

GENERAL INFORMATION

Document Number TNC-0001-9

The Network Center

North Ridge Software, Inc.

Copyright

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

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

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

North Ridge Software, Inc.
1305 11th Street
Bellingham, Washington 98225-7016
U.S.A.

(c) Copyright 1990-2007.

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

Telephone (360) 676-5999
FAX (360) 733-5970
Email support@north-ridge.com
Website http://www.north-ridge.com

Disclaimer

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:

CA ACF2, IDMS, ROSCOE, and TOPSECRET

IBM ACF/VTAM, ACF/TCAM, NMPF, NPDA, VM/GCS, OS/VS1, NETVIEW, NLDM, NPA, CMS, MVS, MVS/XA, MVS/ESA, OS/390, CICS/VS, TSO, IMS, RACF, NPDA, NCCF, z/VM, and z/OS

Table of Contents

Preface	1
Who Should Read this Publication	1
Examples Used in this Document	1
Where to Find More Information	2
How to Send Your Comments to North Ridge Software	2
Introducing the Network Center	3
Expanding VTAM Management, Manipulation, and Control	4
Session Establishment Manager	4
Session Timeout Manager	4
Session Activity Monitor	4
Dynamic Alias Name Management	5
Selection List Manipulation and Traffic Routing Prioritization	5
Interactive Control Block Formatting, Interrogation, and Manipulation	5
Accounting Facility	5
VTAM Command Facility	6
General Architecture	6
The Network Center Server	7
The Network Center Interface	7
General Operating System Structure	8
z/OS Structure	8
z/VM Structure	9
Communication Paths	9
Cross-domain Communications	10
Version 2.0.0 Enhancements and Changes	11
Support for IP LU Data in Access and Timeout Components	11
Access IP Enhancements	12
Timeout IP Enhancements	15
Publications Enhancements	17
Extended Internet Support	17
Base Facilities	19
User Interface	20
Administrative Facilities	21
TNCUTIL Batch Utility Program	21
Interactive Administration	23
Rule Processing	24
Pattern Matching	26
Rule Groups and Rulesets	26
Value Groups	27
Activity Logging	28
File Access	28

Accounting Facility	28
The Network Center Components	29
Access	30
Session Characteristics	31
Rule Processing	32
Alias	40
Session Characteristics	41
Rule Processing	42
Query	46
The Query Menu	47
Control Block Display and Interpretation	48
Select	50
Session Characteristics	52
Rule Processing	53
Timeout	56
Session Characteristics	57
Rule Processing	58
Technical Information	63
Supported Systems	63
Software Characteristics	64
Packaging	65
z/OS Systems	65
z/VM Systems	65
Publications	66
Base Set	66
Optional Components	66
Licensing	67
Ordering Network Center Trials	67
Appendix A. Network Center Trial Agreement	69
Glossary	71
Index	77

List of Illustrations

Figure 1.	Conceptual Network Center Architecture	6
Figure 2.	Network Center General Architecture in z/OS	8
Figure 3.	Network Center General Architecture in z/VM	9
Figure 4.	Communications Path Architecture	10
Figure 5.	Cross-domain Network Center Interface Example (LU to LU)	10
Figure 6.	Access Rule Definition Panel	12
Figure 7.	Access Rule IP Data Entry	13
Figure 8.	IP Data Display in the Message Queue	14
Figure 9.	Timeout Rule Definition Panel	15
Figure 10.	Timeout Rule IP Data Entry	16
Figure 11.	Publication Changes	17
Figure 12.	General CUA Screen Areas within the Network Center	20
Figure 13.	Network Center Administration Menu	23
Figure 14.	LOGAPPL Rule Definition Panel	25
Figure 15.	Pattern Matching Characters	26
Figure 16.	Group Definition Panel	26
Figure 17.	Ruleset Rule Panel	27
Figure 18.	Access Overview	30
Figure 19.	LOCALS Rule Definition Panel	32
Figure 20.	PAYDEPT Rule Definition Panel	33
Figure 21.	PAYDEPT IP Data Update Panel	34
Figure 22.	LOGAPPL Rule Definition Panel	35
Figure 23.	TCAS Rule Definition Panel	36
Figure 24.	TSO Rule Definition Panel	36
Figure 25.	MYSITE Rule Definition Panel	37
Figure 26.	OUTSIDE Rule Definition Panel	38
Figure 27.	DIRECTOR Rule Definition Panel	39
Figure 28.	General Alias Network Structure	40
Figure 29.	T31001 Rule Definition Panel	42
Figure 30.	OTHER Rule Definition Panel	43
Figure 31.	USERS Value Group Definition Panel	44
Figure 32.	NORMAL Rule Definition Panel	45
Figure 33.	Query Overview	46
Figure 34.	Query Selection List	47
Figure 35.	Query Menu Overview	47
Figure 36.	Query Hexadecimal Display	48
Figure 37.	Query Formatted Display	49
Figure 38.	General Select Network Structure	51
Figure 39.	TWOPATHS Select List Panel	53
Figure 40.	TODC2 Rule Definition Panel	54
Figure 41.	CICSPATH Select List Panel	55
Figure 42.	CICS Rule Definition Panel	55
Figure 43.	Timeout Overview	56

Figure 44. LOCALS Rule Definition Panel	58
Figure 45. LOCALS IP Data Update panel	59
Figure 46. PAYDEPT Rule Definition Panel	60
Figure 47. DAYS Rule Definition Panel	61
Figure 48. Supported Systems	63
Figure 49. z/OS Distribution Files	65
Figure 50. z/VM Distribution Files	65

Preface

This document provides general information about the Network Center Version 2 Release 0.0 (TNC 2.0.0) licensed program:

- Introduction to The Network Center
- Summary of new functions, enhancements, and other changes
- Descriptions of basic network facilities, features, and components
- Basic technical information, including packaging and licensing, guide to product documentation, and trial orders.

Who Should Read this Publication

This document is for individuals who plan to use the Network Center at his or her installation. It helps users to evaluate how the Network Center can help manage, manipulate, and control a VTAM network and to assess installation needs. It is also for anyone interested in a general overview of the The Network Center and its Components.

You might use the information in this book if you:

- Need information on the newest Network Center release
- Plan to install or configure the Network Center
- Plan to administer or utilize the Network Center
- Are considering licensing the Network Center at your installation
- Need basic knowledge of the Network Center for any reason

Examples Used in this Document

Examples included in this document are for illustrative purposes only; they should not be taken literally.

