    H                Attempt number
SMRNACCT DS    CL20             Account
SMRNEXTN DS    CL8              Extension
SMRNSIZE EQU   *-SMRHSIZE       Size of LOGON format
```

Figure 54. SMR LOGON Event DSECT

The SARPVAR layout is:

```
SARNFLAG DS    H                LOGON Event type
SARNOK   EQU   4                  Successful LOGON
SARNPSWD EQU   8                  Password not matched
SARNSEC  EQU   12                 Security System rejected
SARNAIE  EQU   16                 Outside TIME or DAY
SARNHELD EQU   20                 Network Element HELD
SARNATE  EQU   24                 At the wrong TERMINAL
SARNMAX  EQU   28                 MAXIMUM= exceeded
SARNVPSW EQU   32                 VERIFY didn't work
SARNNPSW EQU   36                 NEW-PSWD attempt
SARNAUTH EQU   40                 AUTHENTICATION failed
SARNTRY  DS    H                Attempt number
SARNACCT DS    CL20             Account
SARNEXTN DS    CL8              Extension
SARNSIZE EQU   *-SMRPSTRT       Size of LOGON format
```

Figure 55. SAR LOGON Event DSECT

Each of the LOGON fields can be further defined as follows:

Field	*Purpose*
NFLAG	contains an indication about whether the logon attempt was successful or not. If unsuccessful, this flag indicates why the logon attempt failed.
NTRY	is the count of consecutive failed logon attempts made by the terminal operator.
NACCT	contains the Account: field from the ID area, when used.
NEXTN	contains the 8 byte Extension: field from the ID area.
NSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

MSGDEL

The MSGDEL Event is recorded whenever a network user has Deleted a message within the Message Facility.

The SMRPVAR layout is:

```
SMRDTYPE DS    H                Type of message
SMRDCAST EQU   4                  Broadcast
SMRDMEMO EQU   8                  Memo
SMRDNOTE EQU   12                 Note
SMRDDEST DS    CL8              Destination
SMRDORIG DS    CL8              Origin
SMRDNAME DS    CL8              Message Name
SMRDLEN  DS    H                Length of the message
SMRDSIZE EQU   *-SMRHSIZE        Size of MSGDEL format
```

Figure 56. SMR MSGDEL Event DSECT

The SARPVAR layout is:

```
SARDTYPE DS    H                Type of message
SARDCAST EQU   4                  Broadcast
SARDMEMO EQU   8                  Memo
SARDNOTE EQU   12                 Note
SARDDEST DS    CL8              Destination
SARDORIG DS    CL8              Origin
SARDNAME DS    CL8              Message Name
SARDLEN  DS    H                Length of the message
SARDSIZE EQU   *-SMRPSTRT        Size of MSGDEL format
```

Figure 57. SAR MSGDEL Event DSECT

Each of the MSGDEL Fields can be further defined as follows:

Field	***Purpose***
DTYPE	indicates the type of message being Deleted.
DDEST	contains the destination for the message (wild characters are valid).
DORIG	contains the name of the network user that initiated (created) the message.
DNAME	is the message's name.
DLEN	a binary count of the size of the message.
DSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

MSGPRINT

The MSGPRINT Event is recorded whenever a network user has Printed a message within the Message Facility.

The SMRPVAR layout is:

```
SMRTTYPE DS    H                Type of message
SMRTCAST EQU   4                  Broadcast
SMRTMEMO EQU   8                  Memo
SMRTNOTE EQU   12                 Note
SMRTDEST DS    CL8              Destination
SMRTORIG DS    CL8              Origin
SMRTNAME DS    CL8              Message Name
SMRTPRTR DS    CL8              Where it was printed
SMRTLEN  DS    H                Length of the message
SMRTSIZE EQU   *-SMRHSIZE        Size of MSGPRINT format
```

Figure 58. SMR MSGPRINT Event DSECT

The SARPVAR layout is:

```
SARTTYPE DS    H                Type of message
SARTCAST EQU   4                  Broadcast
SARTMEMO EQU   8                  Memo
SARTNOTE EQU   12                 Note
SARTDEST DS    CL8              Destination
SARTORIG DS    CL8              Origin
SARTNAME DS    CL8              Message Name
SARTPRTR DS    CL8              Where it was printed
SARTLEN  DS    H                Length of the message
SARTSIZE EQU   *-SMRPSTRT        Size of MSGPRINT format
```

Figure 59. SAR MSGPRINT Event DSECT

Each of the MSGPRINT Fields can be further defined as follows:

Field	***Purpose***
TTYPE	indicates the type of message being Printed.
TDEST	contains the destination for the message (wild characters are valid).
TORIG	contains the name of the network user that initiated (created) the message.
TNAME	is the message's name.
TPRTR	is the name of the printer the message was printed on.
TLEN	a binary count of the size of the message.

TSIZE is an assembler symbol that is equated to the length (in bytes) of this event record type.

MSGSEND

The MSGSEND Event is recorded whenever a network user has Sent a message within the Message Facility.

The SMRPVAR layout is:

```
SMRSTYPE DS    H                Type of message
SMRSCAST EQU   4                  Broadcast
SMRSMEMO EQU   8                  Memo
SMRSNOTE EQU   12                 Note
SMRSDEST DS    CL8              Destination
SMRSNAME DS    CL8              Message Name
SMRSLEN  DS    H                Length of the message
SMRSSIZE EQU   *-SMRHSIZE       Size of MSGSEND format
```

Figure 60. SMR MSGSEND Event DSECT

The SARPVAR layout is:

```
SARSTYPE DS    H                Type of message
SARSCAST EQU   4                  Broadcast
SARSMEMO EQU   8                  Memo
SARSNOTE EQU   12                 Note
SARSDEST DS    CL8              Destination
SARSNAME DS    CL8              Message Name
SARSLEN  DS    H                Length of the message
SARSSIZE EQU   *-SMRPSTRT       Size of MSGSEND format
```

Figure 61. SAR MSGSEND Event DSECT

Each of the MSGSEND Fields can be further defined as follows:

Field	***Purpose***
STYPE	indicates the type of message being Sent.
SDEST	contains the destination for the message (wild characters are valid).
SNAME	is the message's name.
SLEN	a binary count of the size of the message.
CSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

MSGVIEW

The MSGVIEW Event is recorded whenever a network user has Viewed a message within the Message Facility.

The SMRPVAR layout is:

```
SMRWTYPE DS    H                Type of message
SMRWCAST EQU   4                  Broadcast
SMRWMEMO EQU   8                  Memo
SMRWNOTE EQU   12                 Note
SMRWDEST DS    CL8              Destination
SMRWORIG DS    CL8              Origin
SMRWNAME DS    CL8              Message Name
SMRWLEN  DS    H                Length of the message
SMRWSIZE EQU   *-SMRHSIZE       Size of MSGVIEW format
```

Figure 62. SMR MSGVIEW Event DSECT

The SARPVAR layout is:

```
SARWTYPE DS    H                Type of message
SARWCAST EQU   4                  Broadcast
SARWMEMO EQU   8                  Memo
SARWNOTE EQU   12                 Note
SARWDEST DS    CL8              Destination
SARWORIG DS    CL8              Origin
SARWNAME DS    CL8              Message Name
SARWLEN  DS    H                Length of the message
SARWSIZE EQU   *-SARPSTRT       Size of MSGVIEW format
```

Figure 63. SAR MSGVIEW Event DSECT

Each of the MSGVIEW Fields can be further defined as follows:

Field	*Purpose*
WTYPE	indicates the type of message being Printed.
WDEST	contains the destination for the message (wild characters are valid).
WORIG	contains the name of the network user that initiated (created) the message.
WNAME	is the message's name.
WLEN	a binary count of the size of the message.
WSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

RETURN

The RETURN Event is recorded each time a network element returns to The Network Director's control after having been sent to a subsystem.

The SMRPVAR layout is:

```
SMRRTRGT DS    CL8               Target's VTAM APPLID
SMRRACCT DS    CL20              Account
SMRREXT  DS    CL8               Extension
SMRRAPPL DS    CL8               Logical Application Name
SMRRSTRT DS    PL4               Time of selection
SMRREND  DS    PL4               Time of return
SMRRTIME DS    F                 Duration (in seconds)
SMRRSIZE EQU   *-SMRHSIZE        Size of RETURN format
```

Figure 64. SMR RETURN Event DSECT

The SARPVAR layout is:

```
SARRACCT DS    CL20              Account
SARRAPPL DS    CL8               Logical Application Name
SARRSTRT DS    PL4               Time of selection
SARREND  DS    PL4               Time of return
SARRTIME DS    F                 Duration (in seconds)
SARRSIZE EQU   *-SARPSTRT        Size of RETURN format
```

Figure 65. SAR RETURN Event DSECT

Each of the RETURN fields can be further defined as follows:

Field	*Purpose*
TRGT	is the 8 byte name the device was CLSDST PASSed to.
RACCT	contains the contents of the Account: field from the ID area.
REXT	contains the 8 character Extension: field from the ID area, when used.
RAPPL	is the name The Network Director knows the application by. This is the positional operand on the APPLICATION statement.
RSTRT	is the time of day that the terminal user chose the APPLICATION.
REND	is the time of day that the device returned to The Network Director from the subsystem.
RTIME	is a binary fullword representing the number of seconds the device was connected to the subsystem.
RSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

SELECT

The SELECT Event is recorded each time a network element selects a subsystem.

The SMRPVAR layout is:

```
SMRLTRGT DS    CL8               Target's VTAM APPLID
SMRLACCT DS    CL20              Account
SMRLEXT  DS    CL8               Extension
SMRLAPPL DS    CL8               Logical Application Name
SMRLSTRT DS    PL4               Time of selection
SMRLSIZE EQU   *-SMRHSIZE        Size of RETURN format
```

Figure 66. SMR SELECT Event DSECT

The SARPVAR layout is:

```
SARLTRGT DS    CL8               Target's VTAM Applid
SARLACCT DS    CL20              Account
SARLAPPL DS    CL8               Logical Application Name
SARLSTRT DS    PL4               Time of selection
SARLSIZE EQU   *-SARPSTRT        Size of RETURN format
```

Figure 67. SAR SELECT Event DSECT

Each of the RETURN fields can be further defined as follows:

Field	***Purpose***
LTRGT	is the 8 byte name the device was CLSDST PASSed to.
LACCT	contains the contents of the Account: field from the ID area.
LEXT	contains the 8 character Extension: field from the ID area, when used.
LAPPL	is the name The Network Director knows the application by. This is the positional operand on the APPLICATION statement.
LSTRT	is the time of day that the terminal user chose the APPLICATION.
LSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

VTAMERRS

The VTAMERRS Event is recorded each time a VTAM based RPL receives a non zero condition (non zero RTNCD or unexpected Sense codes).

The SMRPVAR layout is:

```
SMRVCMD  DS    CL8               Type of RPL or SNA Command
SMRVRTN  DS    F                 RTNCD
SMRVFD   DS    F                 FDBK
SMRVFD2  DS    F                 FDBK2
SMRVCAT  DS    F                 Sense Category
SMRVMOD  DS    F                 Sense Modifier
SMRVUSER DS    F                 User Sense
SMRVSIZE EQU   *-SMRHSIZE        Size of VTAMERRS format
```

Figure 68. SMR VTAMERRS Event DSECT

The SARPVAR layout is:

```
SARVCMD  DS    CL8               Type of RPL or SNA Command
SARVRTN  DS    F                 RTNCD
SARVFD   DS    F                 FDBK
SARVFD2  DS    F                 FDBK2
SARVCAT  DS    F                 Sense Category
SARVMOD  DS    F                 Sense Modifier
SARVUSER DS    F                 User Sense
SARVSIZE EQU   *-SARPSTRT        Size of VTAMERRS format
```

Figure 69. SAR VTAMERRS Event DSECT

Each of the VTAMERRS fields can be further defined as follows:

Field	*Purpose*
VCMD	contains a description of the associated RPL (RECEIVE, SEND, etc.).
VRTN	is the binary fullword representing the RTNCD from ACF/VTAM.
VFD	is the binary fullword representing the FDBK field from ACF/VTAM.
VFD2	is the binary fullword representing the FDBK2 field from ACF/VTAM.
VCAT	contains the sense category for the RPL.
VMOD	contains the sense modifier for the RPL.
VUSER	contains the user sense from the RPL.
VSIZE	is an assembler symbol that is equated to the length (in bytes) of this event record type.

Security System Considerations

ACF2

There is a variety of ways to configure The Network Director. If your installation has ACF2 installed as a system level security package, there are several additional alternatives that you should consider when configuring The Network Director for use in your environment.

You can instruct The Network Director to obtain from ACF2 directions on which APPLICATIONS to present to a network user. This can be accomplished utilizing two different approaches. They are:

1. LIDREC Bit Mapping
2. Generalized Resource Rules

A more detailed description of each approach follows.

LIDREC Bit Mapping

Associated with each ACF2 logonid is a logonid record (LIDREC) that can be configured at your installation to contain individual bits associated with "permission" to use a specific subsystem. The Network Director can be instructed to test this *bit* by specifying the name of the bit on the APPLICATION FDE-NAME= operand. (E.G. FDE-NAME=TSO specifies the bit associated with TSO authorization).

To make use of this option, the FDE-NAME value will have to have been included in the ACF2 FDR generation at your installation. If it has been generated, The Network Director will obtain its location in the LIDREC from the FDR at execution time and will use the information in the specific FDE to apply the appropriate test at Application Selection Panel creation to decide whether to include the application choice or not.

Definition of new fields in the FDR is described in the ACF2 System Programmer's Guide under the topic "ACF2 Field Definition Record Generation" and the specific discussion of the @CFDE Macro.

In order for The Network Director to utilize the defined field as an application authorization, it must be defined in the FDR in use at execution time and the field must be defined as a BIT field.

Generalized Resource Rules

The Network Director also supports the use of ACF2 generalized resource rules to dictate when a particular user should receive a particular selection. However, rather than utilize the traditional ACF2 resource validation call, The Network Director utilizes a function within ACF2 Version 5.0 and up called *mass interpret*.

This mass interpret function allows The Network Director to activate resource rule interpretation for all the items associated with a single Application Selection Panel with a single call to ACF2. To avoid excessive disk operations during this process, the ACF2 command is utilized to set operating characteristics of The Network Director as an ACF2 calling subsystem. See "Directory Build" on page 206 for more information.

Activation of the generalized resource rule processing is accomplished in the network definition specification of the possible APPLICATIONS. Insertion of the special keyword **ACF2** indicates that the list of applications that The Network Director would normally present to the user should be subjected to the ACF2 resource rule screening.[21]

Configuration Parameter Specification

An example of a Configuration Parameter entry is:

```
ACF2 TYPE=TND,RULES=RESIDENT

APPLICATION TSO,TARGET=TSO
APPLICATION ADMIN,TARGET=TNDADMIN
APPLICATION CICS,TARGET=CICSDBDC

DEFAULT APPLICATIONS=(TSO,ADMIN,CICS,ACF2)

USER ++++++++
```

Figure 70. Resource Rule Parameter Syntax

When The Network Director detects the character string **ACF2** as an element in the APPLICATIONS= string (on the DEFAULT or applicable TERMINAL, USER, and/or GROUP statements), it will create an appropriate parameter list to have ACF2 validate the selection entries. ACF2 will invoke resource rule logic for each entry in the list based upon the CLASS of R (for resource) and TYPE set by the Network Administrator in the Configuration Parameters on the Network Director statement named ACF2 (**TND** in the preceding example).

The approach portrayed in the preceding figure always passes all applications to ACF2 for rule interpretation. It is possible to utilize The Network Director's other facilities (GROUP=ACF2, LIDREC bit mapping, or simple USERS definitions) to refine which choices ACF2 will select from. Thus, restricting the APPLICATIONS that are specified

---

[21] The ACF2 **APPLICATION** does not need to be defined as a valid APPLICATION and will not appear on the Application Selection Panel.

for presentation to ACF2 for mass interpret can further reduce overhead associated with resource rule interpretation.

As another alternative, if the Network Administrator defines only ACF2 as an APPLICATIONS= operand, The Network Director will create the parameter list for ACF2 processing from **all** defined applications.[22]

Thus, the following figure will produce the same results as the preceding one (presuming the network only has three applications defined):

```
ACF2 TYPE=TND,RULES=RESIDENT

APPLICATION TSO,TARGET=TSO
APPLICATION ADMIN,TARGET=TNDADMIN
APPLICATION CICS,TARGET=CICSDBDC

DEFAULT APPLICATIONS=ACF2

USER ++++++++
```

Figure 71. ACF2 Application Selection

This approach allows ACF2 to control what selections are presented to individual users without putting large effort into creating and maintaining The Network Director's Configuration Parameters.

[22] Usage of Generalized Resource Rules via this specification technique overrides other usage restrictions within The Network Director (SELECTIONS=, FDE-NAME=, etc.).

ACF2 Resource Rule Syntax

The preceding examples discussed the parameters required in The Network Director to activate the ACF2 Resource Rule logic. The following example shows how to authorize various logonids access to the various selections discussed previously (presuming the TYPE is set to **TND** within ACF2).