Where to Find More Information

The Network Center publications library consists of a base set, which is distributed to every Network Center installation, and optional Component manuals, which are distributed to Network Center installations based on Component license.

The base set includes the following manuals:

- *General Information* (TNC-0001): A general overview of the Network Center and each optional Component.
- *User's Guide* (TNC-0002): Guidance for utilizing the Network Center Interface.
- *Installation and Operations* (TNC-0003): Guidance for installing, configuring, and administering the Network Center and optional Components.
- *Query* (TNC-0006): Guidance for utilizing the Query Component.

The optional Component set includes the following manuals:

- *Access* (TNC-0005): Guidance for utilizing the Access Component.
- *Timeout* (TNC-0007): Guidance for utilizing the Timeout Component.
- *Alias* (TNC-0027): Guidance for utilizing the Alias Component.
- *Select* (TNC-0039): Guidance for utilizing the Select Component.

For online versions of these documents, visit the North Ridge Software, Inc. website at www.north-ridge.com.

How to Send Your Comments to North Ridge Software

| We welcome comments and suggestions that might help us to provide improved publications.
| Please send us any feedback using any of the mechanisms described under "Copyright" on page
| ii

Be sure to tell us the name of the document, the publication version, and the page, section, or topic you are commenting on.

Introducing the Network Center

Teleprocessing networks are a continually expanding entity in the data processing environment, making the ability to monitor, manage, and control network activities increasingly critical and complex. The networks must also ensure seamless, efficient communications between network elements and that the host can be easily, but securely, accessed.

These requirements demand an amazing array of hardware, including terminals, CPUs and TCUs, distributed processors, modems, telephone lines, patch cords, and protocol converters. They also demand complex and expensive software like VTAM, the NCP, and Netview, not to mention processing applications like CICS, IMS, TSO, and CMS.

While each data processing environment provides its own approach to managing network elements, many common, host based activities must occur in every network such as session establishment, session pacing, and selection route processing.

VTAM and Netview address many of these activities, but they are inadequate in several key areas such as the ability to deny specific sessions from establishing or to timeout sessions on an installation wide basis.

The Network Center is a suite of software components that work together or alone to resolve these and other inadequacies, allowing VTAM operators to better monitor, manage, control, manipulate, and secure an enterprise network.

The Network Center consists of Base Facilities including:

- Activity Logging
- File Access
- Accounting
- User Interface
- Administrative Facilities
- VTAM command capabilities

Note: See "Base Facilities" on page 19 for more information.

The Network Center Components include:

- Access: Session level access management and security
- Alias: Alias name assignment and monitoring
- Query: Control block interrogation and formatting
- Select: VTAM selection list manipulation and traffic routing prioritization.

- Timeout: Session level timing mechanism

Note: See "The Network Center Components" on page 29 for more information.

Expanding VTAM Management, Manipulation, and Control

The Network Center suite of components provides capabilities that extend your ability to manage, monitor, manipulate, and secure your VTAM network.

Session Establishment Manager

The Network Center's **Access** Component allows you to set Rules that control session establishment between LU pairs. As Access manages your local VTAM domain, it rejects and accepts session requests as directed by the Rules. The Network Center's Message Queue allows you to monitor Access session activity data in real time for both SNA and IP devices.

Note: See "Access" on page 30 for more information

Session Timeout Manager

The Network Center's Timeout Component allows you to set Rules that automatically terminate sessions between any LU pair based on conditions like maximum connect time or idle time intervals. Rule usage perspectives empower you to create efficient parameters, while The Network Center's Message Queue provides real time session activity data for both SNA and IP devices.

Note: See "Timeout" on page 56 for more information

Session Activity Monitor

As part of its base Administration facilities, The Network Center offers the **Message Queue**, which interactively displays Component messages and Network Center Server messages.

The Message Queue allows you to monitor Component based network data quickly and conveniently. Messages inform you of activities like user modifications, matched Rules, active users, and session activity.

For example, the Access Component generates a message for every session approved or denied by a particular rule, e.g. "Session approved between SLU P390 : LCL701 and Plu P390 : A06TSO1 by rule REST175".

Note: See the *Installations and Operations* guide for more information.

Dynamic Alias Name Management

The Network Center's Alias Component allows installations running VTAM to control alias name assignment in the Gateway SSCP for cross Network Sessions. You can set Rules for one to one, predefined, or dynamic alias translation parameters. The Message Queue displays all Alias name translations and activity in real time.

Note: See "Alias" on page 40 for more information.

Selection List Manipulation and Traffic Routing Prioritization

The Network Center's **Select** Component allows you to create Rules that manipulate the contents of VTAM lists, including Virtual routes, Gateway paths, SSCP names, and Adjacent Link Station names. Capabilities include defining, prioritizing, and monitoring contacts with other domains and networks for optimal load balancing efficiency and increased control over cross-network activities.

Status and statistics tools provide data on the amount of session traffic currently assigned to individual resources and other Select activities.

Note: See "Select" on page 50 for more information.

Interactive Control Block Formatting, Interrogation, and Manipulation

The Network Center's Query Component provides complete access to the VTAM control block structure via the Session Management Exit (ISTEXCAA) for extended diagnostic capabilities.

You can dynamically request control blocks in hexadecimal and formatted panels. Color coded, selectable fields allow you to interpret individual bit settings and explore control blocks, buffers, and chain elements related to individual control block fields.

A simple menu and command structure, search tools, and a system programmer console allow you to quickly explore, diagnose, and remedy VTAM problems, while the Message Queue displays the results in real time.

Note: See "Query" on page 46 for more information.

Accounting Facility

The Network Center's Accounting facility allows you to produce a general accounting record for various actions that occur during its processing. The Network Center Server produces **SMF records** for z/OS systems, **VM account records** for z/VM systems, or a **sequential output record** for either system.

Note: See "Accounting Facility" on page 28 for more information.

VTAM Command Facility

Users of the Query Component can issue VTAM operator commands from the Network Center's Command line. The VTAM command accepts any valid VTAM command that can be issued via the VTAM Program Operator interface. These include the VARY, DISPLAY, MODIFY, and REPLY commands.

Note: See "Query" on page 46 for more information.

General Architecture

The Network Center logically resides in and shares information with VTAM as demonstrated in the following figure:

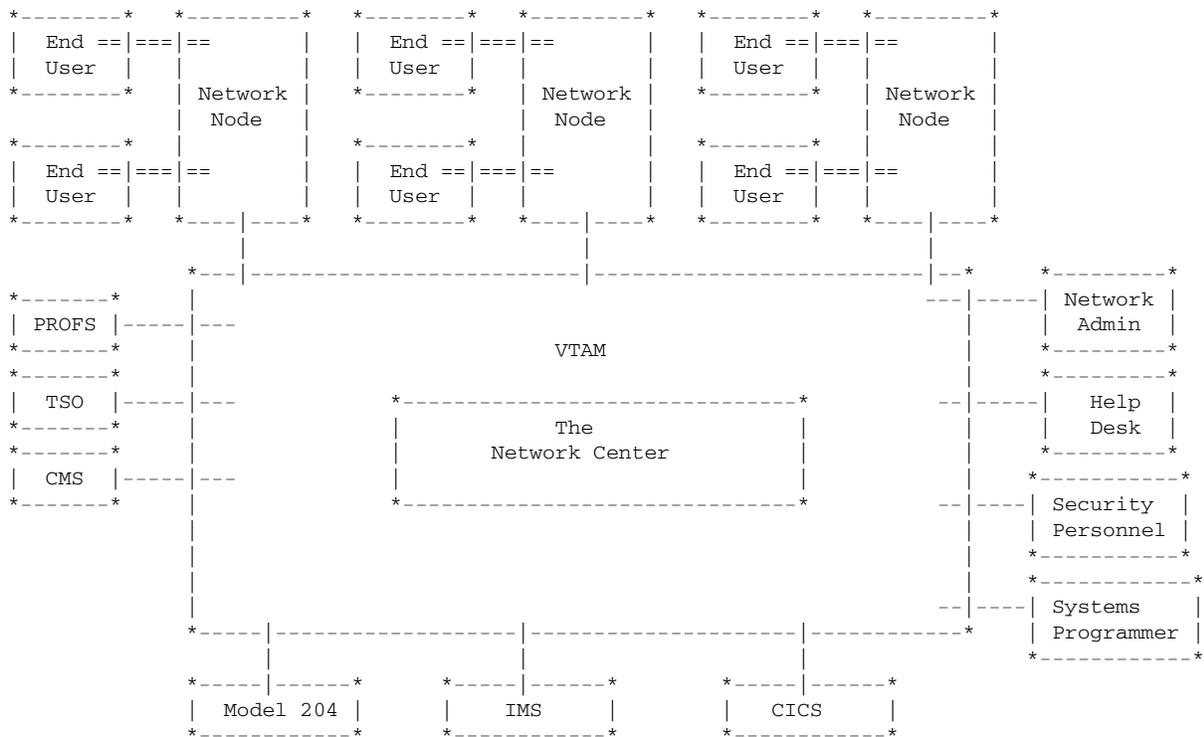


Figure 1. Conceptual Network Center Architecture

Within the Network Center, most of the Components use two logical software elements to carry out their tasks:

1. The **Network Center Server** allows Components to access information that is only available in VTAM's private address area, as necessary.
2. The **Network Center Interface** communicates requests to the Network Center Server via an established logical path. Depending on the operating environment, this path may be implemented using either VTAM LU to LU or IUCV APPC session logic, and can be local, cross-domain, or cross-network.

See "General Operating System Structure" on page 8 for more information on communication paths. The remainder of this section discusses the Server and Interface in detail.

The Network Center Server

The Network Center Server functions as an operating system subtask of VTAM within the VTAM address space or virtual machine. This architecture allows the Server to operate independently of VTAM while retaining access to the VTAM information required for servicing Component requests.

The Network Center Server routines are distributed as fully re-entrant load modules or text files and are activated by normal use of the VTAM Session Management Exit (ISTEXCAA). The ISTEXCAA routine receives control during VTAM initialization and establishes the Network Center's operating environment. Thus, you do not need to IPL or to locally modify VTAM or operating system code at any point of use of the Network Center.

The Network Center Interface

The Network Center communicates with end users through workstations that are owned by a terminal processing system like TSO or CMS. The terminal processing system provides an environment for the Network Center Components to interact with the end user.

The Network Center Interface for each terminal processing system consists of two Network Center Routines:

1. the nucleus routines that are terminal processing system independent
2. the driver routines that are specific to the terminal processing system that the Component operates in.

Currently supported environments for the Network Center Interface routines are CMS and TSO; the routines operate as a command to CMS (a MODULE file) or a command processor to TSO (a LOAD module).

Version 2.0.0 Enhancements and Changes

This chapter provides an overview of new functions and enhancements provided in the Network Center 2.0.0. These new functions and enhancements are briefly described in the following sections:

- Support for IP LU Data in Access and Timeout Components
- Publications Enhancements
- Extended Internet Support

Support for IP LU Data in Access and Timeout Components

The Network Center now offers enhanced capabilities for specifying and monitoring IP data in Access and Timeout. These new capabilities can help you to better secure, control, manage and monitor your network.

Previous versions of Access and Timeout provided control over IP resources via host based translating processes that assign LU names to the IP resources out of a pool. This method - while effective in controlling the masked resource - did not allow users to define, ascertain, or monitor the exact resource connected with the masked name.

With the Network Center 2.0.0 release of Access and Timeout, you can now specifically define the IP SLU partner, rather than depending on a name assigned out of an LU pool. IP information includes IP address, port number, and/or DNS name.

During active operations, the Message Queue displays the IP data in real time, allowing you to interactively view the IP address of any IP resource involved in a session being monitored by Access or Timeout.

Access IP Enhancements

The Network Center now supports the definition and monitoring of IP data in the Access Component.