```
SET RESOURCE(TND)

$KEY(ADMIN) TYPE(TND)
 UID(****OPR) ALLOW
 UID(****SSD) ALLOW
 UID(*) PREVENT

$KEY(CICS****) TYPE(TND)
 UID(*) ALLOW

$KEY(TSO) TYPE(TND)
 UID(****OPR) ALLOW
 UID(****USER) PREVENT
```

Figure 72. ACF2 Resource Rule Syntax

Naturally, any combination of ACF2 operands are valid associated with the rule (TIME, SHIFT, grouping via cross reference resources, etc.).

Directory Build

One side effect of the mass interpret processing associated with the resource rule processing is the potential for a large amount of I/O processing by ACF2/MVS to the rules database. To address this, The Network Director has implemented the statement or command called the ACF2 command (See "ACF2" on page 23). The ACF2 command issues the appropriate ACF2 call to execute what is known as an in storage *directory build*. This causes ACF2 to retain the resource rules in storage (Version 5 of ACF2 will place the rules above the 16M line if the operating system supports native XA operation).

This option provides the ability to significantly reduce the amount of overhead with the processing of ACF2 rule processing by eliminating the I/O operations necessary to the rule data set. The ACF2 command also provides the vehicle to "refresh" the rules for The Network Director after a change has been made to the ACF2 generalized resource rules. Issuing the command again from Network Administration will generate a refresh operation within ACF2. This will cause the updated rules to be loaded to storage. If the refresh is not done, The Network Director will continue to operate with the older copy of the rules that were loaded the first time the ACF2 command was issued.

Mini-LID Support

The Network Director will now test an associated bit in an ACF2/MVS user's logonid record (LIDREC) to establish if the user should receive the selection or not. If the corresponding bit is on, the selection will be included. If the bit is not on, the selection will be bypassed. You can activate this logic by using the FDE-NAME operand of the APPLICATION statement (See "APPLICATION" on page 25 or "LIDREC Bit Mapping" on page 203 for more information).

This support within The Network Director will occur without regard for whether The Network Director is using the full LIDREC or a mini-LID. At execution time, The Network Director establishes whether it is using a mini-LID or not by looking up the MUSASS name it is operating with (if any). The appropriate translations to offsets within the full LIDREC or mini-LID are done at the time the APPLICATION statement is parsed by searching the FDEs chained from the FDR.

ACCVT Locator Logic

Previous versions of The Network Director required that the ACF2/MVS SVC number be provided in the Configuration Parameters. The Network Director will locate the ACF2/MVS ACCVT control block and extract the SVC number dynamically. You can activate this logic by simply removing SECURITY-SVC= from the GLOBALS statement.

If you choose to leave the SECURITY-SVC operand in the GLOBALS definition, it will be honored. NRS recommends that you remove the operand (any future installation of a new ACF2 with a changed SVC number will then not require an update to The Network Director's definitions).

Logical Grouping

Specifying GROUP=ACF2 on an associated USERS definition causes The Network Director to extract the group name from the ACMCB for the user (presuming a logon activity is successful). The Network Director will automatically extract the first 8 characters of the UID string and attempt to use it as a GROUP identifier.

If this extraction is not acceptable, your installation can specify different characters for making up the GROUP name via the use of EXT19 (GROUP Assignment). A sample exit for this purpose is provided on the distribution library (named TNDEXT19).

Once EXT19 and/or the UID extraction is complete, The Network Director will utilize the resulting 8 byte value to establish a group connection. If unsuccessful, The Network Director will then attempt to connect the user to the GROUP definition for **ACF2**, if present. This mechanism can be utilized to connect a user with an otherwise undefined GROUP to a common location.

Inherit Processing

The Network Director offers a facility generally identified as Single System Image. This concept identifies the processes associated with automating the signon process to the various subsystems (CICS, TSO, etc.). The Network Director generally accomplishes this by passing the logonid and password to the subsystem and automating the signon process in the receiving subsystem.

This implies two items that may not be desirable (from a strict security standpoint). They are:

1. The Network Director must "remember" the user's password and keep it available for "passing" to the subsystem
2. the password is sent through ACF/VTAM when the device is forwarded to the subsystem

ACF2/MVS Version 5.0 and up supports an option called **inherit processing**. This support requires specific activities on the part of the subsystem initially accomplishing system entry validation and selection activities. These activities and communications with ACF2/MVS can be utilized to eliminate the two exposures mentioned above. ACF2/MVS "inheritance" implies that the terminal operator will not necessarily be required to complete a total system entry validation process at the receiving subsystem again because ACF2 will recognize that the terminal operator has already successfully passed system entry validation.

This is accomplished by passing information to ACF2 in the receiving subsystem that will cause it to recognize that the incoming user has already had entry validation done for it (hence the name *inheritance*). This can be used between any ACF2 managed nodes that have the ability to share ACF2 data bases and that support inheritance (ACF2/MVS Version 5.0 and up).[23]

---

[23] Inheritance does NOT work across ACF2 nodes in distributed data base (DDB) installations. This is a function of the design of DDB and Inheritance within ACF2 and not introduced by The Network Director.

You can activate this logic in The Network Director by specifying &INHERIT in the INITIAL-DATA string where you would normally insert the &PASSWORD token.[24] Thus, for TSO specify:

```
APPLICATION TSO,TARGET=TSO,
        INITIAL-FUNCTION=LOGON,
        INITIAL-DATA=(&NAME,'/',&INHERIT)
```

Figure 73. Specifying ACF2 Inheritance

Account Code Validation

The Network Director can also be configured to obtain an account code from ACF2 at logon time.

Account codes can also be validated against the ACF2 resource type TAC to verify that a terminal operator has entered a valid code. This will be done **only if** VLD-ACCT (LIDT4ACC) is on in the users LIDREC and the field LIDTFLG4 is included in the Logonid record used within The Network Director (any mini-LID specified should contain the field).

Specify ACCOUNT=ACF2 on the PROFILE statement associated with the USERS, TERMINALS, or GROUP definition. When The Network Director sees a PROFILE with this setting, two activities will occur.

1. If a terminal operator successfully logs on via ACF2, the first 20 characters of LIDACCT will be automatically inserted into The Network Director's Account: field (unless the operator specified one during logon)

2. Regardless of origin, the Account: field value will be checked against the TAC resource types within ACF2.

If the account field value is not acceptable to ACF2, the logon attempt will fail with an appropriate message.

This function is quite useful if you use (or are planning to use) accounting records (SMRs or SARs) to collect information associated with network usage. In addition, the account field can be passed to the subsystems for subsequent account setting (use the &ACCOUNT variable in the INITIAL-DATA operand).

---

[24] The ACF2 INHERIT function requires that The Network Director be APF authorized to make use of &INHERIT properly.

DIRECTOR

The Network Director can be configured to be the responsible password management system within your installation. NRS recommends one of the standard system security offerings for comprehensive security, but offers GLOBALS SECURITY=DIRECTOR as an alternative for installations that require only that the terminal user pass a password validation to gain entrance and utilize the host system.[25]

While The Network Director is not intended to be a full function system security offering, there are two commonly accepted security standards that are equally applicable in The Network Director's environment. These standards are supported by the technical implementation of The Network Director's SECURITY=DIRECTOR and should be discussed and understood in your installation prior to implementation.

1. Passwords should be known and set only by the end user (the Network Administrator should not know or have a list of current passwords).
2. Passwords should be periodically changed with guidelines mandating a reasonable password selection by the user.

Figure 74. General Password Concepts

When SECURITY=DIRECTOR is in effect, any terminal user that attempts to logon to The Network Director with a USER definition that indicates PASSWORD=YES will be subject to the following validations:

1. an AIB (Access Information Block) must have been previously allocated by a Network Director Network Administrator
2. the terminal user must provide the password that was previously stored in the AIB to gain access to the system (errors and notifications are issued as in any other security system interface)
3. the terminal user must periodically change the password as indicated in PSWD-OPTIONS (see "PSWD-OPTIONS" on page 56)
4. any new password is subject to the associated checks and processes implied by the PSWD-OPTIONS and ATTRIBUTES operand settings (see "ATTRIBUTES" on page 47)

---

[25] The Network Director does **not** provide a mechanism for other ACF/VTAM subsystems to make use of the information stored in the External File. It is the responsibility of the installation and the associated subsystems to implement a mechanism to resolve any SSI related issues.

Establishing the Access Information Block

Any Network Administrator authorized to establish USER definitions can create or maintain the Access Information Block (AIB) necessary to register a new user's password with The Network Director. This is done via use of the SHOW command (E.G. SHOW ACCESS=newuser).

Issuing SHOW ACCESS will display **only the AIBs in storage**. You must issue SHOW ACCESS=value to cause The Network Director to retrieve the AIB from the External File if the AIB is not already in storage.[26]

If the AIB exists for the user, it will be retrieved from the External File and presented to the Network Administrator. If it is not in existence, the AIB can be added by issuing the ADD primary command. The resulting initial ACCESS panel will look similar to the following figure:

Figure 75. The Access Information Block SHOW Panel

The fields in this display that are applicable to Network Director password maintenance are:

Field Prompt	*Field Value*
Last Logon	displays information associated with the last time this user logged onto the system
Name	the individual's name (used for information in the LOG display, by the NO-PATTERNS edit, and the system directory)

[26] This is a side effect of The Network Director attempting to minimize it's usage of main storage by allowing AIBs that are not in current use to be "paged" back out to the External File.

Network Element the userid that will be associated with the individual being registered

Phone the individual's phone number (used for informational displays and the system directory)

Password used to enter the **initial** password value (the current password is never displayed). The Network Director will automatically force a user through a password change after using an initial password.

This field can also be used to "reset" an existing user's password to a new value (if the user forgets the password, etc.). **Any change to this field** will require that the user change this password to a new one upon the first attempt to access the system under control of the AIB.

Additional information about the contents of the Password field may be located just to the right of the Password data field in the SHOW panel. The possible values are:

blanks indicates that there has been no action taken against the AIB (no password has been entered or activated, and the user has not set a new password). This will be the normal case when your installation is using Extended Authentication, but SECURITY=DIRECTOR is not in effect.

Is set indicates that the user defined by this Access Information Block has successfully set a password. Entering a new password value into the Password field will update the AIB with the new value and will **require** that the user set a new password the next time a logon is attempted (the user will need to know the password you have just entered).

Force is present when the Access Information Block has had an initial password entered into the Password field, but the user defined by the AIB has not signed on and changed the password yet.

Administering SECURITY=DIRECTOR

When you have elected to operate with SECURITY=DIRECTOR in effect, there are several procedural items you should be aware of.

Activation of the internal password validation is accomplished by specifying GLOBALS SECURITY=DIRECTOR (see "SECURITY" on page 81). This instructs The Network Director that password validation is to be accomplished within The Network Director and that there is not an external security system available.

Identifying the precise individuals that are subject to the password validation is accomplished by specifying PASSWORD=YES on the applicable USER, GROUP, or DEFAULT statements (remember, wild characters are valid on the USER definition to assist in "mapping" the userids). You can set this value into effect on only that portion of the logical network that you would like subject to password checking (this is useful when migrating usage into an existing network).

Procedures

Administering a system with SECURITY=DIRECTOR in effect is made up of responding to a series of requests from the user base. The following procedures are offered as examples of how a Network Administrator could respond to the various requests.

Setting a New Password

The password and new password is entered into The Network Director's Identification Area, which is located at the bottom of The Network Director's panels. The user should tab to the appropriate input field and enter the information necessary to gain access to the system.[27] It is also possible to enter the new password in the Password: field by entering it after the current password and separating the two with a slash ("/").

Additional information about logging on is available under "Identifying Yourself" in the *Network User's Guide* (NRS Publication TND-0202).

---

[27] The precise format of the Identification Area is controlled by the FORMAT-ID that is in effect for the device.

Registering a New User

The following steps can be followed to establish a user within The Network Director that is susceptible to internal password checking (provided that the Configuration Parameters are set as discussed in "Administering SECURITY=DIRECTOR" on page 213).

1. Access the Network Administration internal APPLICATION
2. Issue a SHOW ACCESS=newuser command (where "newuser" is the userid of the individual you would like to define)
3. If a SHOW menu is presented with a TND0342 (AIB not located) message, then enter "ADD" and press ENTER
4. On the SHOW ACCESS detail panel enter the Userid into the field labeled "Network Element" and the initial password into the "Password" field. These items are required.
5. Optionally, enter the individual's Name and Phone into the appropriate fields.
6. Press PF3 to save the Access Block
7. The user may now attempt to signon to the system, will have to know the password you just set, and will be required to set a new password.

Reset an Existing Password

The following steps can be followed to reset a password for an existing user.[28] This will occur when the user has forgotten the current password, etc.

1. Access the Network Administration internal APPLICATION
2. Issue a SHOW ACCESS=newuser command (where "newuser" is the userid of the individual you would like to modify)
3. On the SHOW ACCESS detail panel enter the password that the user will use to access the system with. The literal to the right of the Password data field should change from "Is set" to "Force".
4. Press PF3 to save the Access Block
5. The user may now attempt to signon to the system, will have to know the password you just set, and will be required to set a new password.

---

[28] For security reasons, The Network Director contains no manner to display in clear text form the current password value. Philosophically, the current password should be known only by The Network Director and the end user. For this reason, when a user forgets the password, the Network Administrator can only set a new value to reinstate the user.

Suspending a User

You can temporarily keep a user from logging on to The Network Director by holding the AIB associated with the user. You can accomplish this by:

1. Accessing the Network Administration internal APPLICATION
2. Issue a SHOW ACCESS=newuser command (where "newuser" is the userid of the individual you would like to suspend)
3. Press PF3 to return to the SHOW menu
4. Move the cursor to the underscore in front of the Access Block for the user, enter "H" for Hold, and press ENTER
5. The AIB will now be marked "Held" and any attempt by the user to access the system will be rejected.

Reinstating a User

You can reactivate a held or suspended user by following these steps:

1. Accessing the Network Administration internal APPLICATION
2. Issue a SHOW ACCESS=newuser command (where "newuser" is the userid of the individual you would like to reinstate)
3. Press PF3 to return to the SHOW menu
4. Move the cursor to the underscore in front of the Access Block for the user, enter "R" for Release, and press ENTER
5. The AIB will now be marked "Active" and the user can access the system normally.

Deleting a User

Removal of a user from the internal password mechanism consists of deleting the AIB. This is accomplished by:

1. Accessing the Network Administration internal APPLICATION
2. Issue a SHOW ACCESS=newuser command (where "newuser" is the userid of the individual you would like to reinstate)
3. Press PF3 to return to the SHOW menu
4. Move the cursor to the underscore in front of the Access Block for the user, enter "D" for Delete, and press ENTER
5. The AIB will now be marked "Deleted" and the necessary work to ERASE it from the External File will be scheduled. Once complete, the AIB will be eliminated from the main storage chains. The user is no longer identified to the system and will be unable to logon.

RACF

The following extended facilities are available, if RACF is your installation security package.

Logical Grouping

Specifying GROUP=RACF on an associated USERS definition causes The Network Director to extract the group name from the ACEE for the user (presuming a logon activity is successful). The Network Director will automatically extract the the default connect group and attempt to use it as a GROUP identifier. If there is no defined GROUP with the same name, The Network Director will attempt to connect the user to a GROUP defined as **RACF**.

Specifying Connect Group

It is also possible for the terminal operator to specify the RACF Connect Group desired. Specifying EXTENSION=RACF on the applicable definition statement instructs The Network Director to provide the value entered in the Extension: field of the Id area to RACF as the requested Connect Group. If valid, the user will then be connected to that RACF Connect Group and it will be usable as The Network Director's GROUP (GROUP=RACF) or available for passing to the subsystems (INITIAL-DATA=&EXTENSION).

Thus, the terminal operator can specify the RACF Group desired. If no Extension value is provided, The Network Director will utilize the RACF default Connect Group.

APPLICATION Authorization

If your installation has specified OPSYS=MVS and SECURITY=RACF on the GLOBALS statement, and the user has logged on via RACF, each APPLICATION authorized via the applicable APPLICATIONS= operand that has a PRIVILEGE operand will have the values of the PRIVILEGE operand compared against the list of RACF connect groups that the user is a member of.[29]

The APPLICATION will be placed on the Application Selection Panel if any one of the PRIVILEGE operand values match any one of the items in the RACF connect group list. This scan is accomplished by locating the ACEE in The Network Director's address space and comparing each entry in the group list with each entry in the PRIVILEGE operand.

---

[29] The list of groups option will have to have been set for The Network Director to receive a complete connect group list from RACF. This is activated by specifying SETROPTS GRPLIST to RACF. If NOGRPLIST is in effect, only APPLICATIONS with no PRIVILEGE requirements or PRIVILEGEs equal to the user's default connect group will appear on the Application Selection Panel.

As an example, assume that a user with the RACF Userid of SYS140 logged onto the system. The SYS140 user has been defined within RACF as being logically related to four Connect Groups, identified as SYSTEMS, OPERS, CICSUSER, and IMSTEST. The following Configuration Parameters are active within The Network Director:

```
APPLICATION TSO,TARGET=TSO,
         PRIVILEGE=(SYS+++++,PGMRS,USERS,OPERS)
APPLICATION CICSTEST,TARGET=CICS004,
         PRIVILEGE=(CICS++++,PGMRS)
APPLICATION CICSPROD,TARGET=CICS001,
         PRIVILEGE=(PGMRS,USERS)
APPLICATION IMSPROD,TARGET=IMSDB,
         PRIVILEGE=(USERS,IMS+++++)
*
USERS SYS+++++,APPLICATIONS=(TSO,CICSTEST,CICSPROD,IMSPROD)
```

The Network Director will log the user on and extract the APPLICATIONS= list of potential selections, which includes all four defined applications. During selection panel creation, The Network Director will evaluate each of the 4 application's PRIVILEGE operand values against the RACF List of Groups associated with SYS140.

TSO will be permitted because the SYS140 user is connected to the SYSTEMS group, which matches the first operand pattern of the TSO PRIVILEGE= specification (SYS140 matches SYS+++++).

CICSTEST is also permitted because the third RACF Connect group for the user (CICSUSER) matches the first PRIVILEGE operand value (CICS++++)

CICSPROD will not appear on SYS140's Application Selection Panel because neither of the specified PRIVILEGE operands (PGMRS or USERS) appear in the List of Groups for SYS140

IMSPROD does appear in the Application Selection Panel because the last RACF Connect Group (IMSTEST) does match the final PRIVILEGE operand for IMSPROD (IMS+++++)

The PRIVILEGE operand can be utilized to add an additional check to the Application Selection Panel composition, but can also be utilized to logically "move" the APPLICATIONS= authorization completely to a RACF based mechanism. To accomplish this, your installation must have a way to relate each APPLICATION to one or more RACF connect groups. Specify which connect groups have access to the APPLICATION by placing the list of connect group names on the APPLICATION PRIVILEGE operand. Then specify all the APPLICATIONS on the DEFAULT statement. This instructs The Network Director to allow every user access to every APPLICATION, but RACF controls the actual selection entries by which connect groups the user is a member of.

TopSecret/MVS

The **TopSecret/MVS** interface allows you to reduce duplicate maintenance of authorizations in TopSecret/MVS and The Network Director, as well as improve the information available within The Network Director for individual users. The TopSecret/MVS interface will:

1. retrieve the user's name from TopSecret/MVS, place it into The Network Director's System Directory, and use its value in several common Network Director messages (you may make use of it via the &USER-NAME variable)

2. obtain the TopSecret/MVS Department and Division values assigned to the individual user. This will be useful if you would like The Network Director to categorize users by their TopSecret/MVS Department or Division value

3. allocate storage within The Network Director's address space for the TopSecret list of facilities that the terminal operator is authorized for. This can be used with the APPLICATION PRIVILEGE operand within The Network Director to dynamically determine the contents of The Network Director's Application Selection Panels.

&USER-NAME

The Network Director will contact TopSecret/MVS (via the CA provided TSSAI routine at the 4.2 level or higher) and retrieves the user's name, as it is known to TopSecret/MVS. This name is placed into The Network Director's System Directory and can be used in LOGOs, etc. via use of the &USER-NAME variable.

It is also automatically inserted into several standard Network Director messages to improve the readability of the Administrator's LOG. E.G. When a user successfully completes logon, TND0165S will now include the TopSecret/MVS derived name:

```
TND0165S Id USER - USER'S NAME is now active at LUNAME
```

The use of the "USER'S NAME" in various locations can be of great assistance to the HELP desk and other support personnel.

Dynamic GROUP Support

The TopSecret/MVS interface dynamically extracts the TopSecret/MVS Department and Division values and places them into the System Directory. They can be referenced in LOGOs, INFO panels, or messages via use of the &DIRGRP or &DIRDEPT variables.

The Network Director can also dynamically assign a specific user to a Network Director GROUP based upon the value stored in TopSecret/MVS's Division or Department values. E.G. Assume that an individual named SAM is in the TopSecret/MVS Division ADMIN and Department SYSTEMS. If The Network Director is operating with the following partial definitions:

```
GLOBALS SECURITY=TOPSECRET
GROUP ADMIN,APPLICATIONS=(ADMIN,CICSPROD)
GROUP SYSTEMS,APPLICATIONS=(TSO,NETVIEW)
USER S+++++++,GROUP=TSSDEPT,PASSWORD=YES
```

When SAM successfully provides a password approved of by TopSecret/MVS, The Network Director will locate the USER definition that matches (S+++++++ in our example). The Network Director detects the specification of TSSDEPT on the GROUP operand and will search Network Director GROUP definitions for a GROUP equal to SYSTEMS (SAM's TopSecret/MVS Department assignment). When it is located, The Network Director will present SAM with a menu containing TSO and NETVIEW, which are the only elements allowed by the SYSTEMS GROUP definition.

Specification of GROUP=TSSDIV on the S+++++++ definition would cause The Network Director to assign SAM to the ADMIN GROUP instead, which would cause ADMIN and CICSPROD to be presented on the menu.

This mechanism becomes useful if you develop a strategy that adopts menus by TopSecret/MVS Division or Department code.

PRIVILEGE Support

The Network Director also extracts the TopSecret/MVS list of authorized facilities and keeps it in storage while the user is logged on. This list can then be utilized to determine which APPLICATIONs the user should receive. E.G. Assume that SAM is authorized with TopSecret/MVS for the BATCH, TSO, and PAYROLL facilities. Given the following Network Director parameters:

```
GLOBALS SECURITY=TOPSECRET
APPLICATION TSO,PRIVILEGE=(TSO)
APPLICATION CICS12,PRIVILEGE=(ONLINE,COSTS)
APPLICATION CICS23,PRIVILEGE=(PAY+++++,ONLINE)
APPLICATION NETVIEW,PRIVILEGE=(SYSTEMS)
APPLICATION ADMIN,PRIVILEGE=(SYSTEMS)
DEFAULT APPLICATIONS=(TSO,CICS12,CICS23,NETVIEW,ADMIN)
USER S+++++++,PASSWORD=YES
```

When SAM logs on, The Network Director will begin to include all the APPLICATIONS that have been defined on the DEFAULT definition. However, as it places each element into the menu, it will compare the list of PRIVILEGE operands against the list of authorized facilities associated with the user. SAM will receive only TSO and CICS23 on his menu because the PRIVILEGEs required for CICS12, NETVIEW, and ADMIN are not in his facilities list (note that wild characters are valid).

This mechanism can be used to eliminate the need to specify individual APPLICATIONS on specific definitions. In practice, some installations have defined all the APPLICATIONS one time (on the DEFAULT definition) and allowed the security system's facilities list to dictate which user gets which items.

Note: The PRIVILEGE operand can have multiple operands any of which can be made up of wild characters. If **any match**, then The Network Director will present the menu choice.

Technical Notes

The information being utilized by The Network Director is retrieved via usage of the TopSecret/MVS TSSAI (Application Interface) routine. The interface was written for the TopSecret/MVS 4.2 level. It has been tested with both 4.2 and 4.3 releases of TopSecret/MVS.

It is important to note that the 4.2 TSSAI routine is incapable of operating in 31 bit addressing mode. Therefore, The Network Director locates appropriate parameter lists below the line and switches to 24 bit AMODE prior to calling TSSAI. After calling TSSAI, The Network Director returns to 31 bit AMODE and relocates the TopSecret/MVS provided information above the line (to conserve on storage below the line).

TopSecret/VM

There are many manners in which TopSecret/VM and The Network Director can work together to enable the security checking desired at your installation. If your installation is using TopSecret/VM, you should consider the following alternatives (in addition to basic userid and password checking):

1. DIVISION and DEPARTMENT Support

2. TopSecret/VM Resource Support

DIVISION and DEPARTMENT Support

The Network Director retains the TopSecret/VM Department and Division ACID values from the TSS LIST result that occurs at logon time and has them available for reporting (DISPLAY NET=). In addition, The Network Director can be configured to utilize one of these values as the GROUP assignment for the user logging on. Specify GROUP=TSSDIV (for Division) or GROUP=TSSDEPT (for Department) on the appropriate Network Director definition statement and The Network Director will retrieve the appropriate value from TopSecret/VM and attempt to assign the user to The Network Director GROUP of the same name.

As an example, assume the following TopSecret/VM ACID characteristics:

```
tss list(testuser)
ACCESSORID = TESTUSER  NAME       = TEST USER ONE
TYPE       = USER      FACILITY   = VM
DEPT ACID  = PAYROLL   DEPARTMENT = PAYROLL ADMINISTRATION
DIV ACID   = ADMIN     DIVISION   = GENERAL ADMINISTRATION
CREATED    = 01/10/95  LAST MOD   = 01/10/95
LAST USED  = 01/10/95 13:37 CPU(NRS ) FAC(VM     ) COUNT(00016)
```

Assume also the following Network Director definitions:

```
GLOBALS SECURITY=TOPSECRET,OPSYS=VM
GROUP   PAYROLL,APPLICATIONS=(PAYABLES,CMS,MVSNET)
GROUP   ADMIN,APPLICATIONS=(STOCK,PERSON)
USERS   TESTUS++,GROUP=TSSDEPT,PASSWORD=YES
USERS   TEST++++,GROUP=TSSDIV,PASSWORD=YES
```

When TESTUSER accesses The Network Director by providing a TopSecret/VM approved combination of Id: and Password:, The Network Director search the USERS definitions from the top down. The USERS definition for TESTUS++ will be located. The GROUP=TSSDEPT instructs The Network Director to obtain the department ACID value of *PAYROLL* from the TSS LIST command and use that to connect to a Network Director GROUP. As a result, TESTUSER will receive PAYABLES, CMS and MVSNET on the resulting Application Selection Panel.

If the TESTUS++ definition is not present, the TEST++++ definition will apply and TESTUSER will be assigned to The Network Director GROUP of ADMIN and will receive the selections identified by the STOCK and PERSON APPLICATION definitions.

If the resulting GROUP value is not located within The Network Director's definitions, The Network Director will attempt to connect to a GROUP with the literal identifiers of *TSSDEPT* and *TSSDIV*, as appropriate. If these are not located, no GROUP assignment will occur.

Resource Support

TopSecret/VM provides a large range of facilities to manage and control *resources* within the processing environment. It reserves many keywords on the CREATE, ADDTO, PERMIT, etc. commands to allow a Security Administrator to control access to the resources.

An individual Network Director selection (APPLICATION) can be thought of as a TopSecret/VM *resource*, which can be controlled in the same manner as access to a mini-disk or any other resource. To provide this support, The Network Director recognizes the APPLICATION PRIVILEGE operand as specifying a TopSecret/VM resource, which permits access to the associated selection. This *resource* is called the DIRECTOR[30] resource in this document, but can be referenced by the *class* name that you select at your installation.

This optional Network Director facility can be utilized to allow TopSecret/VM to administer the individual selections on all Network Director Application Selection Panels. Essentially, the administration of the contents of the Application Selection Panel can be moved from The Network Director's parameters to TopSecret/VM's Security file.

---

[30] Whenever this document references the literal string of DIRECTOR, you can replace it with the character string of your choice. DIRECTOR is used in this manual only to clarify the examples.

As an example, assume the following Network Director parameters:

```
APPLICATION ADMIN,TARGET=TNDADMIN,TITLE='Network Administration',
            PRIVILEGE=(ADMIN,SCA)
APPLICATION CMS,TARGET=VM,TITLE='CMS - Programming',
            PRIVILEGE=(PROG,ADMIN)
APPLICATION PAYROLL,TARGET=CICS,TITLE='Payroll Inquiry',
            PRIVILEGE=(PAYROLL)
USERS ++++++++,PASSWORD=YES,APPLICATIONS=(ADMIN,CMS,PAYROLL)
```

Assume also the following TopSecret/VM commands have been previously issued:

```
 TSS ADD(RDT) RESCLASS(DIRECTOR) RESCODE(2E) ATTR(DEFPROT)

 TSS ADDTO(DIRECTOR)  DIRECTOR(ADMIN,PROG,PAYROLL)

 TSS PERMIT(TS001)    DIRECTOR(PROG)
 TSS PERMIT(TESTUSER) DIRECTOR(PAYROLL) FOR(1)
 TSS PERMIT(SYSTEMS)  DIRECTOR(ADMIN,PAYROLL)
```

All terminal users that successfully pass TopSecret/VM's userid and password check will be assigned to the USERS definition. The Network Director will select the APPLICATIONS named ADMIN, CMS, and PAYROLL from the USERS definition and then apply individual resource checks on behalf of the user based upon the PRIVILEGE operands of the APPLICATION statement. The TS001 user will end up with only the APPLICATION named CMS on the Application Selection Panel because only the CMS APPLICATION has PROG on the PRIVILEGE operand.

TESTUSER will have only the PAYROLL application on the menu and only for the duration set as a result of the FOR(1) operand.

The SYSTEMS user will have all the APPLICATIONS on the Application Selection Panel. PAYROLL allows the PAYROLL APPLICATION and ADMIN allows the ADMIN and CMS APPLICATIONs.

Essentially, the Application Selection Panel will contain the selection if the user logged on via The Network Director and TopSecret/VM **and** the user's ACID has been PERMITted to one or more of the DIRECTOR resources defined on the PRIVILEGE operand of the APPLICATION definition.

VM

Specifying SECURITY=VM instructs The Network Director to:

1. validate userid and password combinations for PASSWORD=YES situations against the VM system directory

2. dynamically set The Network Director's GROUP assignment from the ACIGROUP entry for GROUP=VM specifications

As a result of how the VM Directory operates, other security "package" options (password update, error message generation, etc.) are **not available**. These types of functions require an additional security package (RACF, ACF2, TopSecret/VM, etc.). You can consider using SECURITY=DIRECTOR as an option if no security package is planned.

INFO Facility

The Network Director provides a generalized Information Facility to aid network users in the use of the network. It can also be expanded to provide general information associated with the entire computing facility.

This section of the manual is dedicated to demonstrating how you may modify and extend The Network Director provided information to better suit your installation's requirements. This portion of the manual also presumes that you have read and are familiar with the portions of the *Network User's Guide* that deal with the INFO Facility.

The External File

The INFO information is stored on a Network Director controlled external file. It is the repository for all the data and text necessary to enable the INFO facility to function.

During installation, you should have installed the basic Network Director external file. This file will have multiple INFO topics already defined that are intended to assist network users in utilizing The Network Director. You can logically update any INFO panel distributed by NRS by updating the panel using the INFO Editor. The online DELETE command will specifically prohibit you from deleting a NRS distributed panel. If you would like to eliminate these panels from the External File, you can execute IDCAMS and use REPRO to eliminate NRS records (they are identified by the letter **N** in position 34 of the VSAM key.

Extending the INFO Information

The Network Director's INFO file can be extended by any terminal operator who has access to a INFO APPLICATION definition with UPDATES=YES specified.

Once an authorized UPDATE user has entered the INFO facility, UPDATE mode can be entered by simply entering EDIT on the INFO Primary Command line. This will cause the terminal to take on an appearance similar to the Message Edit panel with the current INFO information. The difference will be in the Title Area, which is adjusted to meet INFO's requirements, and there may appear special text character sequences in the INFO Display Area.

To create a new or existing INFO topic and associated INFO panel number, enter EDIT xxxxx where xxxxx is the panel number of the INFO topic you are about to create or modify. INFO will respond with a Edit panel and you may enter the INFO information. The following figure represents the response to a EDIT 951 command.

Figure 76. The INFO Edit Panel

The INFO Editor

All the standard Message Editor Primary and Prefix commands are supported.

In addition to simple text entry in the Display Area, the INFO Editor provides an additional mechanism to manage the presentation of INFO Prompt Menus and to support the INFO Prompt Command Type. This mechanism, identified as Prompt List Identification, is implemented as a specialized character string embedded in the Display Area along with the traditional Prompt list.

Prompt List Identification

A Prompt List is defined as a series of simple entries in a list form on a panel that will assist the operator in selecting the next location that the INFO facility should transfer to. It is used to establish the values that can be used in the Primary Command Area to indicate selection.

A Prompt List Entry is identified by entering the character string "+(" followed by a number representing the value to be used during INFO Prompt Commands. The Prompt Text immediately follows and is terminated by a ")=" character string.

After the ")=" character string is the panel number that should be displayed if the associated prompt list entry is selected. It is in the form xxxxx, where each x indicates a INFO level number. The panel number must be immediately followed by the termination string ")+".

The following sample should help clarify this facility:

Figure 77. INFO Edit Panel

When this panel is SAVEd, its text will be automatically available to other network users. It is important that you assign uses to the various logical branches of the INFO tree structure. The Network Director maintains the INFO information for all the network users. Typically, INFO file updates are centralized to allow proper synchronization.

The previous panel will appear as follows when it is displayed by a network user.

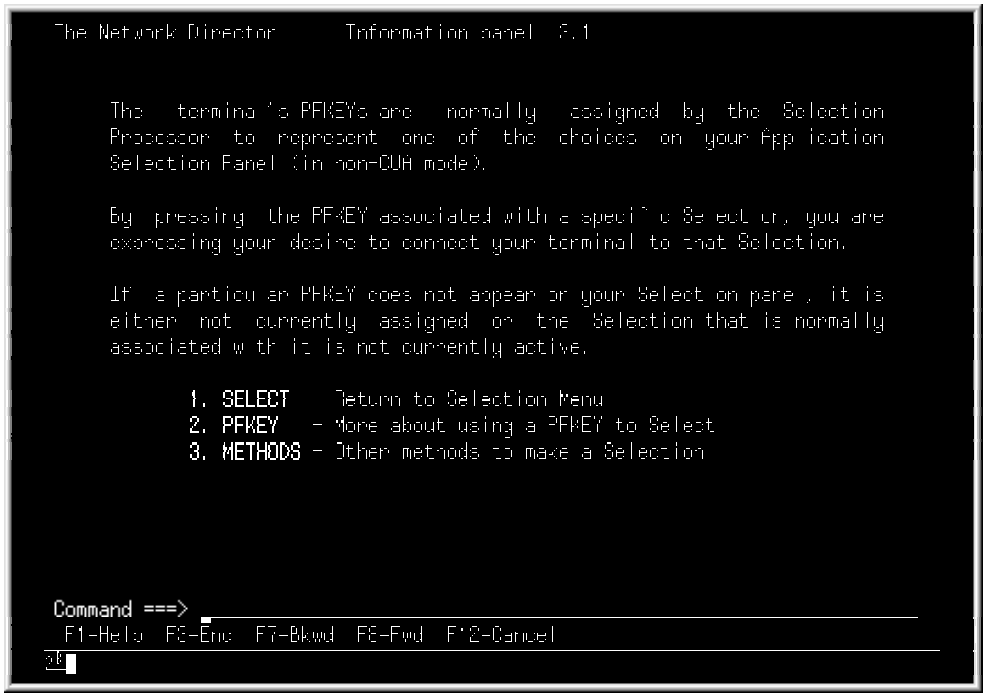


Figure 78. Sample INFO Display

The INFO Index

Each unique panel within the INFO hierarchy may also have a *text string* or keyword associated with it. This information is maintained in a control block and External File record called a INFO or HELP Index (HIX). You may access and update the HIX by entering the command EDIT HIXxxxxx where xxxxx is the HIX level that you would like to update.

You will be presented with a specialized HIX update panel similar to the following:

Figure 79. INFO Index Update Panel

To actually accomplish the update, simply move the 3270 cursor keys to the appropriate definition slot and enter the INFO keyword that you would like associated with the panel at that level. When you are satisfied with the contents of the panel simply strike the ENTER key to commit the changes. If you would like to terminate the Index update without changes, enter the QUIT command (default PF04) or strike the CLEAR key.

Automatic INFO Placement

The INFO facility will also respond to a INFO text command that is placed on the INITIAL-DATA operand of the APPLICATION statement. Normally, no INITIAL-DATA operand is present and INFO automatically displays INFO panel 0 or a INFO panel about the last Network Director message that was received or associated with the device (this is called *contextual HELP*).[31]

When the INITIAL-DATA operand is present, INFO will scan through the indexes and attempt to locate the exact INFO panel to initially display.