Within Access Rules you can identify the IP address, Port Number, and DNS name of an Olu(Slu) device. The following figure shows the Access Rule panel:

TNCRULD	Network Center Rule Definition	ACCESS
Date: 01/15/2007	Time: 15:29:58	User: EXAMPLE
		Version: 2.0.0

Name	_____	Title _____
Count	_____	
Action	Allow_____	. . Alias . . *
Date. .first *	_____	. . Aliasnet *
. . . . last *	_____	. . Hcvname. *
Day *	_____	. . Hcvtype. 0_
Dlu (Plu) . . *	_____	. . Netid . . *
. . Adjsscp *	_____	. . Sscp . . *
. . Alias . . *	_____	. . Subarea. *
. . Aliasnet *	_____	. . IP data. No_
. . Hcvname. *	_____	Option . . . None_____
. . Hcvtype. 0_	_____	Rule type . Slu-Plu
. . Netid . . *	_____	Ruleset . . No_
. . Sscp . . *	_____	Time. .first *
. . Subarea. *	_____ last *
From *	_____	Session type *_____
Mode	Active_	
Olu (Slu) . . *	_____	
. . Adjsscp *	_____	

Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

Figure 6. Access Rule Definition Panel

Simply enter **Yes** in the IP data field; then, keeping the cursor pointed at the IP data field, press F11=Select to open the IP data entry window:

```

TNCRULD                      Network Center Rule Definition                      ACCESS
Date: 01/15/2007             Time: 16:35:27                      User: EXAMPLE                      Version: 2.0.0

Name . . . . EXAMPLE_                      Title example_____
Count . *-----*
Action . | TNCIPDT      IP Data Display/Update |
Date. .f |-----|
. . . . | Modify the following data fields. Then Enter. |
Day . . |-----|
Dlu (Plu | IP address * _____ |
. . Adjs | Port Number * _____ |
. . Alia | DNS Name . * _____ |
. . Alia |-----|
. . Hcvn |-----|
. . Hcvt | Enter F1=Help F3=Exit F12=Cancel F16=Save |
. . Neti *-----*
. . Sscp . . * _____ Time. .first * ____
. . Subarea. * _____ . . . . last * ____
From . . . . * _____ Session type * _____
Mode . . . . Active_
Olu (Slu) . * _____
. . Adjsscp * _____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 7. Access Rule IP Data Entry

You can then enter the desired IP data. To control the inclusion or exclusion of one or more values for the IP address, Port Number, and/or DNS Name fields, you can create pattern matching masks.

Upon activation, Access 2.0.0 will collect and display any IP data associated with the active Rules, including the IP address of the SLU involved in the session. This information is displayed within **containing symbols** in applicable Message Queue notifications, as shown in the following example:

```

-----
TNCMSGQ                Network Center Message Queue                More:  -  +
-----
TIMEOUT  TIMEOUT issuing SENDCMD to terminate session
CENTER   VARY NET, TERM, SID=E85B1C9151C4D829
CENTER   Network Services RU was received by NSXT
CENTER   Session between Slu P390 : SC0TCP01 and Plu P390 : A06TSO01 has termin
CENTER   Session between Slu P390 : A06TNC1 and Plu P390 : A06ZOS has terminate
ACCESS   Session approved between SLU P390 : SC0TCP01 < 4.33.18.202 > and Plu P
TIMEOUT  Timeout set for Slu P390 : SC0TCP01 < 4.33.18.202 > and Plu P390 : A06
ACCESS   Session approved between SLU P390 : SC0TCP01 < 4.33.18.202 > and Plu P
TIMEOUT  Timeout set for Slu P390 : SC0TCP01 < 4.33.18.202 > and Plu P390 : A06
ACCESS   Session approved between SLU P390 : A06TNC1 and PLU P390 : A06ZOS by r
TIMEOUT  Timeout disabled for Slu P390 : A06TNC1 and Plu P390 : A06ZOS by rule
CENTER   LU0 Path has been established to A06TNC1
CENTER   TSO User EXAMPLE requested Query Contact Center
CENTER   ACCESS resource granted to user EXAMPLE by RES1175 Rule
CENTER   TSO User EXAMPLE requested File Read
CENTER   TSO User EXAMPLE requested File Read
CENTER   TSO User EXAMPLE requested File Read
CENTER   TSO User EXAMPLE requested File Request FAB information
CENTER   TSO User EXAMPLE requested File Read
CENTER   TSO User EXAMPLE requested File Read
-----
F1=Help  F2=Prefix  F7=Bkwd  F8=Fwd  F11=Find  F12=Cancel  F19=Left  F20=Right
-----

```

Figure 8. IP Data Display in the Message Queue

To view messages that exceed the panel, use the F19=Left and F20=Right keys.

Timeout IP Enhancements

The Network Center now supports the definition and monitoring of IP data in the Timeout Component.

Within Timeout Rules, you can identify the IP address, Port Number, and DNS name of an Olu(Slu) device. The following figure shows the Timeout Rules panel.

TNCRULD	Network Center Rule Definition	TIMEOUT
Date: 01/15/2007	Time: 16:40:30	User: EXAMPLE
		Version: 2.0.0

Name _____		Title _____
Count		
Action . . . Monitor__	. . Alias . * _____	Hour .first * _____
Date .first * _____	. . Aliasnet * _____ last * _____
. . . . last * _____	. . Hcvname. * _____	Inactivity . 0 _____
Day * _____	. . Hcvtype. 0_ _____	Period start * _____
Dlu (Plu) . * _____	. . Netid . * _____ end * _____
. . Adjsscp * _____	. . Sscp . . * _____	Weekday . . * _____
. . Alias . * _____	. . Subarea. * _____	
. . Aliasnet * _____	. . IP data. No_ _____	
. . Hcvname. * _____	Option . . . None_____	
. . Hcvtype. 0_ _____	Rule type . Slu-Plu _____	
. . Netid . * _____	Ruleset . . No_ _____	
. . Sscp . . * _____	Time .first * _____	
. . Subarea. * _____ last * _____	
From * _____	Session type * _____	
Mode Active_ _____	Timeout conditions _____	
Olu (Slu) . * _____	Connect time 0 _____	
. . Adjsscp * _____	Force . . . No_ _____	

Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

Figure 9. Timeout Rule Definition Panel

Simply enter **Yes** in the IP data field; then, keeping the cursor pointed at the IP data field, press F11=Select to open the IP data entry window:

```

TNCRULD                      Network Center Rule Definition                      TIMEOUT
Date: 01/15/2007             Time: 16:40:30                      User: EXAMPLE                 Version: 2.0.0

Name . . . . EXAMPLE_          Title example_____
Count . *-----*
Action . | TNCIPDT      IP Data Display/Update | first * ____
Date . .f |-----| last * ____
. . . . | Modify the following data fields. Then Enter. | ty . 0 ____
Day . . |-----| tart * ____
Dlu (Plu | IP address * _____ | end * ____
. . Adjs | Port Number * _____ | . . * ____
. . Alia | DNS Name . * _____ |
. . Alia |-----|
. . Hcvn |-----|
. . Hcvt | Enter F1=Help F3=Exit F12=Cancel F16=Save |
. . Neti *-----*
. . Sscp . . * _____ Time. .first * ____
. . Subarea. * _____ . . . . last * ____
From . . . . * _____ Session type * ____
Mode . . . . Active_      Timeout conditions
Olu (Slu) . * _____ Connect time 0 ____
. . Adjsscp * _____ Force . . . No_
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 10. Timeout Rule IP Data Entry

You can then enter the IP data. To control the inclusion or exclusion of one or more values for the IP address, Port Number, and/or DNS Name fields, you can create pattern matching masks.

Upon activation, Timeout 2.0.0 will collect and display IP data associated the active Rules, including the IP address of the SLU involved in the session. This information is displayed within **containing symbols** in applicable Message Queue notifications, as shown in Figure 8 on page 14.

Publications Enhancements

All of the Network Center manuals have been revised and updated.

The following table shows information that has been relocated within the Network Center publication set.

Topics	Old Location	New Location
Release information	Release Guide (TNC-0182-1)	General Information (TNC-0001-9)

Figure 11. Publication Changes

A key objective for the publications in this release of The Network Center is to make the documentation available in a variety of formats (paper, Adobe's Acrobat Reader (PDF), and IBM's Softcopy Reader (BOOK). To facilitate this, we have modified the figures that are distributed throughout the publications to text based graphical portrayals. We acknowledge that this has caused a reduction in the overall quality of the figures in the printed materials, but believe this loss in quality to be offset by the benefits associated with having the publications available in a wider range of formats.

Extended Internet Support

We now offer a variety of Client oriented facilities based upon our website (www.north-ridge.com), including:

- Accounting and billing information
- Creating and managing service requests
- Reviewing and submitting APARs
- Reviewing or requesting PTFs or product release buckets
- FTP support for downloading distribution libraries, etc.
- Complete documentation available as downloads (BOOK or PDF format)

Please visit our site at <http://www.north-ridge.com> for the latest events and activities associated with North Ridge Software, Inc. and The Network Center.

Base Facilities

This chapter identifies some of the key facilities and architectures that provide ease of use across the Network Center, including:

- User Interface
- Administrative Facilities
- File Access
- Accounting Facility

User Interface

The Network Center's interface complies with the Common User Access (CUA) portion of IBM's Systems Application Architecture (SAA). These standards ensure that information is consistently presented and processed.

The following figure shows all of the general CUA screen areas available for a Network Center panel, including the action bar at the top of the panel, the function key area at the bottom of the panel, and the panel body:

```
-----  
Options  Exit  Help  
-----  
TNQMENU                                Query Menu  
  
Select one of the following choices by typing the number, or make a selection  
by positioning the cursor at your choice. Then Enter.  
  
____ 1. Application program blocks  
      2. Buffer pool directory  
      3. Buffer pool start options  
      4. Configuration table  
      5. Resource definition table  
      6. Session information blocks  
      7. Symbolic resolution table  
      8. System/user logmode tables  
      9. Vector table  
     10. Virtual route blocks  
     11. Vtam start options  
  
-----  
Enter  F1=Help  F3=Exit  F10=Actions  F12=Cancel  F13=Keys  F21=Command  
-----
```

Figure 12. General CUA Screen Areas within the Network Center

The Interface allows you to easily enter and manipulate data using standard entry and selection techniques, including keyboard and cursor tools. Color coding helps you to distinguish entry fields, command lines, available command actions, and special conditions like error messages and Rule violations.

Note: For more information on the Network Center Interface, see the *User's Guide* (NRS Publication TNC-0002).

Administrative Facilities

This section discusses the Network Center Server and the Network Center Components management and administration tools, which include:

- TNCUTIL Batch Utility Program
- Interactive Administration
- Component Administration
- Activity Logging
- File Access
- Accounting Facility

TNCUTIL Batch Utility Program

The Network Center and its Components use standard disk space to store and retrieve information. This disk space is called the **Network Data File** and is processed via BSAM (Basic Sequential Access Method) using READ, WRITE, and POINT.

A batch utility program called **TNCUTIL** allows you to install and maintain the Network Data File. TNCUTIL operates as a job in z/OS address space or as a command in a CMS virtual machine. Following are the available TNCUTIL commands and their purposes:

ADD	Inserts or updates a single data record or block in the Network Data File.
AUTHORIZATION	Adds a 15 digit authorization value to the list of values that permits the Network Center or a Component to operate.
CLEAR	Copies the contents of a single TNCLOGn sequential log file.
CONSOLE	Indicates whether the Network Center Server will initialize with the operator's console interface enabled (WTOR).
DELETE	Removes one or more data record(s) or block(s) from the Network Data File.
EXPORT	Extracts one or more Components and all associated records from the Network Data File and places the result in a sequential file suitable for subsequent input processing. Records are in LOAD format.
FORCE	Sets specific processing characteristics associated with concurrent processing of the Network Data File.
FORMAT	Initializes the Network Data File's blocks to an appropriate format.
ID	Establishes the Network Center Component that subsequent TNCUTIL commands will apply to.
INIT	Preformats the disk space that will be used as a recording medium for a TNCLOGn output.
INSTALL	Identifies the Network Center Component that is being installed and associates it with a logical identifier.

LANGUAGE	Sets the language code to be used for a single execution of TNCUTIL.
LOAD	Adds or replaces a data record to the Network Data File from a compressed input stream format.
LOG	Sets the message classes that will be written to the TNCLOG output printer file.
LOGMAX	Establishes the highest value that will be used in the TNCLOGn recording processes
LOGSIZE	Sets the size (in blocks) for each of the TNCLOGn disk files.
PASSWORD	Sets the one to eight character string that represents the password required for The Network Center to use the VTAM APPL definition set via the SERVER operand.
PRINT	Produces a hardcopy listing of one or more data records or data blocks on the output printer file (TNCLOG).
REMOVE	Deletes one or more Components from the Network Data File (REMOVE is the opposite of INSTALL).
SERVER	Sets the one to eight character value that is the VTAM APPLID or the IUCV path identity that will identify the Network Center Server to the Network Center Interface user.
SSCP	Establishes the identity for the OPTIONS record within the Network Data File.
UNLOAD	Extracts one or more records from the Network Data File and places them into a sequential output file in a format suitable for subsequent input to TNCUTIL. Records are in compressed LOAD format.
WTO	Sets the message classes that will be automatically written to the operator console. Classes include Critical, Internal, Notification, and Trace.