```
APPLICATION INFO,TARGET=TNDINFO,
            INITIAL-DATA=('HELP SCHEDULE')
```

will cause INFO to display the INFO topic associated with the text **HELP SCHEDULE**. This mechanism can be utilized to "publish" your system's scheduled availability, etc. or as a general network "bulletin board".

When INITIAL-DATA is specified, the user is automatically routed to the INFO panel with the assigned HIX keywords. When the terminal operator uses the END (F3), Bkwd (F7), or Fwd (F8) commands and the current INFO panel is exhausted (there is no more to display), the user will be automatically returned to the Application Selection Panel because the INITIAL-DATA value was provided.[32]

This tries to simplify the usage of INFO, make it more logical for the end user, and eliminate the difficulties associated with a novice terminal operator receiving INFO about topics that was not specifically requested.

---

[31] Contextual HELP can be eliminated by placing INITIAL-DATA=' ' on the APPLICATION definition for the INFO facility. INFO panel 0 will always be displayed and the messages interpretation will be eliminated.

[32] If INITIAL-DATA is not provided, INFO will position at the next logical INFO panel.

It is also possible to activate the INFO facility from another selection element by use of the Action Characters. Specifying:

```
APPLICATION HELP,TARGET=TNDINFO
APPLICATION TSO,TARGET=TSOA,
        ACTIONS=(H,'HELP TSO')
```

will cause any operator entering the letter **H** in the selection character before the TSO selection to receive the INFO panel associated with the TSO keyword. This technique can be used to provide the terminal network user with additional extended information about a specific selection (availability, new releases, etc.).

Adding Installation Specific Information

The following sample session demonstrates how to add an installation specific panel that contains the *system schedule* and then activate a single keystroke selection to view the panel. A quick checklist on how to accomplish this is:

1. Select an INFO location to establish your bulletin (information)
2. Create the INFO panel containing your information
3. Update the index element to include your panel's "name"
4. Allocate an APPLICATION statement with an appropriate TITLE

Once this process is complete, the terminal operators will be capable of pressing a single PFKEY (or any other selection method) and viewing the information you desire.

Select an INFO Location

As discussed in the *Network User's Guide*, the INFO facility identifies panels by a unique 5 digit identifier. INFO is essentially a inverted tree structure with each significant digit identifying a "branch" on the tree. NRS distributes panels that utilize branches 1xxxx through 4xxxx. Thus, to establish your own information, select one of the other "branches" for your use. Our example will use panels that begin with a 9 (branch 9xxxx).

Create the INFO Panel

To create the INFO panel, enter the INFO facility and type **EDIT 90000** on the primary command line. You will be presented with the editor's panel for topic 90000. Enter the information you would like presented to the users and SAVE it. The following example shows the panel at the moment prior to striking ENTER to SAVE the INFO panel.

Figure 80. Sample Bulletin Board Edit Panel

Once you have SAVEd the panel, the INFO processor will immediately display it back as if you had issued a request to view it.

Update the Index Element

After the panel has been created, associate a *keyword* with the panel by editing the index element associated with the panel's "root" location. Enter **EDIT HIX00000** and strike ENTER. Tab forward to the location for the ninth panel and enter **SCHEDULE**. The following panel demonstrates this immediately prior to saving the index update.

Figure 81. INFO Index Schedule Update Panel

Pressing PF3 will also issue the END command, which causes the index update to be accepted.

Allocate an APPLICATION Statement

At this point the INFO file contains all the information we want the terminal operators to be able to access. All that is left is to grant access to the schedule panel in an easy manner. Define a Network Director APPLICATION similar to the following:

```
APPLICATION SCHEDULE,TARGET=TNDINFO,
            TITLE='System Schedule',
            INITIAL-DATA=('INFO SCHEDULE')
```

We have now defined an APPLICATION named SCHEDULE that can be associated with a USER, GROUP, TERMINAL, or DEFAULT APPLICATIONS operand exactly as any other application would be. The selection processor will allocate a spot on the Application Selection Panel and assign a pfkey to it. When a terminal operator selects the SCHEDULE application, The Network Director will format the INITIAL-DATA operand of 'INFO SCHEDULE' and pass it to the INFO processor. INFO will look at the first "token" of **SCHEDULE** and will look up in the HIX which panel is associated with the keyword **SCHEDULE** Panel 9 will be identified and subsequently displayed.

Viewing the Panel

The terminal operator can look at the SCHEDULE by simply selecting it from a selection panel via any valid selection technique. A sample of the panel that is received follows.

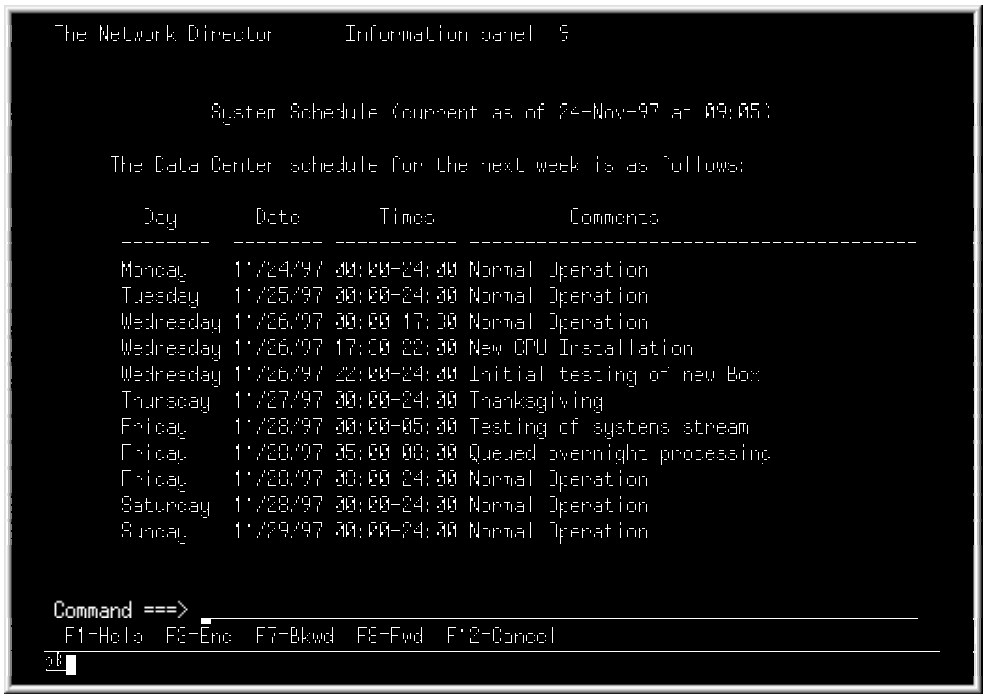


Figure 82. Sample Bulletin Board View Panel

The terminal operator terminates the viewing of the INFO panel through appropriate use of the CLEAR key, or issues the END or QUIT command (default PF3 or PF4).

There are many more uses for the INFO facility to contain your installation specific information. You can define entire structures to contain any information that is appropriate for access by the terminal network.

Monitoring INFO Growth

The INFO information is stored on The Network Director's External File, which is VSAM. It is the Network Administrator's responsibility to utilize standard VSAM provided facilities (Access Method Services) to manage the External File's growth requirements. Additionally, a regular cycle of backing up the External File should be placed into operation. This becomes important if your site has a large amount of activity against the file.

TNDUTIL (see "External File Maintenance (DISPLAY/DELETE)" on page 260) also provides facilities to manage how the External File usage is proceeding.

Deleting INFO Panels

While operating in the INFO facility, an authorized INFO user (UPDATES=YES on the APPLICATION statement) may cause an INFO panel to be deleted by entering DELETE on the INFO command line while viewing the panel to be deleted. Alternatively, enter DELETE xxxxx, where xxxxx is the INFO panel number to be deleted.

NRS distributed INFO panels may not be deleted in this fashion. They may be updated with an installation panel, but not deleted online.

Operational Issues

In general, network operations are discussed in the *Network Operator's Guide*. However, the following information is operational information more appropriate for the Network Administrator.

Color Support

The Network Director contains full support for the 3270 Extended Data Stream facilities to exploit a full 7 colors and the three extended attributes that can be set with the Start Field Extended (SFE) 3270 order.

A specific color and attribute is set into the 3270 data stream by the use of a specific reserved symbol. The reserved symbols and their default meanings are:

Symbol	Hex	Color	Extended Attribute	Intensity	GLOBALS COLORS=
%	X'6C'	White		High	WD%
}	X'D0'	White	Reverse	High	WR}
!	X'5A'	White	Underscore	High	WU!
	X'A1'	default	default	normal	DD
$	X'5B'	Turquoise		normal	TD$
****	X'E0'	Turquoise	Underscore	high	TU\
+	X'4E'	Blue		normal	BD+
{	X'C0'	Blue	Reverse	high	BR{
@	X'7C'	Green		Normal	GD@
¬	X'5F'	Yellow		normal	YD¬
]	X'6A'	Pink		normal	PD]
¢	X'4A'	Red		high	RD¢

Figure 83. Color Characters

You should exercise caution when assigning the color character. If you select a commonly used character (E.G. the letter "A"), then it is entirely possible that the panels presented by The Network Director will suddenly take on unusual color characteristics. For this reason, you should select a symbol that is **not generally** used by The Network Director or on The Network Director's panels.

You may place these special symbols into any data field that will be presented to the device on a Network Director panel (including a selection or identification panel, a message or info display panel, etc.) subject to the rules identified under "Scan Logic" on page 239.

A device is considered a "color device" if it responds with an appropriate Color structured field in the reply to the Read Partition Query issued as a result of WSF=YES or if WSF=COLOR is in effect. Therefore, you must turn on the WSF option to obtain the full color support.[33]

Read Partition Query

If your installation has a "mixture" of devices (some capable of color, some not), the following steps are used by The Network Director to determine whether a device is color capable or not:

1. If WSF=COLOR is specified, assume extended data stream (color) will work
2. If WSF=NO, assume the device is not capable of extended data stream
3. If WSF=YES or WSF=KEEP **and** the EDATS bit is on in the PSERVC of the BIND image (X'80' at offset X'E')
    a. Issue a Write Structured Field Read Partition Query to to determine the characteristics of the device
    b. If a Color Reply structured field is found (X'8186'), assume the device is color capable
    c. If a Color Reply structured field is not found, assume the device is not color capable

NRS recommends that you operate with WSF=YES in effect to enable as much function as possible within your network. Current 3270 control units and emulators generally support the Read Partition Query (even if their answer is minimal).

If you are uncertain about the contents of the reply from the device, specify WSF=KEEP and use the Network Administrator DUMP command to view the reply in storage (anchored on The Network Director's virtual NIB for the device).

---

[33] The Network Director will automatically convert the special symbols from the preceding table to high or normal intensity for non color devices. As a result, you can create LOGOs, etc. for full color devices and The Network Director will make the necessary adjustments during execution to allow them to be portrayed appropriately on a non color device.

Scan Logic

The Network Director scans each output transmission for the presence of one or more of the special symbols. When one of the special symbols is encountered, the character is replaced by a Start Field Extended order, as set by the GLOBALS COLORS= operand.

The location in the output stream where the special character exists will be represented as a blank in the final presentation to the terminal user. Essentially, the special symbol **will** take a position on the panel when presented to the user.

The Network Director will **not** do any replacement of special symbols if the 3270 data field containing the symbol is considered to be an "input" field or the scan has been deactivated via use of the activator character. This is to eliminate any potential translation of the special symbols in the editor or other panel where the symbol has actual use (i.e. the at sign "@" may be a portion of the userid) and may be entered by the terminal operator.

Activator Character

You can include special symbols as a portion of the text by "turning off" the color scan. This is done by using the **Activator** character (a double quote(**"**)). The scan for special symbols will terminate until another activator character is encountered, which turns on the color scan again.

Assume the following sample text string (using the default COLORS settings):

```
%The total$amount is"zero percent (0%) of $38.50"or¢nothing
```

"The total" will be displayed as white characters, "amount is" will be will be displayed as turquoise. The activator character immediately before "zero" turns off the color scan to cause the 0% and $38.50 literals to include the percent and dollar sign. Thus, "amount is zero percent (0%) of $38.50 or" will all be turquoise. The second activator character causes the color scan to begin again, and the "nothing" string will be set to the color red.[34]

The resulting output will physically appear as:

```
The total amount is zero percent (0%) of $38.50 or nothing
```

Special symbols that are replaced will have a blank inserted in the same location that the special symbol is in.

---

[34] You can include the double quote activator character as a portion of the text by placing two consecutive quotes. The scan logic specifically ignores the character immediately following the activator character for purposes of locating another activator character.

Any character immediately following the activator character will be ignored for purposes of translation. This logic enables you to place a double quote into the data stream by specifying two consecutive double quotes (the second one will not qualify as an activator character because the character following an activator is not scanned).

Panel Support

The Network Director internally uses the special symbols to set color into it's panels. As a result, if you change their meanings via the GLOBALS COLORS= operand the changes will apply to internal Network Director usage also.[35]

The following standards have been internally implemented for The Network Director's internally generated panels:

Panel Area	Color
Input Fields	Green
Field Prompts	Turquoise
Panel Titles	Yellow
Informational Items	Blue
Command lines	White

Figure 84. Panel Area Color Usage

Additionally, there are additional panel elements that have default colors associated with them within The Network Director. These areas are:

Panel Element	Color
Selection Status	White (if available) or Blue (if not available)
Selection Title	White (if available) or Blue (if not available)
LOGO	default
Id area field titles	Blue

Figure 85. Panel Element Color Usage

If you insert one or more color characters in the APPLICATION TITLE, the setting will remain in effect for the selection status area.

---

[35] The Network Director internally uses a relative offset mechanism that allows you to actually change the character without impacting The Network Director. However, the color changes you make will effect The Network Director's panels.

Network Director Messages

The Network Director defines the internal messages into 6 message classes and associated specific colors with each of the classes. The message classes and colors are:

Class	Color	General Category
C	Turquoise	Change Message class, contains messages that indicate some type of a status change or unexpected return code
G	Blue	General Message class, normally contains informational only items
I	Red	Internal Message class, are usually messages representing some type of an internal Network Director difficulty
R	Yellow	Reply/response class, are messages associated with a Network Administrator based request
S	White	Security Message class, groups information from a security standpoint
D	Red	Debug Message class, typically permits the evaluation of actions taken during the normal processing of The Network Director (VTAM return codes, INQUIRE operations, etc.).
T	Green	Trace Message class, describes internal messages associated with normal dispatching activities that is usually applicable to the internal operations of The Network Director

Figure 86. Network Director Message Class and Colors

The System Directory

The Network Director contains the logic necessary to manage, interrogate, and utilize information about the network users. This information is collected by The Network Director into the **System Directory**, which is then utilized for the following purposes:

1. resolution of &USER-NAME and &USER-PHONE variables.
2. DIRECTORY interrogation (via SHOW or the new DIRECTORY command).
3. creation of distribution lists via the LIST command in the Message Facility.
4. keeps track of which user has received the NEWS in a single day.
5. records where and when the user last logged on or off The Network Director and what subsystem was used last.

When a network user logs on at a network device, The Network Director connects an individual Directory entry for the user to the device. This entry is connected by looking in the current System Directory for an entry that matches the current user's Userid. If located, the Directory entry is logically related to the current device (the ANE). If not located, a new Directory entry is allocated and filled.

The individual Directory entries are filled from the DIRECTORY statement present in the Configuration Parameters (if present),[36] by obtaining the information from the External File (if present), and finally from the currently operational security system (RACF, ACF2, VMSECURE, TOPSECRET, etc.) and in that order.

If a particular Directory field is present in the individual System Directory entry for a user, it will not be overlaid by the next "source" for the directory information.

The following information is extracted from the security system (set via the GLOBALS SECURITY= operand) and will override the current contents of the System Directory for a specific user unless the DIRECTORY statement was used to create the Directory entry.

ACF2 The Directory entry's name (LIDNAME) and phone (LIDPHONE) are derive from the ACF2 LIDREC associated with the user's ACMCB.

DIRECTOR The Directory entry's name (AIBNAME) and phone (AIBPHONE) are obtained from the applicable Access Information Block (AIB).

RACF The Directory entry's name (ACEEUNAM) is extracted from the ACEE allocated by RACF in The Network Director's address space (MVS only).

TOPSECRET TopSecret/VM installations will have the Directory entry's name (ACCESSORID), group (DIVISION), and department (DEPT) set from the response to the TSS LIST command.

TopSecret/MVS systems will have the name (ACCESSORID), group (DIVISION), and department (DEPT) set via calls to the TopSecret/MVS Application Interface (TSSAI).

---

[36] The Directory information can be specified via usage of the DIRECTORY Statement (see "DIRECTORY" on page 63).

VMSECURE The Directory entry's name (*NM), phone (*PH), and information (*LO) are retrieved from the VMSECURE virtual machine. The *LO or Directory Information can be inserted via direct editing of the VMSECURE Directory entry or can be placed into the entry by utilizing the TNDVMS ADDINFO function.

Interrogating the Directory

The System Directory can be accessed from Network Administration by issuing the SHOW DIRECTORY command or from the Message Facility by entering the primary command SHOW or DIRECTORY (either on the Primary Messages Menu or the Message Editor).

In either case, The Network Director will respond with the contents of the first portion of the System Directory in a format similar to the following figure:[37]

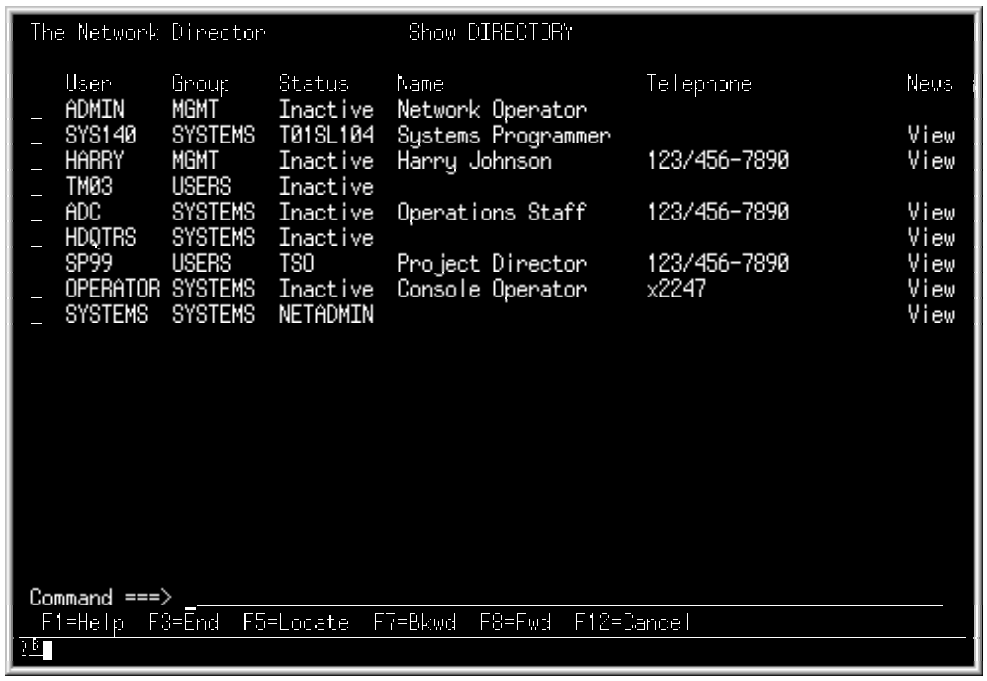


Figure 87. System Directory Menu

The "Status" field of each entry will indicate **Inactive** if the user associated with the entry is not currently logged on, the **Luname** if the Directory's Logon time is greater than the Logoff time, or the **Application** name if the "Appl chosen at" time is greater than the Logoff time.[38]

---

[37] Not all the security systems provide the name and phone number for use within the Directory. If your security system does not provide it, you may provide the information via The Network Director's DIRECTORY definition statement.

[38] If the user logs on multiple times (MAXIMUM= specifies more than 1), the System Directory will reflect the latest logon or logoff activity. You should exercise care about interpreting the System Directory when MAXIMUM is greater than 1 to avoid confusion.

You can manipulate the System Directory via primary or prefix commands, exactly as with other SHOW list panels.

Entering a **S** for "select" will cause the detail panel for the individual Directory entry to be displayed.

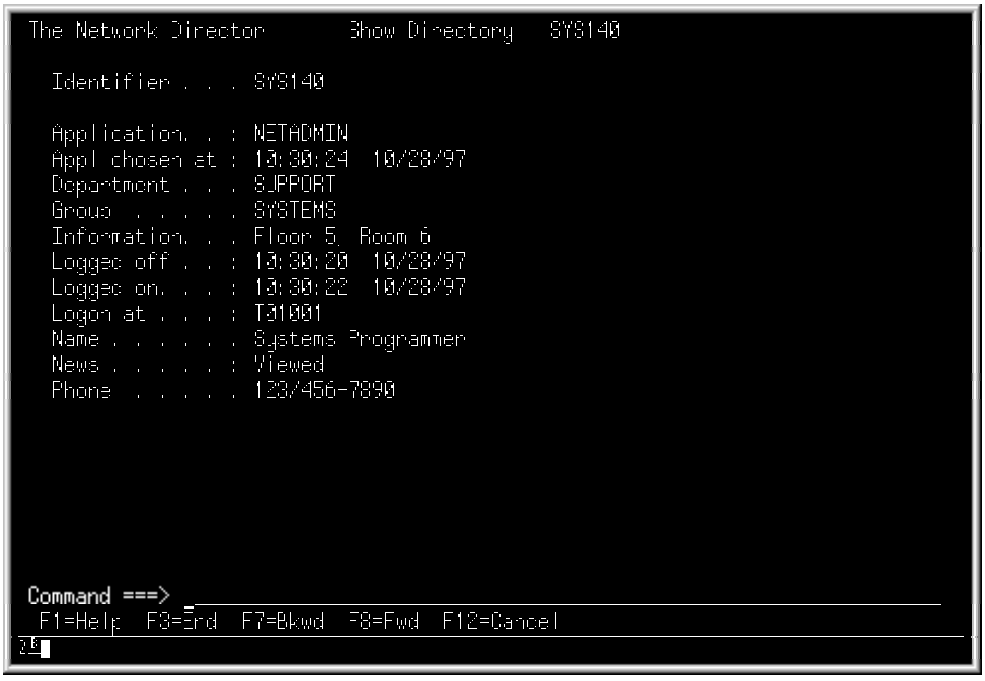


Figure 88. Individual Directory Panel

The "News" field will be blank for a Directory entry whose user has not received the News or **View** if the News has been sent to the user. If your installation is not making usage of the News facility within The Network Director, the Directory News entry will always be blank.

The END (F3) or CANCEL (F12) action will return your device to the prior panel.

DISPLAY NETWORK-ELEMENT

The System Directory allows The Network Director to keep track of the users of the network that are logged off of the system, in addition to those that are logged on. Consider the following response by The Network Director when a user that was logged onto The Network Director at one point is no longer logged on:

```
DISPLAY NET=USERID

TND0795G Id USERID - Test Name was logged off at 10:34:43 on 05/08/95
TND0796G   Last logon was at T02004 at 10:22:12 on 05/08/95
TND0797G   last used ADMIN at 10:33:52 on 05/08/95
```

The Network Director can report on what a network user was doing the last time that the user was identifiable to The Network Director.

NEWS

The Network Director also supports an additional facility identified as the **NEWS**, which represents a special "message" to the network users. This message (which must be named "NEWS") will be delivered to each network user prior to the first Application Selection Panel (menu) presented to the user in an individual calendar day after the user has successfully logged on.

This "delivery" of the NEWS will result in the terminal user being presented with a Message Facility VIEW panel of the NEWS message immediately prior to a normal selection panel (this typically occurs right after the user has logged on or returned from a subsystem). Terminating the Message Editor via END (F3), QUIT (F4) or CANCEL (F12) will terminate the NEWS and allow the terminal operator to continue with the normal selection process.

Creating the NEWS

You create the NEWS from any authorized Message Facility user by accessing the Primary Messages menu and invoking the Editor for a message identified as "NEWS" (UPPER case required). You can set the destination to a subset of the network (if desired), You can identify the "subset" of the network by utilizing The Network Director's Wild character, specify a defined Network Director GROUP, or a defined APPLICATION. The following example is preparing NEWS for every user of The Network Director:

Figure 89. Initiating the NEWS

You will then be presented with a standard Message Editor input panel that you can complete to inform the network users of whatever your desired NEWS information is.

The following example shows a typical "bulletin" type NEWS edit panel.[39]

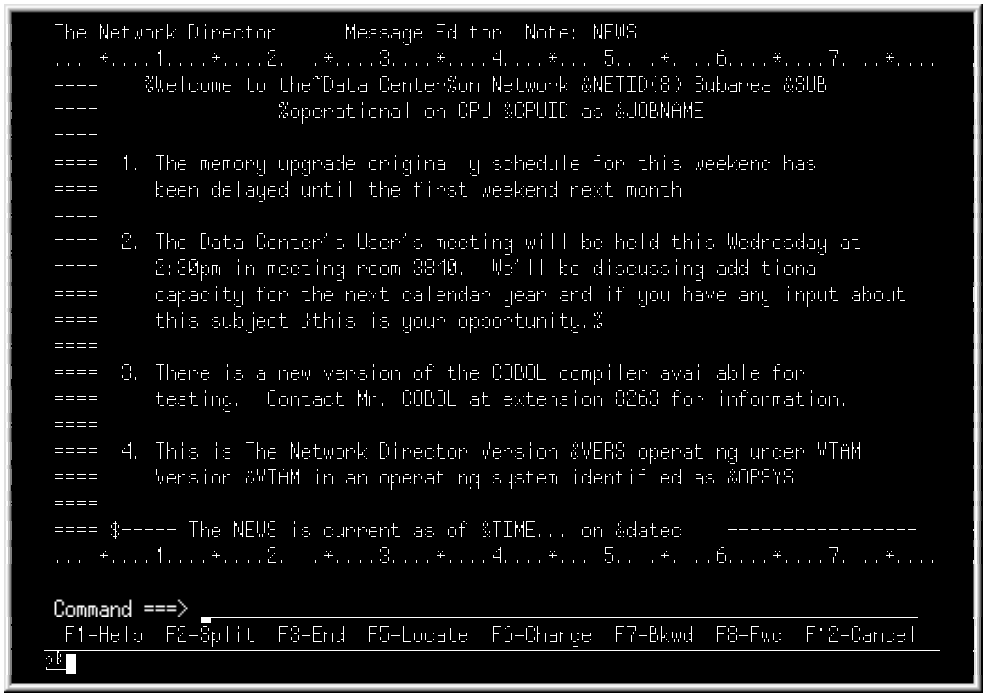


Figure 90. Creating the NEWS Contents

To SAVE the NEWS, simply execute the END (F3) command.

---

[39] Notice the usage of the color characters to enhance the content of the NEWS panel. Remember that symbolic variables are replaced by their appropriate values when the message is Sent. This means the NEWS panel will reflect the values in effect at the time you send it and **not when the destination reads the NEWS**.

To place the NEWS "online", simply send the NEWS by entering a S (Send) action in front of the NEWS message line on the messages menu, as follows:

Figure 91. Sending the NEWS

After the NEWS has been Sent, any user that logs onto The Network Director that has not already received the NEWS for the current calendar day (and that is eligible for the NEWS as if the user was a Message Facility user) will receive the NEWS panel prior to the Application Selection Panel.[40] If the user has multiple NEWS messages, the most recent one will be delivered. The other NEWS message panels will be accessible via the Message Facility Primary Messages Menu.

The fact that a specific individual has already received the NEWS on a given calendar day is kept in the System Directory. This means that an individual user will receive the NEWS only **once**, regardless of how many times or terminals the individual logs onto.

Refreshing the NEWS

During the course of a processing day, you may decide that you need to update the NEWS **and** you would like individuals that have already seen the NEWS for the current calendar day to see it again. Simply access Network Administration and issue the "RELEASE NEWS" command. This causes The Network Director to reset the NEWS characteristic in the entire System Directory to a "not viewed" status, which will force the user through the NEWS panel again (the next time they logon).

---

[40] The user sending the NEWS will have it allocated in his message queue and will, as a result, always receive the NEWS also.

Application Selection Panel Default Actions

The Network Director supports the use of individual Action characters on the non-CUA Application Selection Panel via the ACTIONS= operand. There are a few standard actions that are supported to assist the menu users in their use of the network.

The default actions supported by The Network Director assume that there is not a corresponding action already defined via the ACTIONS= operand. If there is, the ACTIONS= definition will take precedence. If there is not a predefined ACTION, then the following characters will be supported:

H The "Help" action indicates to The Network Director that it should format a HELP command with the COMMENTS= operand as an operand. This will cause The Network Director's INFO processor to receive control and display the information associated with the identified panel. The terminal user simply presses the F3=End key to return to the Application Selection Panel

CUA users can also move the cursor to the desired selection and press the F1=Help key.

I The "Information" action requests that The Network Director format a single line message containing the Owner and Telephone number of the individual or department that is responsible for the selection. The message is delivered to the terminal operator in the standard Network Director Broadcast or Message area.

? Same as the I or Information action

Note: Because The Network Director will honor any user installation defined ACTIONS, these action characters may be used for other purposes at your installation, if desired. If you would like to reassign these actions to other characters, simply define the desired characters via the ACTIONS= operand to the appropriate OWNER and HELP commands.

FLASH

The Network Director contains a command identified as **FLASH** that allows you to test the throughput characteristics of the connection between The Network Director and one or more actual devices. Flash causes The Network Director to write the DEFAULT LOGO and DEFAULT ID-LOGO in alternating fashion to the output terminal a specified number of times or for a specific duration. Upon completion, the FLASH command indicates how many output transmissions were done, how many bytes were logically sent, and how long an average output cycle took (elapsed time). This information can provide a base line to compare the relative performance of different terminal connection mechanisms.

The command can be executed from two different locations within The Network Director.

1. As a Network Administrator command
2. As a terminal operator command

FLASH can be utilized to create a significant amount of output transmissions on multiple VTAM sessions. Thus, performance characteristics of various portions of a terminal network can be evaluated. However, the evaluation of the results are the responsibility of the observer (The Network Director has no "benchmark" logic that determines if a given configuration is running well).

Measurement of performance requires a methodical plan identifying what you would like to measure and how you will go about it. Remember, the conclusions drawn from analysis will only be accurate if the methodology is sound.

Network Administration Command

When issued as a Network Administrator's command,[41] FLASH has the following syntax:

FLASH [{1|number|duration} {delay|1} {chase|8} {lu-pattern|++++++++}]

Figure 92. Network Administrator FLASH Command

where:

chase is number of output transmissions that should be sent between SNA CHASE commands, which will clear the session of activity prior to additional output transmissions.

delay is number of seconds between output transmissions that the FLASH should wait before it schedules the next output

duration indicates the length of time (from current time) that output should continue to be transmitted. The Network Director detects that you are requesting a "duration" by locating one of the non-numeric multipliers in the operand (M = minutes, S = seconds, H = hours, D = days).

---

[41] The Administrator command can be issued from the Network Administration LOG display, via the GCS WTOR, or CP SMSG from an authorized virtual machine.

lu-pattern is the pattern of lunames that should have their existing LOGO rewritten to the screen. Standard Network Director pattern matching is acceptable.

number indicates the total number of times that output should be scheduled to the device entering the command

The FLASH command is a request to initiate the repetitive FLASH operation on all devices specified by the FLASH pattern. The Network Director will attach the FLASH function to any device that is active, does not already have another function (DFB) connected to it, and it is currently in session with The Network Director.

Logic

The FLASH Administrator command causes a single Network Director DFB to be attached within The Network Director's dispatching environment for each device that is currently in session with The Network Director and that matches the provided "lu pattern". Each device will begin to operate (flash) as if it had entered the terminal initiated command from the individual device.

Example

The following extracted Network Director TNDLOG messages provide an example of the Administrator FLASH command's operation:

```
OPERATOR  0249R Input: flash T01+++ 5
FLASH     0823G Flash initiated on 3 sessions
T01005    0827G Flash complete, 361 output(s) 39,826 bytes, average 1.2 seconds
```

This example shows The Network Director serially updating 3 devices that it is in session with.

The actual time of transmissions associated with the TND0823 and TND0827 messages can be displayed via appropriate usage of the Network Administration PREFIX TIMES command. Alternatively, the messages are always time stamped in the TNDLOG virtual printer.

Terminal Operator Command

When issued as a terminal operator command from the Command: line, FLASH has the following syntax:

FLASH [{1|number|duration} {delay|1} {chase|8}

Figure 93. Terminal Operator FLASH Command

where:

chase is number of output transmissions that should be sent between SNA CHASE commands, which will clear the session of activity prior to additional output transmissions.

delay is number of seconds between output transmissions that the FLASH should wait before it schedules the next output

duration indicates the length of time (from current time) that output should continue to be transmitted. The Network Director detects that you are requesting a "duration" by locating one of the non-numeric multipliers in the operand (M = minutes, S = seconds, H = hours, D = days).

number indicates the total number of times that output should be scheduled to the device entering the command

Logic

Each FLASH command initiates a single dispatchable element (DFB) for the device it is initiated from. This DFB will alternate between sending the full LOGO and ID-LOGO to the device for the number of times or length of time specified (with the specified delay between output transmissions).[42]

The terminal FLASH command does not relinquish control to the device (SNA Change Direction) after every output to the device. It will do so after the last output is scheduled or periodically during the FLASH process (default is every 8 output transmissions). The SNA direction is kept by The Network Director to optimize the output volume that can be sent to the device. However, the periodic direction change is done to minimize the impact upon ACF/VTAM resources (a SNA CHASE command is sent to insure that all output on a given session is complete before sending more).

FLASH can be interrupted by pressing an AID key and causing The Network Director to react to it (FLASH detects this has been done and issues TND0826 before terminating).[43]

---

[42] Normal Network Director SBA translation is bypassed during FLASH processing. Devices with other than 80 character widths (such as Model 5 devices) will see the LOGO "run together" across the screen (it will not be formatted normally). This may not look appealing, but will still accomplish FLASH's objectives.

[43] SNA devices should use the ATTN key to get the direction in the middle of an active FLASH process.

Example

The following extracted Network Director TNDLOG messages provide an example of the Terminal Operator FLASH command's operation:

```
T01005    0249R Input: flash 5m 0
T01005    0827G Flash complete, 361 output(s) 39,826 bytes, average 1.2 seconds
```

This example shows the terminal operator requesting that FLASH continue alternating between ID-LOGO and LOGO for approximately 5 minutes elapsed with no delay between scheduled outputs. The SNA CHASE command will be issued every 8 outputs (8 is the default, but can be overridden by the third positional parameter on the FLASH command).

The TND0827 message shows the total number of output transmissions initiated by this FLASH command, the total number of **logical bytes** that were sent, and the average time between FLASH transmissions.

Message Facilities

The Network Director's Message Facility is generally described in the *Network User's Guide*. This section of the manual reviews a few more topics that apply to the overall environment.

Broadcast Authorization

The MESSAGES= operand of the USER, TERMINAL, GROUP, or DEFAULT statement controls which messages a particular operator is authorized to issue. The Network Director typically allows all the network users to operate as they choose on Memos and Notes. Broadcast messages are normally restricted to the Network Administrator and perhaps the operator's console.

The Broadcast message is typically restricted as it will take immediate effect throughout the network. It will cause immediate rewriting of the terminal panels and can be considered an disruptive type message. Thus, it is important that the Broadcast type message is not used indiscriminately.

Characteristics

Each Message type's characteristics are controlled within the network via its own operand on the GLOBALS statement (MEMOS=, NOTES=, and BROADCASTS=). These operands control how The Network Director will manage messages in each of these categories.

Disk queuing is mandatory for any messages that are required to survive Network Director restarts. However, disk access will be slower and necessitate more management of the External File. Storage queuing will be much quicker and less

demanding upon I/O devices and channels, but all storage queued Message will be lost when The Network Director is not executing.

The expiration time interval is intended to be utilized to simplify and minimize manual intervention within the External File. When a Message has reached its expiration date, The Network Director will automatically purge the Message from the External File or storage queue that it is on. Of course, if the expiration period is too short, The Network Director may purge a Message before it has been processed by the Destination. It is important that your installation set the expiration interval to a value that is acceptable at your site and that the network users have been informed.

Monitoring

As mentioned "Message Facilities" on page 253, The Message Facility and its External File can be managed through the use of the DISPLAY statement. The DISPLAY MESSAGES, NOTES, and MEMOS commands will produce information of use when monitoring the Message Facilities External File usage.

The External File

The Message Facility makes use of The Network Director's standard External File. It shares the file with the INFO information and several other disk oriented mechanisms (see the Internals Manual for more information). It is the Network Administrator's responsibility to manage the disk space allocation and disk file backups using standard operating system provided services (Access Method Services).

The Network Director will not be capable of any Disk Message Queuing if the External File is not available. In this event, The Network Director will continue to process all messages normally, but will caution each user editing a Message that it may not be saved.

Cross Domain/Cross Network Considerations

When operating The Network Director in a multiple domain or multiple network VTAM environment, The Network Director can be configured in a variety of manners to manage all or a portion of a distributed network. There are operational advantages and disadvantages to operating a single Network Director for an entire network as well as operational advantages and disadvantages to operating a Network Director in each domain.

The use of The Network Director in a multiple domain or multiple network network needs to be carefully combined with other requirements associated with the processing requirements of the network. While The Network Director does not require that you operate in any particular manner, The Network Director does offer services that can be utilized to assist when dealing with a multiple domain situation. The following topics should be reviewed for applicability in cross domain environments.

Single System Image

In an environment with multiple Network Director's, it is typical for a primary or "home" Network Director to have selections representing the secondary Network Directors as APPLICATION choices. Specifying SSI=YES on the APPLICATION definition for the secondary Network Director, will cause the primary Network Director to forward the appropriate information to enable an automated signon attempt at the secondary location.

Naturally, this presumes that the userid and password combinations at the two locations match. If they do not match, the secondary location will reject the signon effort with an appropriate message. If they do match, the terminal operator will be presented with a Application Selection Panel from the secondary Network Director.

It is also possible to forward an INITIAL-DATA string to The Network Director that represents a Command: line input string. If present, the receiving Network Director will attempt to process the incoming string exactly as if it had been typed on the Command: line. This facility can be used to control the activity at the secondary host.

SITE Definitions

The Network Director will also monitor the availability of other domains in the network via the specification of a SITE statement for each of the other nodes operating a Network Director. If you provide these statements, the message editor will also allow messages to be transferred between nodes via LU to LU sessions between The Network Directors. These SITE definitions are also utilized to track individual terminal activity within the network (see the following discussion for more about this topic).

NETID and SUBAREA

The SUBAREA (for cross domain) and NETID (for cross network) operands allow you to isolate various TERMINALS and USERS based upon the specific location the device involved originated from. This can be utilized to present customized selection menus for specific subsets of the entire logical network.

The NETID and SUBAREA values are also displayed in many of the informational messages produced by The Network Director, as well as included in many of the Network Administrator DISPLAY commands.

RETURN Command

The Command: line command RETURN provides a manner for a terminal operator to express a desire to "return" to The Network Director that was previously in control of the device. Utilization of RETURN and TERMINAL ACQUIRE=SELECT enables a terminal operator in a multiple domain network to make use of the network in a more understandable fashion, but without sacrificing security. Operationally, a terminal user can go to another domain, process multiple application choices there, and "return" to the previous domain when desired (by issuing the RETURN command).

Background

As an example, a device owned by Domain 1 can select The Network Director in Domain 2 and subsequently select an APPLICATION in Domain 2 (CICS as an example). Normally, when the device logs off of CICS in Domain 2, the device is returned to Domain 1's Network Director (because of the LOGAPPL specification). This leaves the device logically logged on in Domain 2's Network Director. The use of SSI=YES between Network Director's addresses this (if a different operator logs on at the device in Domain 1 and then selects Domain 2, The Network Director in Domain 2 detects this and logs the first user off).

However, the terminal operator may wish to return to The Network Director in Domain 2 when finished with the chosen application. If this is the case, a TERMINAL ACQUIRE=SELECT specification in Domain 2's Network Director allows this (APPLICATION ATTRIBUTE=(NOACQUIRE) should be specified for other Network Director APPLICATION definitions).

In this case, if a terminal user with a device in Domain 2 logs off and another user (USER2) logs on in Domain 2 and issues **DROP**, then The Network Director in Domain 1 will restore USER1's Application Selection Panel (presuming Domain 1 is the LOGAPPL domain). While DROP is a restricted command, a potential security exposure exists. This is a result of The Network Director in Domain 1 receiving no confirmation from The Network Director in Domain 2 that USER1 is still at the device.

The RETURN command is intended to address this situation.

Specification

The network definitions do **not** have to be updated to authorize access to RETURN (it is an unauthorized Command: line command). However, each Network Director in the logical network will require a SITE and a APPLICATION definition for the other Network Director's that make up the logical network. For the previous example, the following definitions would apply to Domain 1:

```
APPLICATION DOMAIN2,TARGET=TND2,
            SSI=EXTENDED,ATTRIBUTES=NO-ACQUIRE,
            TITLE='Alternate Data Center'
SITE  DOMAIN2,TARGET=TND2
TERMINALS ++++++++,ACQUIRE=SELECT,
                  APPLICATIONS=DOMAIN2
```

Domain 2's definitions would be:

```
APPLICATION DOMAIN1,TARGET=TND1,
            SSI=EXTENDED,ATTRIBUTES=NO-ACQUIRE,
            TITLE='Primary Data Center'
SITE  DOMAIN1,TARGET=TND1
APPLICATION TESTCICS,TARGET=CICS,
                      TITLE='Test New Transids'
TERMINALS ++++++++,ACQUIRE=SELECT,
                  APPLICATIONS=(DOMAIN1,TESTCICS)
```

The device at Domain 1 selects DOMAIN2. The Network Director in Domain 1 would normally queue an acquire (TERMINALS ACQUIRE=SELECT), but does not in this case (APPLICATION ATTRIBUTE=NOACQUIRE). The Network Director also detects the user has just selected another SITE (by scanning the SITE definitions) and forwards the device to DOMAIN2 with the userid, password, and site filled in (SSI=EXTENDED).

The device user is automatically signed on and presented with an Application Selection Panel. The user selects TESTCICS and The Network Director in Domain 2 queues an ACQUIRE (ACQUIRE=SELECT). When the user logs off of CICS, the queued ACQUIRE will cause the device to return to The Network Director in Domain 2 (allowing the terminal operator to "stay" in Domain 2). Issuing RETURN (entering it on the Command: line, pressing a Profile PFKEY, TNDCMD, etc.) will cause the device to be logged off in Domain 2 and CLSDST PASSed back to The Network Director in Domain 1 with the userid, password, and site name filled in. The Network Director in Domain 1 (who knew the user went to another Network Director) checks to insure that the returning device has the same userid as when it left. If it does not, the device is logged off and then prompted with the default panel for The Network Director in Domain 1.

If a user selects another Network Director that is recognized as a SITE, the device **must** return with a properly formatted SSX (SSI eXtended control block) or it will be logged off. DROP, DISC, and VTAM VARY commands do not create the potential for a user to receive a previous user's Application Selection Panel because these actions will cause the device to be returned to The Network Director in Domain 1 with no SSX, which

will cause an automatic LOGOFF operation and thereby eliminate any exposure that may exist.

LU 6.2 (APPC) Support

The Network Director supports an Application Program to Program Communication (APPC) interface to other programs. This interface supports the basic Network System Interface (NSI) functions, as documented in the *Network User's Guide*.[44]

You can activate this support within The Network Director's nucleus by completing the following tasks:

Step	Activity	Done
1	Define a LU6.2 MODETAB entry identified as TNDNSI62 to an appropriate VTAM Mode Table (NRS recommends creating a new Logmode Table identified as TNDINCLM)	
2	Add APPC=YES and MODETAB=modetab-name to the applicable Network Director and NSI VTAMLST APPL definitions	
3	Link the NSI calling application with TNDNSI62 from the distribution tape	
4	Restart VTAM with the new Modetable and revised APPL definitions or use the appropriate VTAM VARY command to activate the revised definitions.	
5	Restart The Network Director	
6	Verify the operations of the LU 6.2 NSI connection by using the defined NSI application and watch for appropriate results in The Network Director	

A discussion of a few of the key steps associated with this process follow:

[44] ACF/VTAM 3.2 or a later release is required.

The LU 6.2 Logmode

LU 6.2 requires a specific LOGMODE name to facilitate "conversations" between partners (in this case, the NSI calling program and The Network Director). You should allocate a LOGMODE entry named TNDNSI62 and activate it within VTAM by placing it into an existing LOGMODE table or creating a new one.

An example of the Logmode table entry within a unique Logmode table is:

```
TNDINCLM TITLE 'NRS Logmode Table (LU 6.2 enabled)'
*
TNDINCLM MODETAB
*************************************************************************
*                                                                       *
*       The Network Director's Network System Interface LOGMODE         *
*                                                                       *
*************************************************************************
TNDNSI62 MODEENT LOGMODE=TNDNSI62,FMPROF=X'13',TSPROF=X'07',            *
               PRIPROT=X'B0',SECPROT=X'B0',COMPROT=X'D0B1',             *
               RUSIZES=X'8585',ENCR=B'0000',                            *
               PSERVIC=X'060200000000000000000300'
         MODEEND ,
         END                          , END OF TNDINCLM
```

The APPL Definition

Each ACF/VTAM processing system that needs to utilize LU 6.2 services must be enabled for this via an entry in the appropriate VTAMLST member, file, or book. The APPC=YES operand is required. You must also indicate the LOGMODE table name (if not the default).

An example of the required APPL definitions is:

```
A01TND   APPL  AUTH=(NVPACE,PASS,ACQ,SPO),ACBNAME=DIRECTOR,            X
               APPC=YES,MODETAB=TNDINCLM
A01NSI   APPL  AUTH=(NVPACE),ACBNAME=TNDNSI,                           X
               APPC=YES,MODETAB=TNDINCLM
```

These definitions indicate to ACF/VTAM that the application programs using these particular ACBs are enabled to use the services of LU 6.2 to start and stop conversations.

Dynamic Network Changes

As previously referenced, you may make modification and additions to existing network definitions from any authorized Network Administrator's display. To accomplish this, you simply enter the SHOW command with the appropriate operands to identify the element or elements you would like to change. The procedures and mechanisms for all dynamic network changes are documented further in the *Network Operator's Guide* (TND-0210).

Network definitions that have been modified while The Network Director is operating can be saved and reloaded (used for a later execution) by appropriate use of the SAVE and RELOAD commands. These commands are also documented in the *Network Operator's Guide*.

External File Maintenance (DISPLAY/DELETE)

The External File (VSAM) can be processed offline by a batch utility program named TNDUTIL. TNDUTIL operates as a batch program in a separate address space, partition, or virtual machine and accepts simple keyword requests and accesses the External File to process the request. Sample Job control or EXECs are distributed on the distribution tape as TNDUTILJ.

TNDUTIL reads the input file (TNDPARMS or SYSIPT) and processes the request against the External File (TNDFILE) and produces the output onto an output printer (TNDLOG or SYSLST). Input parameters supported are:

```
DISPLAY     ACCESS        [ =userid ]
            DIRECTORY     [ = userid ]
            DMTS
            HIX           [ =hixlevel ]
            INFO          [ =panel number ]
            LISTS         [ = userid ]
            MESSAGES      [ =[(]userid[,message)] ]
            MIX           [ =userid ]
            PROFILES      [ =network name ]
            SAVED         [ =(setname,version) ]
            SUMMARY

DELETE      ACCESS=userid
            DIRECTORY     [ = userid ]
            DMTS          =message numbers
            HIX           =hixlevel
            INFO          =panel number
            LISTS         [ = userid ]
            MESSAGES      =[(]userid[,message)]
            MIX           [ =userid ]
            PROFILES      =network name
            SAVED         =(setname,version)
```

Figure 94. TNDUTIL Request Syntax

Upper case information needs to be coded as portrayed and the lower case items provided. The keywords follow standard Network Director syntax (you must only specify enough to uniquely identify the keyword). Wild characters are valid wherever operand values are provided. E.G., DISPLAY MESSAGES=TS++++++ will display all messages for every network element that begins with the letters **TS**.

TNDUTIL can be used to display items from the External File while The Network Director is operating. However, the DELETE function will cause TNDUTIL to open the External File for update, which cannot be done at the same time as the file is open to The Network Director. You can use The Network Director's CLOSE and OPEN command from Network Administration to make the file available to TNDUTIL for update activities.

ACCESS

An Access Information Block represents the information associated with an individual user gaining access to the system. It is utilized for AUTHENTICATION checking and SECURITY=DIRECTOR logic.

DIRECTORY

The System Directory causes an individual record to be stored in the External File identified as a "Directory" entry. You can manipulate these items via usage of the DELETE and DISPLAY command.

The following DISPLAY commands are all valid:

```
DISPLAY DIRECTORY
DISPLAY DIRECTORY=USER
```

The first DISPLAY command provides a single line for each Directory Entry stored in the External File. The second DISPLAY command (wild characters are valid) requests that each Directory Entry should be expanded into a detail display with each Directory Entry displayed on a unique printer page.

Both display options produce an expansion of the full Directory Entry, but in different formats.

DMT

A Director Message Text represents a modified, standard message that has been placed into the External File as a result of a message EDIT command from an authorized Network Administrator's terminal. The DMT will contain the modified text, overrides the distributed message text, and is loaded at initialization time by The Network Director.

HIX

This HIX represents a single level of the INFO index, as described on "The INFO Index" on page 229. It contains the keywords related to the 10 panels at a particular level within the INFO facility structure.

INFO

An INFO record contains the actual text associated with a single INFO facility panel. The data is stored as compressed strings of text, is loaded into storage as required by terminal operator reference, and is displayed by the INFO processor.

LISTS

The LIST command enables the Network Administrator and Message Facility users to create Network Distribution Lists, which can be utilized as message destinations for the routing of messages.

The following DISPLAY commands are now available to support the External File's storage of the Distribution Lists:

```
DISPLAY LISTS
DISPLAY LISTS=USER
```

The first DISPLAY command provides a single line for each Distribution List stored in the External File (one line to a list). The second DISPLAY command (wild characters are valid) requests that each Distribution List should be expanded into a detail display with each List displayed on a unique printer page.

MESSAGES

A message record contains the actual text associated with a single message facility message. The message is stored as compressed strings of text, is loaded into storage as required by terminal operator reference, and is displayed by the message editor. Specifying a userid causes TNDUTIL to expand all message records for a specific user (wild characters are valid) and print or delete each message on a single page of output.

You may also specify the specific message name or name pattern that should be displayed or deleted by enclosing the operand in parenthesis (E.G. DISPLAY MESSAGES=(TESTUSER,M+++++++) requests all messages for the user TESTUSER that start with a M).

MIX

A Message IndeX record contains the messages that a particular network element is involved. with. The MIX is no longer utilized in Version 3 and up of The Network Director and may be deleted to expand the usable space on the External File.

PROFILES

Each PROFILE record contains the profile data elements associated with a network element. It is loaded by The Network Director when a network element becomes active or whenever a terminal operator issues the PROFILE command.

SAVED

All definitions saved via the SAVE command are stored into the External File. This operand allows a batch execution of TNDUTIL to display an overview or itemized display of the various sets of SAVEd definitions. Specifying SAVED as a positional operand produces a single line for each saved set of definitions. Specifying it as a keyword causes the individual saved definitions that match the criteria to be displayed. E.G., DISPLAY SAVED=(TEST,4) will display a single line for each definition that is a portion of the set of definitions with the name TEST stored with a VERSION of 4.

SUMMARY

This operand requests a summary display of the contents of the entire External File. This will produce a single line for each type of record present on the file, how many there are, the total size in bytes, average size, and the number of the record type that are supplied by NRS. An example of DISPLAY SUMMARY follows.

```
--12/05/1997--------------------T h e   N e t w o r k   D i r e c t o r   (4.2.2) - File Summary-----------------Page  1--

Input (18:56:39): DISPLAY SUMMARY


                      Type       Record Count   Total Bytes     Average     NRS
                  -------------  ------------   -----------   ---------   -------
                  Info Text             1,004       324,444         323     1,004
                  Info Index               45         4,770         106        45
                  Profiles                  3         1,003         334
                  Access Blocks             9         3,179         353
                  Saved Items             118        32,886         278
```

Figure 95. Sample TNDUTIL Output

VSAM File Description

The External File is a VSAM Key Sequenced file with the following key definition:

Field	Length	Offset	Value	Usage
EFRTYPE	1	0		Indicates the type of External File record
EFRCB			X'01'	Saved control block
EFRHDE			X'02'	HELP/INFO Data Record
EFRHIX			X'04'	HELP/INFO Index Record
EFRPDE			X'08'	Profile Data Element
EFRDMT			X'10'	Stored Director Message Text
EFRMIX			X'20'	Message Index (unused in Version 3 and up systems)
EFRDIR			X'21'	System Directory record
EFRNDL			X'22'	Network Directory List
EFRMDE			X'40'	Message Facility Message
EFRAIB			X'80'	Authentication Record
	3		1	Unused bytes
EFRDATE	4	4		STCK value for when the message will expire
EFRMTYPE	1	8		Type of Message (values defined in the TNDMDE DSECT)
EFRNAME	8		9	Message Name
EFRUSER	8		17	Message Owner
EFROTHER	8		25	Message Destination
EFRSCRNO	5		4	INFO Panel Number (for HELP/INFO records)
EFRCSRID	8		4	SAVE/RELOAD Set Name
EFRCVERS	1		12	SAVE/RELOAD Version Number
EFRCTYPE	1		13	SAVE/RELOAD Control Block Type Record
EFRCORDR	2		14	SAVE/RELOAD Sequence Field
EFRCNAME	8		16	SAVE/RELOAD Control Block Name
EFRCEXTN	8		24	SAVE/RELOAD Control Block Extension

Field	Length	Offset	Value	Usage
EFRMSGNO	2		4	Director Message Text Message Number
EFRNEL	8		4	Authentication Network Element Name
EFROWNER	1		34	An Internal Sequence Number/Owner Id
EFRNRS		C'N'	34	NRS Distributed Record
EFRSITE		C' '	34	Installation Added Record

Figure 96. External File Key Description

Additional information can be obtained by locating the TNDEFR DSECT available on The Network Director's distribution library for use within Assembler programs. This DSECT also includes basic information about how the data record portion of the External File record is constructed.

Internal Debugging Facilities

The Network Director provides several DISPLAY options that are intended to provide a view of the activity occurring within the network. DISPLAY DFBS shows the currently active items (dispatchable functions). Other options provide information that can be easily interpreted based on the message text itself.

For interested Network Administrators, The Network Director also provides a facility to *dump main storage*. This mechanism is intended to allow the knowledgeable Network Administrator to interactively view the contents of the various Network Director control blocks and the various chains.

The DUMP command is entered on the Primary Command line. Its format is:

```
DUMP

   [ address ]
   [ TNDcsect ]
   [ ADB [ =applications name ] ]
   [ ANE [ =network element name ] ]
   [ DFB [ =DFB name ] ]
   [ DIR [ =userid ] ]
   [ DMT [ =message number ] ]
   [ EFR ]
   [ GDB [ =group name ] ]
   [ HDE [ =INFO topic number ] ]
   [ HIX [ =INFO index key ] ]
   [ MDE ]
   [ MIX [ =message index owner ] ]
   [ NDL ]
   [ NIB [ =LU name ] ]
   [ PDA ]
   [ PDE [ =profile name ] ]
   [ PPE ]
   [ RPL ]
   [ SDB ]
   [ SMR ]
   [ TDB [ =terminal name ] ]
   [ UDB [ =user id ] ]
```

Figure 97. DUMP Command Syntax

address is a 1 to 8 byte hexadecimal address in main storage you would like displayed.

TNDcsect is a 4 to 8 character constant beginning with **TND** that requests The Network Director to begin the DUMP display with the virtual storage location that the designated CSECT (csect) is at

xxx =value all the other DUMP operands specify the control block name that should be dumped (represented as xxx in this entry). Some of the control block chains will allow you to specify an operand that will dictate which control block on the specified chain that should be dumped. If you do not specify a value (=value) then DUMP will dump the first control block on the chain.

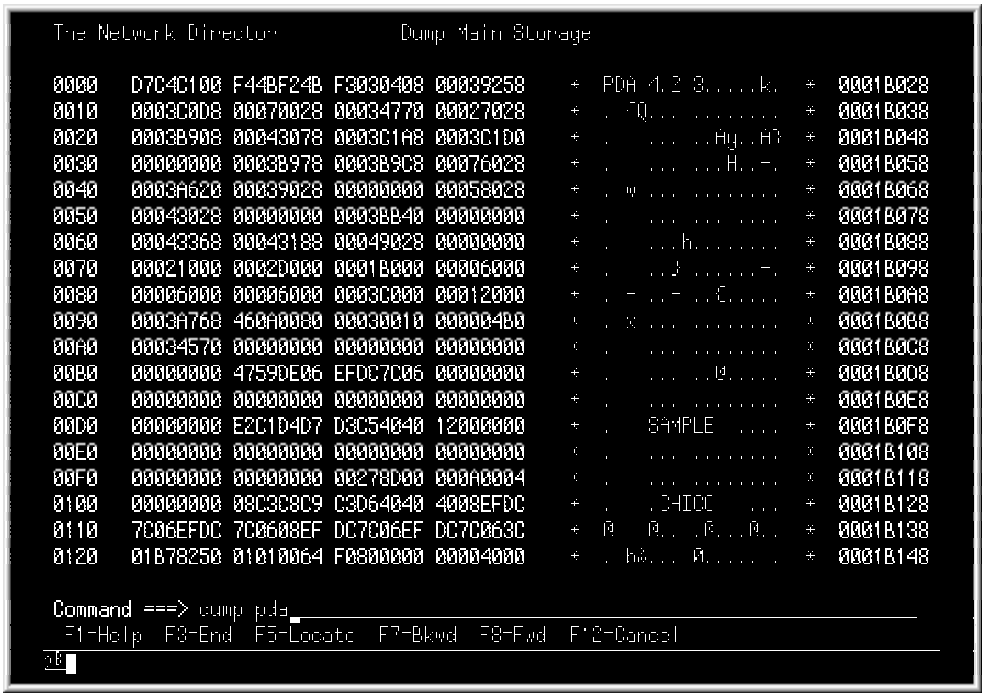


Figure 98. Sample DUMP Output Panel

You may also enter commands on the DUMP Primary Command line or press appropriate PFKEYS to control the DUMP mechanism.

The following commands are supported:

Command	Purpose
+hexvalue	relocates the current display forward in storage the specified hexvalue
-hexvalue	relocates the current display backward in storage the specified hexvalue
Bkwd (PF7)	"pages" back through main storage a panel full at a time

Command	Purpose
Cancel (PF12)	returns your terminal to the Network Administration panel
Dump	any valid DUMP command on the Primary Command line to redirect the dump facility to another location in main storage.
End (PF3)	returns your terminal to the Network Administration panel
Fwd (PF8)	"pages" forward through main storage a panel at a time
Locate (PF5)	fetches the value at offset four in the current display and refreshes the display at that address. This is useful when "running" down a control block chain for viewing successive control blocks.

It is possible to cause the DUMP command to attempt to reference storage that The Network Director does not have access to. This can produce a Protection Exception (OS S0C4). If RECOVERY=YES is in effect, you will be presented with a DUMP of the PDA and a message indicating the program interrupt.

If RECOVERY=NO is in effect, you will cause the entire Network Director to ABEND. It is the **responsibility of the Network Administrator to exercise proper controls** over the DUMP command and its usage.

Error Message Attributes

The Network Director will, during the course of execution, issue many single line messages that are intended to keep the Network Administrator aware of activity occurring. These messages will be "printed" on a standard output print file and may be maintained in the storage queue known as the LOG.

Each message utilized by The Network Director has several Attributes. They are as follows:

Number

The message Number is assigned by The Network Director and is unique within The Network Director's environment. The number normally takes the form TNDxxxxi, where **TND** is a constant, **xxxx** is a four digit number uniquely identifying the message, and **i** is the Class identifier.

Each message is identified externally by its full Number. Within The Network Director, each message is referenced only by its four digits.

Abend

The Abend attribute indicates to The Network Director whether it should take a dump or not the first time this message is issued. The Abend attribute defaults to NO and when activated will cause The Network Director to force a program interruption through the recovery logic (where the DUMP= operand controls the type of dump).

If RECOVERY=NO is in effect, setting the Abend message attribute will **bring down the entire Network Director**. As a result, you should exercise extreme care when setting the Abend characteristic on a message.

Class

Each Network Director message is also assigned a Class code and has an implied Class Level. The Class attribute is provided to group messages and to provide logical groupings that can be controlled via the WTO and LOG operands of the GLOBALS statement.

The seven currently defined Classes are Internal, Reply, Security, Change, General, Debug, and Trace. These classes are identified as Class Level 20, 40, 50, 60, 80, 90, and 100 respectively.

Internal messages are related to the internal functioning of The Network Director and will only be produced when a logical error or unanticipated condition has occurred. Unanticipated VTAM and VSAM feedback codes are examples of Internal Class messages. Typical or "expected" non-zero return codes are categorized into the Debug Class.

Reply messages are specific responses or prompts to the Operator's Console.

Security messages are associated with network element status changes (LOGON/LOGOFF) and any logical violations that occur during a network user's session with the network. Repeated attempts to LOGON with the wrong Password is an

example of a Security Class message. Application status changes is an example of a Status Class message.

Changes class messages are associated with Application status changes or any unusual return codes that may be received during execution.

General messages describe events that can be considered "informational". These occur during normal processing and typically describe valid actions performed during the network's normal processing. A User Sending a message or logically connecting to a target subsystem are examples of General Class messages.

Trace messages describe events that are internal in nature, but describe specific events occurring within The Network Director. Care should be exercised when activating Trace level logging due to the large volume of output that will occur. An example of a Trace message is the Dispatcher dispatching a specific DFB or subfunction.

Text

The message Text is a single line of less than 72 characters that contains an expanded description of what the message Number means. The Text can contain variable information that is filled in by The Network Director during execution.

The variables are represented as symbolic variables (alphanumeric literals beginning with an ampersand (**&**) or as positional constants using the characters **$** (alphanumeric) and # (numeric)

Symbolic Variables

A **Symbolic Variable** has the following general form:

```
&name[({type-specification|A8})]
```

Figure 99. Variable Syntax

where:

& identifies a potential symbolic variable to The Network Director

name is the one to eight character assigned identity that represents a particular piece of variable information. It may be specified in either UPPER or lower case.

type-specification identifies the characteristics of the variable that is input to the formatting process and how many significant positions the result of the variable replacement should be. The default is "A8", which is interpreted as Alphanumeric, 8 characters long.

Type Specification: The **type specification** is present as a "suffix" to the actual variable (when required or desired) and is enclosed in parends. When The Network Director's variable processor detects a type specification, it scans for numeric and alphabetic characters. The numeric digits are accumulated and treated as a decimal value, indicating the desired length of the significant characters or digits in the result.[45]

Individual alphabetic characters are treated as an indication to the variable processor of the type of input the variable should be handled as. Defined input types are:

[45] It is possible that certain numeric conversions and inserted commas, etc. may cause a variable replacement to exceed the numeric type specification value.

Type	Translation
A	Alphanumeric EBCDIC data input. Output will be translated to insure it contains EBCDIC printable characters.
D	The input is a 32 bit binary fullword containing a decimal value to the resolution of one hundreths. The result will be formatted as nnn,nnn,nnn.nn in the output stream.
E	Alphanumeric field that has already been edited (no translation or validation is required).
F	The input will be treated as a 32 bit binary whole numeric value. The output will be formatted as nn,nnn,nnn,nnn with appropriate commas inserted
H	A 16 bit binary numeric value. The output will be formatted as nn,nnn with appropriate commas inserted
M	The input 32 bit binary fullword contains milliseconds and will be formatted in mm,mmm:ss.ths format.
N	The data is treated as a binary halfword with no editing requirements.
Q	The input is a 4 byte packed field containing a calendar date
S	The data is treated as a binary fullword with no editing requirements.
W	Input field is a 4 byte packed field in storage containing a time of day in hh:mm:ss format
X	Data will be treated as hexadecimal and will be formatted on output as two EBCDIC bytes per character, represented as 0-9, A-F.

As examples, assume that the &TERM variable is the alphanumeric value "TERM4321" and &COUNT is a binary fullword of X'00001005' The following specifications would produce the following translations:

Variable	Interpretation	Result
&name	No type specification is present. Therefore, The Network Director will use A8 as the implied specification (no variable compression will be done)	TERM4321
&name(5)	The numeric 5 causes the variable to be truncated at 5 characters	TERM4
&name(x8)	Indicates that the input should be treated as 8 characters hexadecimal.	E3C5D9D4F4F3F2F1
&count(F)	The input binary fullword is treated as a standard decimal number	4,101
&count(d)	Indicates that the number is a decimal value accurate to the hundreths precision	41.01
&count(h)	The H or halfword specification indicates that the input field consists of only two bytes in storage. Because this improperly matches the data being pointed at, the variable processor will produce the result "0", which is the numeric equivalent of the first half of the &COUNT field. This example demonstrates why you need to be careful in utilizing the type specifications correctly.	0

Positional Constants: Some versions of The Network Director utilize two special symbols in the internal messages (TNDMSGS CSECT) to establish the location in the message where the positional parameters were to be placed. The dollar sign ($) represents alphanumeric data and the pound sign (#) represents numeric values. The number of contiguous special symbols indicated how many characters are to be replaced.

Blank Suppression: The Network Director's variable processor simply replaces Positional Constants with the result field without regard for any information that might be present adjacent to the variable itself. If you place additional text immediately to the right of the variable, it is possible that variable replacement will overlay it.

As an example, the string "$$$$$ 12345678" would be changed to "NRS 345678", if the variable value is "NRS".

If there is a type specification (indicating a Symbolic Variable), The Network Director's variable processor will shift the result field appropriately to insert the variable. Thus, a specification of "&SITE(8) 12345678" will produce "NRS 12345678". In most cases, this is a desirable effect, but you may wish to keep this in mind when designing LOGOs, etc.

Example

The system variables discussed under "Variables" on page 16 may also be utilized in the message text. An example of this can be portrayed as:

```
TND0152S Application $$$$$$$$ is now Active from &NETID..
```

The Network Director will fill the first Positional Constant with the first value passed to the Variable Processor and &NETID with the value as defined by the Symbolic Variable named NETID. This message can also be specified as follows to utilize all Symbolic Variables:

```
TND0152S Application &1(a8) is now Active from &NETID..
```

Use Count

Each active message in the DMT storage chain contains a use count. This use count is used internally to identify messages that have been recently used (issued, interpreted, etc.). When a message in the storage chain has not been used recently, The Network Director will automatically remove it from the chain (to save storage) and place another message in its place.

The Use Count is only of use by The Network Director for managing storage consumption, but is contained in the DMT panel for informational purposes.

Write to Log

For OS and GCS systems, the Write to Log attribute allows the installation to identify specific messages that should be sent to the system log (in addition to TNDLOG and the LOG queue). When set to YES (default is NO), The Network Director will issue WTL to place the message text into the system log.

Modifying the Attributes

Every Network Director message has Error Message Attributes. Each message has assigned defaults that can be changed at your installation via the SHOW processor.

To invoke SHOW to operate on a Network Director message and its attributes, you must be an authorized Network Administrator (UPDATES=YES). Simply enter SHOW MESSAGE=nnn (where nnn is the message number) on the Network Administrator Command line.

Entering **SHOW MESSAGE=196** would result in the following panel:

Figure 100. Network Director Message Edit

You can then tab to the appropriate location and modify most of the message attributes.

Modification to the text or Message Class is available to you to enable tailoring of the messages and creation of additional Message Classes.

Once you have committed your changes (pressed F3), The Network Director will save your changes into the External File. These items will be reloaded each time The Network Director initializes so that your changes will be kept across executions.

Message Philosophy

During the course of execution, The Network Director may encounter several error conditions within the VTAM, VSAM, or other interfaces to operating system services. The Network Director's internal service routines will automatically produce error messages containing the exact return codes from the Access Methods, etc. These return codes should be utilized to investigate the type of error that is occurring to cause the unexpected return code.

As an aid to the Network Administrator, The Network Director will also attempt to identify and interpret exactly what the error condition implies. The Director will then place into the LOG one or more messages describing the event that has occurred. This interpretation is intended to minimize the hunt that so often occurs within subsystem Messages and Codes manuals. While this characteristic of The Network Director is useful and helpful, the Network Administrator is reminded that the initial error and return codes are the authoritative source for exploring problems.

Along with these interpretive messages, The Network Director will also *indent* messages that are subordinate to a *primary* message. As an example:

```
TND0116C Sense: X"08", Modifier: X"31", User: X"0000", LU: TM03
TND0406G   LU Component disconnected (Power Off - Test Request)
```

This indicates that The Network Director has received VTAM Sense information from the device named TM03. Message 406 is The Director's attempt at interpreting what the Sense information means.

When The Network Director reacts to a situation, it will also place an indented message into the LOG to inform the Network Administrator exactly what activity it will perform based upon the activity occurring. Reviewing entries within the LOG can frequently provide all the necessary information the Network Administrator may need for problem diagnosis and resolution.

Technical Support

North Ridge Software, Inc. places a large emphasis on The Network Director operating as designed and documented in these publications. However, if and when an inconsistency or confusion occurs, we have made efforts to establish support processes and procedures that will permit our licensed installations to obtain a resolution to software related difficulties as quickly as possible.

This section of the manual discusses how we have organized our support process, describes the mechanisms in place, and provides a basic introduction to how you can obtain Technical Support.

Problem Reporting

Whenever you have encountered a problem within The Network Director's environment, you should carefully collect all information that applies to the situation prior to contacting North Ridge Software, Inc.

Problems are generally grouped into two general categories (ABENDs and Processing Errors).

ABEND

For ABENDs, you should collect information as described in the associated Installation manual. This information will differ for each Operating Environment (OS, DOS, or VM), but will typically include the LOG output listing, any core dumps produced, etc.

You should also be prepared to respond to general questions about the physical terminal network in use (terminal types and model numbers).

Processing Errors

Processing errors are usually related to two general areas (network definition errors or External File errors).

Network definition errors can usually be resolved through proper utilization of Network Administrator DISPLAY commands and online modifications. Use the DISPLAY command to interrogate The Network Director about the network element in question. Insure that the relationships implied within the network definitions represent the desired logical network.

The Network Director offers a wide variety of operands that interact with each other. If you are uncertain as to how they should operate in conjunction with one another please contact North Ridge Software, Inc. Technical Support.

External File errors are usually related to heavy activity against the file without intervening preventative maintenance. This includes increasing the allocation as the usage of the Message Facility increases (space problems). Normally, External File problems can be corrected (with the network still "up") by closing the External File via Operator Command (CLOSE EXTERNAL) and rebuilding it in another batch partition or address space.

Remember that when the External File is closed, the Message Facility will not be capable of saving any messages on the External file and the majority of the INFO mechanism will not be available. Network Director message Text and stored Profiles will also be restricted in use. However, The Network Director will continue to service the network. When the necessary corrections have been made, open the External File via Operator Command (OPEN EXTERNAL) and the processing errors should be corrected.

In the event that a Processing Error occurs that is not covered by the preceding discussion, you should collect the following information prior to contacting NRS Technical Support:

1. Network Director facility associated with the Processing Error (Selection, NSI, SSI, Message Facility, INFO Mechanism, etc.)
2. Type of Processing Error (incorrect results, invalid response, etc.)
3. Detailed description of the Processing Error

Resolution

North Ridge Software, Inc. Technical Support personnel will immediately identify your problem report with a unique number called a Problem Number or an APAR.

This number will be used to track your reported problem and will be used to identify any fix that is eventually written to correct the difficulty. You should make a note of the number and use it in any correspondence or further communication about the Problem.

If the problem report results in a PTF (correction) to The Network Director, it will normally be made available on the next normal maintenance tape. In the interim, individual installations may choose to install specific fixes on The Network Director to resolve specific problems. The fixes will be available to authorized Maintenance sites in "zap" or "patch" format (OS IMASPZAP, DOS MSHP, VM ZAP statements). Source changes (where necessary) will be available in OS IEBUPDTE, DOS LIBR, and CMS UPDATE decks.

Any PTFs that are applied at your site should be carefully documented. It is the installation's responsibility to insure that the next maintenance tape received includes all the necessary corrections.

PTFs, APARs, and Problem Numbers

Interactions with NRS, requests for product enhancements or corrections, and actual product fixes are all identified by unique identifiers. The exact identifier scheme used is a function of the type of interaction transpiring.

Definitions

The following terms and definitions are used at North Ridge Software, Inc.:

Term	Definition
APAR	an Authorized Program Analysis Request. This is generated for all enhancement requests or requests to research a problem, shortcoming, or problem within a product. NRS Level 1 technical support will generate APARs from Problem reports that have been validated as requiring additional effort on NRS' part.
PTF	Program Temporary Fix. This represents a product correction that is generally applicable to all installations utilizing the product. PTFs will be incorporated into the product source during the next maintenance cycle.

Figure 101. Problem Report Definitions

The format for the names of the individual interactions is NRSnnnn or TNDvvvnn where:

NRS identifies a problem report or request (APAR) that NRS personnel have taken or will take action upon.

TND establishes the element as a Network Director PTF.

nnnn or nn is a unique identity for the specific interaction between NRS and your installation.

vvv is the version number that the PTF applies to.

Status Value Meanings

Each APAR or PTF has a North Ridge Software, Inc. assigned status value.

Status	Meaning
ACCEPT	represents a request for enhancement that has been accepted by North Ridge Software, Inc. and will be implemented within The Network Director in a following product release
CALL	identifies that the associated APAR or PTF is pending a call to the originating location from NRS personne.
CLOSED	is a APAR, PTF, or Problem that has had a resolution or an answer provided
CONFIRM	indicates that the interaction has had a response delivered to the originating location and is waiting for a confirmation that the PTF or problem resolution did, in fact, correct the reported difficulty.
DOCUM	identifies the APAR or Problem as representing a correction to the manual or documentation set
LOCAL	identifies a PTF that is specific to a particular client or condition and will not be incorporated during normal product maintenance cycles.
FUTURE	is a request for enhancement that is currently being considered
OPEN	is an APAR or Problem that has been presented to North Ridge Software, Inc. and no reply or fix has been generated yet
REJECT	is an APAR whose content requested a change, but will not be implemented in a future version of The Network Director
WAIT	represents a situation where additional information is required

Figure 102. APAR, PTF, and Problem Number Status Values

The following examples should help to clarify service name usage within North Ridge Software, Inc.

Number Meaning

NRS3210 is APAR number 3210 that requires or required NRS technical support action

TND36032 is PTF number 32 and was generated based upon the 3.6.0 version of The Network Director

NRS Web Site

North Ridge Software, Inc. operates a dedicated Web Server dedicated to supporting NRS licensed locations at WWW.NRSINC.COM. This server is directly connected to the Internet and can be used to improve communications both directions between NRS and NRS licensed locations.

HTTP service is provided from the NRS Home Page at http://www.nrsinc.com/index.html, which has an appearance (as of the date of this publication) similar to:

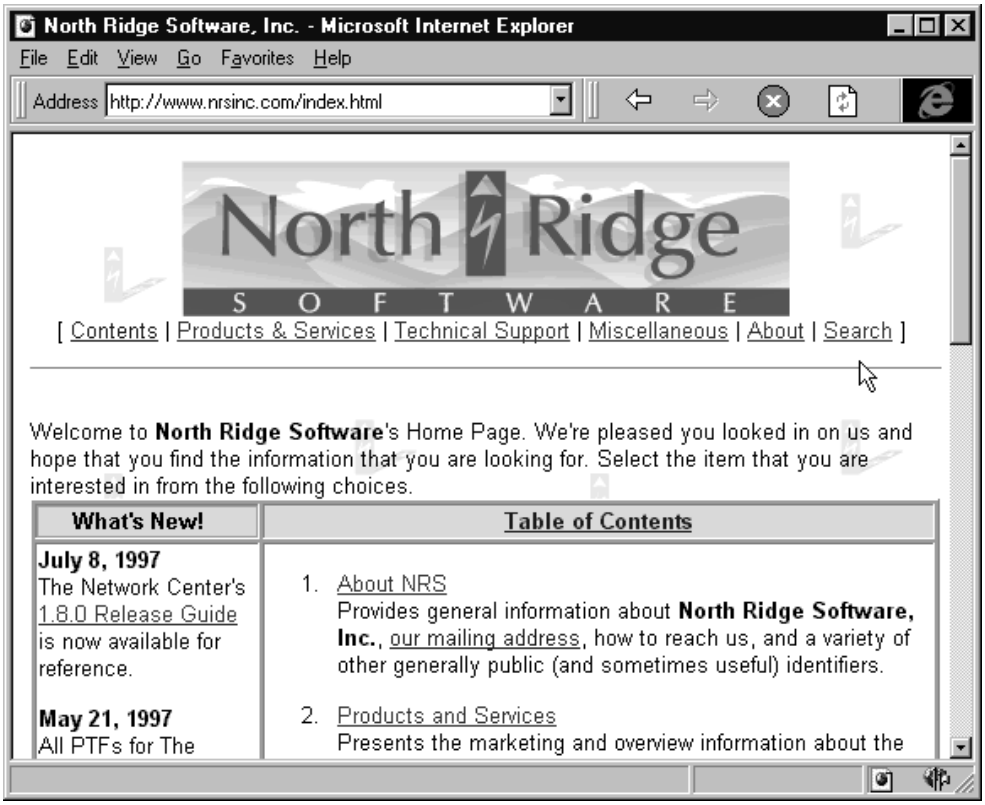


Figure 103. WWW.NRSINC.COM

Services offered by NRS to its clients associated with this server via the Internet are listed in the following paragraphs.

Mail Processing

You can communicate directly with NRS staff by sending mail to:

```
userid@NRSINC.COM
```

Figure 104. NRS Email Ids

Where:

userid can be the first name of the individual you would like to communicate with. It can also be one of the following generic Email ids:

- **ACCOUNTING** questions, requests, or comments about any aspect of NRS invoicing processes
- **INFO** requests for general information about North Ridge Software, Inc.
- **SALES** any issue related to sales activities associated with NRS products
- **STAFF** general items of interest to any staff member within NRS
- **SUPPORT** accepts mail related to the technical support of any NRS software product
- **WEBMASTER** suggestions, requests, or observations associated with the NRS Web site or related issues

NRSINC.COM is the North Ridge Software, Inc. registered Domain Name and must be specified as indicated

The NRS Mail Server supports all standard SMTP services, including the use of "attached files". If your mail package does not support the use of attached files, consider using FTP services to transfer and receive machine readable copies of files.

Marketing

The NRS Web Site contains marketing descriptions of all the NRS product offerings, which can be utilized to orient yourself to any NRS products that you may not be licensed for. This is also useful to use as a reference point for features in the products you may already have licensed.

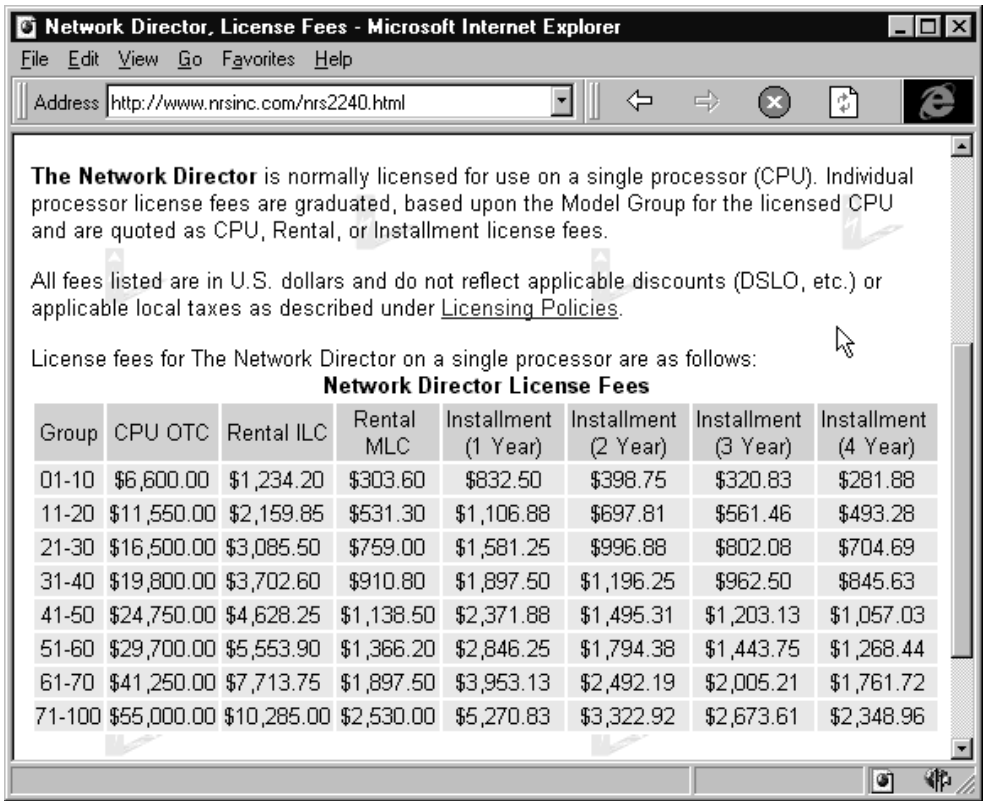
Many of the "pages" contain conceptual charts and diagrams identifying how a particular NRS products operates, as follows:

Figure 105. Web Marketing Page

However, remember that these pages are general in view (that's our definition of "Marketing"). If you are looking for detailed information, see "Publications" on page 286)

License Fee Schedules

The current NRS License Fee schedules for our products are also available via the Web Site. The license fee schedules not only identify what the fees are associated with acquiring a new license, but also imply the annual maintenance fees



Group	CPU OTC	Rental ILC	Rental MLC	Installment (1 Year)	Installment (2 Year)	Installment (3 Year)	Installment (4 Year)
01-10	$6,600.00	$1,234.20	$303.60	$832.50	$398.75	$320.83	$281.88
11-20	$11,550.00	$2,159.85	$531.30	$1,106.88	$697.81	$561.46	$493.28
21-30	$16,500.00	$3,085.50	$759.00	$1,581.25	$996.88	$802.08	$704.69
31-40	$19,800.00	$3,702.60	$910.80	$1,897.50	$1,196.25	$962.50	$845.63
41-50	$24,750.00	$4,628.25	$1,138.50	$2,371.88	$1,495.31	$1,203.13	$1,057.03
51-60	$29,700.00	$5,553.90	$1,366.20	$2,846.25	$1,794.38	$1,443.75	$1,268.44
61-70	$41,250.00	$7,713.75	$1,897.50	$3,953.13	$2,492.19	$2,005.21	$1,761.72
71-100	$55,000.00	$10,285.00	$2,530.00	$5,270.83	$3,322.92	$2,673.61	$2,348.96

Figure 106. Web Based License Fee Schedule

Note: The actual invoice amounts may differ from what is listed if your installation has applicable Volume Discounts or Enterprise License arrangements.

Buckets

The NRSINC Web Page also contains the text for the current buckets for all supported releases of The Network Director and The Network Center available online. You can browse the actual contents of a particular bucket:

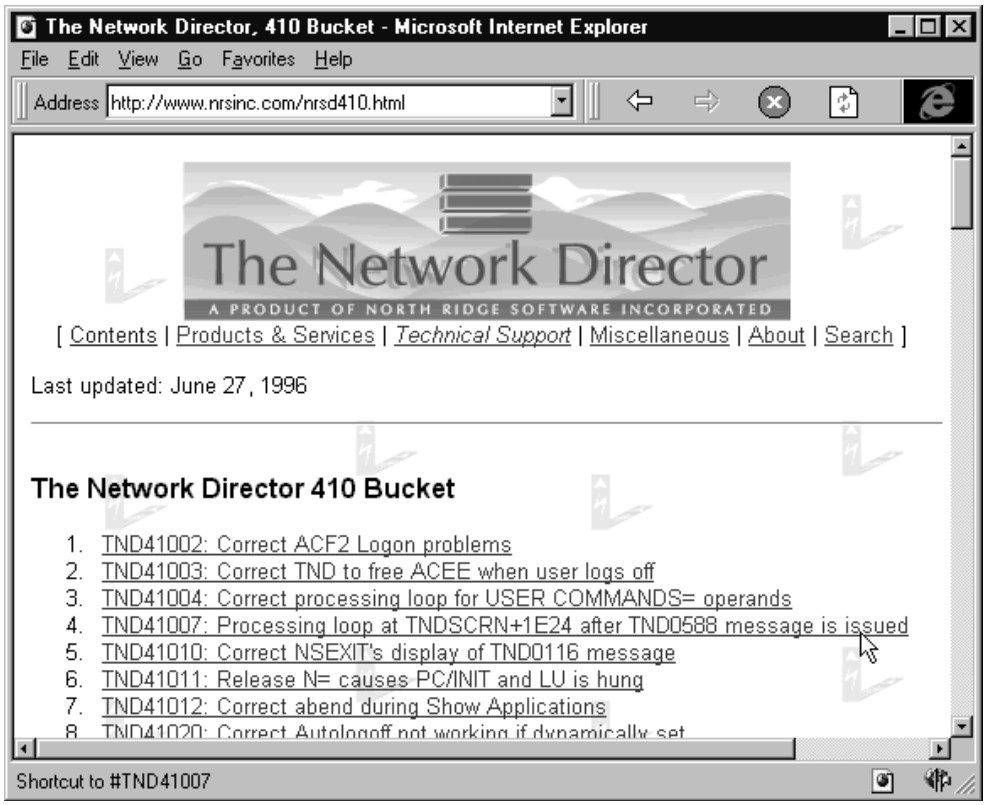


Figure 107. Web Based Network Director Bucket

It is also possible to use FTP (File Transfer Protocol) to obtain a copy of the applicable bucket from the NRSINC system at FTP.NRSINC.COM/NRSINC.

If you find that you have a need to FTP a file to NRS Technical Support, you may send files to FTP.NRSINC.COM/PUBLIC. Please use the applicable NRS APAR number as a portion of the FileName so that NRS can identify what the file relates to. It is also wise to send an Email message to the appropriate individual or function within NRS Technical Support to let them know you have uploaded a file that requires some type of action.

Publications

The more recent versions of the NRS product publications have also been converted to HTML for Web browsing. You can see the actual contents of the manuals without ever having the actual hardcopy.

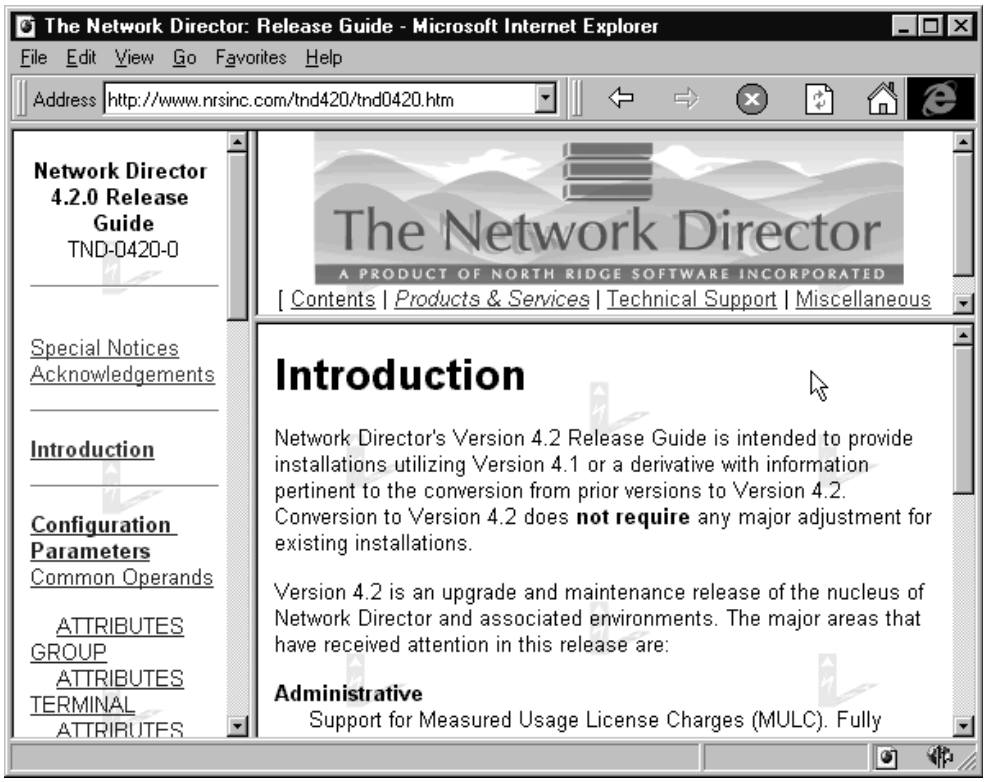


Figure 108. Web Based Network Director Publication

These publications are a direct conversion of the DCF source that produces the hardcopy manuals and will replicate exactly what they contain (any errors contained in the hardcopy manuals will be replicated in the Web based versions). Keep in mind we try to update the publications regularly, but the Web based publications are intended to reflect the status of the publications at a specific point in time (watch the publication TNL level to identify a specific level of the publication).

Glossary

ACB: Access Method Control Block - the operating system control block that identifies The Network Director to VTAM and VSAM.

ACF2: the system security offering from Computer Associates.

APPLICATION: The Network Director's definition used to identify a logical application.

APAR: Authorized Program Analysis Request, a request for enhancement or investigation into a current feature

APPLID: The 1 to 8 byte code that identifies The Network Director to VTAM. Used in conjunction with the ACB and the GLOBALS APPLID operand.

BROADCAST: A type of message within The Network Director that is sent immediately to its targeted users.

CANCEL: A Network Director operator command that terminates a DFB immediately.

CLOSE: A Network Director operator command used to manage the external interfaces.

Combined Display: A type of network DISPLAY that requires multiple operands to properly identify the request.

CUA: Common User Access, a portion of Systems Application Architecture that specifies how a computer application should portray and obtain information from a terminal user.

A "CUA Application Selection Panel" user is a Network Director user that is using The Network Director's CUA method of communication with The Network Director

DEFAULT: A network definition that sets basic values for all network users.

DISCONNECT: A Network Director operator command that breaks the session between The Network Director and a VTAM terminal.

DISPLAY: The generalized Network Director reporting command. This command has the types: Overview, Specific, and Combined.

External File: The VSAM KSDS file used by The Network Director for storing Profiles, Messages, and INFO information.

LOG: Identifies both the external Print file (SYSPRINT or SYSLST) and the main storage queue used for LOG viewing by the Network Administrator.

GROUP: A network definition that identifies a logical network element that can be shared by multiple network elements.

HOLD: An operator command to remove a network element from eligibility within the network. Also, it is the condition network elements are in when a HOLD operator command has been processed against it.

ICCF: The DOS Interactive Communication Control Facility. An online program development subsystem within DOS/VSE.

LOGAPPL: The VTAM operand on the LU or PU statement that can be used to direct terminals to The Network Director.

LU: The acronym for a VTAM Logical Unit. Typically dealt with as a *terminal*.

LU1: The acronym used to identify a type of terminal that is not capable of accepting the 3270 data stream for output. NTO and many available protocol convertors accept LU1 transmissions from the host and convert it to a data stream acceptable to line mode devices (VT100, IBM 3101s, PCs, etc.)

Maintenance: The process associated with installing a new release of a software product to incorporate upgrades, fixes, and enhancements.

Message Class: The grouping of Network Director issued messages into various categories (Internal, Reply, Change, Status, General, and Trace).

Message Number: The unique 4 byte identifying number associated with a Network Director message (not a Message Facility message).

Message Text: The actual text associated with a Network Director message.

Network Administration: The process of managing the logical network to guarantee availability, security, and usability.

network element: The Network Director's term for a specific user or terminal that is active within the network.

network entity: Used to identify any element within The Network Director's environment that is to be managed. It includes APPLICATIONs, TERMINALs, USERs, GROUPs, PROFILEs, as well as network elements.

non-CUA mode: a method of interaction between the terminal user and The Network Director that does not follow the CUA standard. This was the "original" mode of communication between a terminal user and The Network Director (the original Network Director Application Selection Panel was released years before CUA was published).

OPEN: The Network Director operator command to enable an external interface. Opposite of CLOSE.

operating environment: the basic operating system that The Network Director will execute in (OS, DOS, or VM

Operator Interface: The defined mechanism within OS and DOS to communicate with the operating system console.

Overview Display: A type of Network Director DISPLAY that presents summary information about the network.

Parameter Name: The 1 to 8 byte identifier that identifies the network entity within the network definitions. The Parameter Name assigns a logical name to the network element being defined.

Parameter Operands: Individual arguments present on a network definition. The Operands give each definition its unique characteristics.

Parameter Statement: The combination of the Parameter Name, Statement Identifier, and Parameter Operands that defines a network entity.

PROFILE: The Configuration Parameter statement that defines basic operator characteristics associated with utilizing The Network Director's facilities.

program operator: A VTAM facility that allows standard VTAM "application programs" to issue and receive VTAM commands and messages.

Prompt List: Identifies a series of choices available to a network operator when using the INFO facility.

PTF: Program Temporary Fix, a correction to the software that should be incorporated by all using installations to prevent undesired software difficulties

PU: A VTAM Physical Unit. Typically identifies a single physical terminal.

RACF: the system security offering from IBM Corporation

RELEASE: A Network Director operator command to reverse the effect of a HOLD command.

Release Letter: Describes the cover letter that accompanies the distribution tape and contains information specific to the tape and its contents.

REPRO: A facility within VSAM's Access Method Services that allows a file to be reproduced.

SHOW: The interactive command to manipulate Network Director definitions and associated control blocks.

SIMLOGON: A Network Director operator command that facilitates the testing and acquisition of a specific terminal.

SITE: A Network Director statement that identifies another computer installation that is also operating The Network Director. This definition allows the computing facility to control and take advantage of communications between The Network Director in the two CPUs.

Specific Display: A type of DISPLAY request that produces detailed information about a network element.

Stage One: The process of deciding major characteristics associated with the installation of The Network Director.

Stage One Listing: One of the results of Stage One, which describes that activities that should be followed to complete installation.

Stage Two: One of the results of the Stage One process. Stage Two consists of multiple jobs that should be run to complete the installation as specified in the Stage One deck.

Statement Identifier: One of the major definition Statements used to identify network elements. The Statement Identifiers are: APPLICATION, PROFILE, SITE, TERMINAL, USER, GROUP, DEFAULT, GLOBALS, DISPLAY, SHOW, etc.

STOP: An operator command used to terminate the execution of The Network Director.

SYSIPT: The standard DOS input file. The Network Director expects the Configuration Parameters to be present in SYSIPT.

SYSLST: The standard DOS output file. The Network Director will produce its printed LOG file on SYSLST.

SYSPRINT: The OS DD statement typically defining a SYSOUT=A printer that The Network Director will place its printer LOG file on.

TERMINAL: A network definition defining one or more specific terminals and their characteristics.

TNDGEN: The Stage One generation Macro. This is used to produce the Stage Two jobs and the Stage One Listing.

TNDPARMS: The OS DD statement (typically DD *) defining The Network Director's input Configuration Parameter file.

TSO: IBM's Time Sharing Option. A program development facility for MVS installations.

USER: The network definition that identifies one or more specific network users and their specific characteristics.

Wild Character: The plus ("+") sign. Used within many of the network definitions to generally group network elements and their characteristics.

zap: the process normally used to identify the application of a PTF

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z