Interactive Administration

The Network Center's Administration menu allows you to perform tasks associated with installing, specifying, and maintaining the Component definitions stored in the Network Data File. You can access the Administration menu from the Network Center Interface main menu.

The Administration Menu appears as follows:

```
Options  Exit  Help  Component
-----
TNCADMN          Network Center Administration          CENTER

Select one of the following choices by typing the number, or make a selection
by positioning the cursor at your choice. Then Enter.

___  1.  Applied PtfS
     2.  Authorization
     3.  Center options
     4.  Close TNCLOG output
     5.  Install a component
     6.  Message queue
     7.  Network data file
     8.  Reload Data File
     9.  Remove a component
    10.  Reset Anchor Blocks
    11.  Rule processing
    12.  Storage usage
    13.  Status output log
    14.  Swap output log

-----
Enter  F1=Help  F2=Component  F3=Exit  F12=Cancel  F13=Keys  F21=Command
-----
```

Figure 13. Network Center Administration Menu

The Administration menu choices provide the following operations:

Menu Entry	Purpose
Applied PTFs	Displays the number of any PTF activity applied against the operating Network Center and Components.
Authorization	Displays or enters the authorization values that enable the Network Center and Components to operate. NRS provides these values during licensing procedures.
Center options	Establishes the global settings that determine the Network Center's operation.
Close TNCLOG output	Closes the TNCLOG sysout file, which routes it to the operating system for processing.
Install a component	Allows the Network Administrator to interactively install a logical Component.
Message queue	Displays the messages issued by the Network Center or the Components during their execution.

Network Data File	Allows the Network Administrator to interactively manipulate the Network Data File contents, including Query's control block definitions and Network Center Help and Message text and characteristics.
Reload Data File	Allows the Network Administrator to initialize the Network Center Server from the information on the Network Data File. (The Network Center Server does not actually restart. Instead, all Network Center Server initialization information is read from the Network Data File and the Server is then logically initialized.
Remove a component	Eliminates a logical Component from the Network Data File.
Reset anchor blocks	Allows the Network Administrator to reinitialize a Component as if the VTAM Address Space or virtual machine was completely restarted.
Rule processing	Provides entry to the Network Center's Rule processes and definition procedures.
Storage usage	Displays the internal storage allocations made by the Network Center to support the domain.
Status output log	Identifies current TNCLOGn file (if BSAM LOG support is active).
Swap output log	Allows the Network Administrator to manually switch from one TNCLOGn file to the next logical file.

Rule Processing

Many Network Center and Component actions are based on **Rules** that you can interactively define, activate, and maintain. For example, you can

- Define **Access** Component Rules that allow or deny session access
- Define **Alias** Component Rules that translate cross-network resource names to local domain aliases
- Define **Select** Component Rules that determine a session's logical communication path
- Define **Timeout** Rules that timeout inactive devices
- Define **Center** Rules that control user access to the Network Center.

Note: The Query Component does not operate based on user defined Rules. For more information, see "Query" on page 46

You define and activate Rules using the particular Component's Rule Administration panels. Each Rule allows you to apply specific criteria, which may include the Network id, Subarea, OLU name (SLU), DLU name (PLU), Time of day, Day of week, SSCPname, and/or the Network Alias name for one or both of the session partners. As a result, it is possible to configure each Component to apply different conditions to any definable portion of your network.

For example, the following Access Rule would allow sessions to establish that are initiated by the LOGAPPL specification in VTAMLST:

```

-----
TNCRULD                      Network Center Rule Definition                      ACCESS
Date: 01/15/2007             Time: 17:04:08                      User: EXAMPLE                      Version: 2.0.0

Name . . . . LOGAPPL_                      Title Allow_any_device_to_LOGAPPL_
Count . . . .
Action . . . . Allow_____ . . Alias . * _____
Date .first * _____ . . Aliasnet * _____
. . . . last * _____ . . Hcvname. * _____
Day . . . . * _____ . . Hcvtype. 0_
Dlu (Plu) . * _____ . . Netid . * _____
. . Adjsscp * _____ . . Sscp . . * _____
. . Alias . * _____ . . Subarea. * _____
. . Aliasnet * _____ . . IP data. No_
. . Hcvname. * _____ Option . . . None_____
. . Hcvtype. 0_ Rule type . Slu-Plu
. . Netid . * _____ Ruleset . . No_
. . Sscp . . * _____ Time. .first * _____
. . Subarea. * _____ . . . . last * _____
From . . . . * _____ Session type Autologon__
Mode . . . . Active_
Olu (Slu) . * _____
. . Adjsscp * _____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete
-----

```

Figure 14. LOGAPPL Rule Definition Panel

You can use the following techniques to define Rules quickly and to place them in an efficient processing order:

- Pattern Matching
- Rule Groups and Rulesets
- Value Groups

The remainder of this section briefly describes these techniques.

Pattern Matching

When defining a Rule, Ruleset, Group, or Value Group, you can set many of the operands to identify a specific value, a range of values, or all values using pattern matching masks. This allows you to include or exclude almost any value when desired, permitting you to create simple but powerful Rules.

The Network Center supports the following the pattern matching characters:

Character Meaning	
*	The asterisk represents any number of characters from none to the maximum number of characters in the operand or field. For example, the mask "*" would match any alphanumeric value. Likewise, the mask "NY*" would match any alphanumeric value starting with "NY".
%	The percent sign represents a single character of any value at the position that the percent sign is placed. You can use as many percent signs as necessary within the operand. For example, the mask "NY%%1" would match any value from NY0001 to NY9991.

Figure 15. Pattern Matching Characters

Note: See the *Installations and Operations* guide (TNC-0003) for more information.

Rule Groups and Rulesets

You can create Rule Groups using the Group Definition panel, shown below:

TNCGRPD	Group Definition	ACCESS
Date: 08/08/05	Time: 11:43:30	User: EXAMPLE
		Version: 2.0.0

Type the desired values in the listed entry fields. Then Enter.

Name	_____	Title _____
1.	_____	31. _____
2.	_____	32. _____
3.	_____	33. _____
4.	_____	34. _____
5.	_____	35. _____
6.	_____	36. _____
7.	_____	37. _____
8.	_____	38. _____
9.	_____	39. _____
10.	_____	40. _____
11.	_____	41. _____
12.	_____	42. _____
13.	_____	43. _____
14.	_____	44. _____
15.	_____	45. _____
16.	_____	46. _____
17.	_____	47. _____
18.	_____	48. _____
19.	_____	49. _____
20.	_____	50. _____
21.	_____	51. _____
22.	_____	52. _____
23.	_____	53. _____
24.	_____	54. _____
25.	_____	55. _____
26.	_____	56. _____
27.	_____	57. _____
28.	_____	58. _____
29.	_____	59. _____
30.	_____	60. _____

Enter F1=Help F3=Exit F7=Bkwd F8=Fwd F11=Select F16=Save F20=Delete

Figure 16. Group Definition Panel

Rule Groups allow you to place any variety of Rules, Rulesets, or other Groups into a particular processing order. You can interactively activate and deactivate the Groups as required by your installation.

You can also group Rules together into a Ruleset, which is a Rule that acts as a "gate" for other Rules. If a particular session's criterion does not match the Ruleset Rule, the Rules it contains will not be processed. This conditional testing allows you to define Rules into a simple structure that reduces CPU consumption. Rulesets are available by marking "yes" in the Ruleset field of a Rule definition panel and appear as follows:

TNCRNAM	Ruleset Rule Name List			ACCESS
Date: 01/15/2007	Time: 17:51:24	User: EXAMPLE	Version: 2.0.0	
1. _____	20. _____	39. _____	58. _____	
2. _____	21. _____	40. _____	59. _____	
3. _____	22. _____	41. _____	60. _____	
4. _____	23. _____	42. _____	61. _____	
5. _____	24. _____	43. _____	62. _____	
6. _____	25. _____	44. _____	63. _____	
7. _____	26. _____	45. _____	64. _____	
8. _____	27. _____	46. _____	65. _____	
9. _____	28. _____	47. _____	66. _____	
10. _____	29. _____	48. _____	67. _____	
11. _____	30. _____	49. _____	68. _____	
12. _____	31. _____	50. _____	69. _____	
13. _____	32. _____	51. _____	70. _____	
14. _____	33. _____	52. _____	71. _____	
15. _____	34. _____	53. _____	72. _____	
16. _____	35. _____	54. _____	73. _____	
17. _____	36. _____	55. _____	74. _____	
18. _____	37. _____	56. _____	75. _____	
19. _____	38. _____	57. _____	76. _____	

Enter F1=Help F3=Exit F7=Bkwd F8=Fwd F11=Select F16=Save F20=Delete				

Figure 17. Ruleset Rule Panel

Note: For more information on Groups and Rulesets, see the Network Center guide for the Component(s) installed at your installation.

Value Groups

At times, pattern matching may not suffice for masking diverse values for a specific operand. In these situations, you can usually define the values within a special Group called a **Value Group**. You can define the Value Group using a Group Definition panel (see Figure 16 on page 26 for an example).

To identify the Group as a Value Group, simply type an ampersand (&) at the beginning of the Group's name. Then, fill in the blanks with the appropriate values, which can consist of pattern matched strings, other Value Groups, or literal values.

The Value Groups can then be referenced from a Rule, Group, or Value Group in the same manner as literal and pattern matched operand values.

Note: For more information on Value Groups, see the Network Center guide for the Component(s) installed at your installation.

Activity Logging

The Network Center maintains a log of all activity within standard operating facilities. All Component activities are maintained in a standard listing file (z/OS SYSOUT, z/VM virtual printer, or multiple disk based files) in a single location.

File Access

The Network Center provides disk file storage for all Component based information via a unique "relative record" internal indexing mechanism called the Network Data File. You can physically access the file using BSAM access routines.

Accounting Facility

You can log activities undertaken by the Network Center and its Components via z/OS SMF or z/VM ACCOUNT records. Accounting provides a standardized audit trail and historical reference point for activities occurring within the network.

The Network Center Components

Each Network Center Component performs a unique VTAM management, manipulation, or security function and can be used alone or together for improved network control. This chapter provides a brief overview of each Component:

- "Access" on page 30
- "Alias" on page 40
- "Query" on page 46
- "Select" on page 50
- "Timeout" on page 56

Access

Many SNA networks are interconnected and Internet accessible. If the local domain does not have absolute control over session establishment, any cross-system user can access the host applications, leading to costly security violations.

The Access Component logically resides in VTAM and empowers you to control which LUs may go into session with another LU within a local VTAM domain, as demonstrated in the following figure:

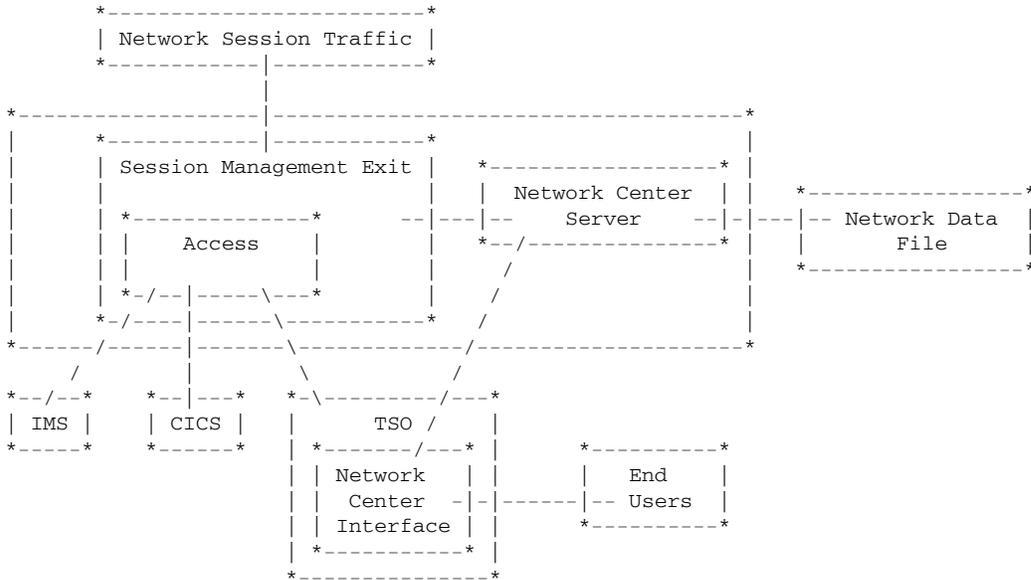


Figure 18. Access Overview

This architecture makes Access particularly beneficial to cross-domain or cross-network (SNI) configurations with remote domains that are not acceptably secured.

You can define session Rules during VTAM initialization or interactively after initialization. By combining multiple session conditions, you can approve or reject particular sessions under particular circumstances.

Rule conditions can include parameters like LU name, time of day, day of week, originating node (subarea and/or netid), subsystem being requested, etc. For example, you can specify that devices from a particular subarea may only use specific subsystems during certain times of the day.

While Access operates, it produces messages that indicate which sessions are being accepted, conditionally accepted, or rejected into a standard Network Center LOG. You can also use the Network Center's standard Accounting mechanism to record session information. You can view recent LOG information online using the Message Queue.

Session Characteristics

As VTAM processes each session, Access receives control and obtains the following characteristics that describes the session partners:¹

Adjsscp	Identifies the name of the SSCP adjacent to the current node in the direction of the requesting LU (normally, the SLU)
Alias	Identifies the LU's alias, if alias assignment has been made.
Aliasnet	Identifies the Network id where the LU's ALIAS is known.
Day	Identifies the day(s) of the week the Rule will be effective. Ranges and groupings of days are valid.
Date	Identifies the calendar date range that the Rule will be effective.
Dlu	Identifies the destination logical unit (DLU), which is typically the requested application or PLU.
From	Identifies the PLU (for instance, a controlling application) initiating the session.
Hcvname	Identifies the name of the major or minor node within VTAMLST that defines the LU.
Hcvtype	Establishes the type of major or minor node for the LU that is acceptable.
IP data	Identifies the IP data address, and/or Port Number, and/or DNS name of the Olu(Slu) associated with the session.
Netid	Identifies the home network of the LU.
Olu	Identifies the originating logical unit (typically the terminal or SLU).
Rule type	Establishes the type of Rule matching that will occur when the Rule is evaluated (can be set to OLU-DLU, SLU-PLU, or DUAL).
Session type	Identifies the type of session initiation, such as PLU requested, SLU requested, Autologon, Third Party, or Resource Directed Search.
Sscp	Identifies the SSCP for the domain that manages the LU.
Subarea	Identifies the subarea associated with the LU's domain.
Time	Identifies the time range that the Rule will be effective.

¹ Adjsscp, Alias, Aliasnet, Hcvname, Hcvtype, Netid, Sscp, and Subarea are collected for both the OLU (SLU) and PLU (DLU).

Rule Processing

After collecting session characteristics, Access compares them against the active Rules, which control whether the session will be approved or denied.

Access Rules are identified by **NAME** and **TITLE** and may be written to **ALLOW** or **DENY** the proposed session. Rule status may be **ACTIVE**, **DORMANT**, or **WARN**, where WARN produces an audit of Rule processing but sessions are not rejected.

For example, the following Rule, called LOCALS, allows any LU starting with "NY" and with the NETID of "NRS" to go into session with any application (any LU without this naming pattern will be rejected):

```

LOCALS      TNCRULE SLU=NY*,NETID=NRS,
            ACTION=ALLOW
  
```

The Rule Definition panel would appear as follows:

```

-----
TNCRULD          Network Center Rule Definition          ACCESS
Date: 01/15/2007    Time: 17:54:05          User: EXAMPLE          Version: 2.0.0

Name . . . . Locals__          Title Allow NY* LUs_____
Count . . . .
Action . . . . Allow_____    . . Alias . * _____
Date. .first * _____    . . Aliasnet * _____
. . . . last * _____    . . Hcvname. * _____
Day . . . . * _____    . . Hcvtype. 0_
Dlu (Plu) . * _____    . . Netid . NRS_____
. . Adjsscp * _____    . . Sscp . . * _____
. . Alias . * _____    . . Subarea. * _____
. . Aliasnet * _____    . . IP data. No_
. . Hcvname. * _____    Option . . . None_____
. . Hcvtype. 0_          Rule type . Slu-Plu
. . Netid . * _____    Ruleset . . No_          -
. . Sscp . . * _____    Time. .first * _____
. . Subarea. * _____    . . . . last * _____
From . . . . * _____    Session type * _____
Mode . . . . Active_
Olu (Slu) . NY*_____
. . Adjsscp * _____

-----
Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
  
```

Figure 19. LOCALS Rule Definition Panel

The next Rule example sets more operand restrictions: it allows any LU starting with "PAY" from subarea "3" and with an IP address pattern of "4.*.18.2%%" to establish a session with "DBDCCICS" Monday through Friday between 7:00am and 6:00pm. Access will deny any session requests from LUs that are outside of these specifications:

```

PAYDEPT  TNCRULE SLU=PAY*, SUBAREA=3, IPDATA=YES,
          PLU=DBDCCICS,
          TIME=(0700,1800), DAY=WEEKDAYS,
          ACTION=ALLOW

```

The Rule definition panel would be defined as follows:

```

-----
TNCRULD          Network Center Rule Definition          ACCESS
Date: 01/15/2007      Time: 17:57:06      User: EXAMPLE      Version: 2.0.0

Name . . . . PAYDEPT_          Title Allow_PAY*_LUs_____
Count . . . .
Action . . . . Allow_____ . . Alias . *_____
Date. .first *_____ . . Aliasnet *_____
. . . . last *_____ . . Hcvname. *_____
Day . . . . Weekday__ . . Hcvtype. 0_
Dlu (Plu) . DBDCCICS . . Netid . *_____
. . Adjsscp *_____ . . Sscp . . *_____
. . Alias . *_____ . . Subarea. 00000003
. . Aliasnet *_____ . . IP data. Yes
. . Hcvname. *_____ Option . . . None____
. . Hcvtype. 0_ Rule type . Slu-Plu
. . Netid . *_____ Ruleset . . No_ _
. . Sscp . . *_____ Time. .first 07:00
. . Subarea. *_____ . . . . last 18:00
From . . . . *_____ Session type *_____
Mode . . . . Active_
Olu (Slu) . PAY*_____
. . Adjsscp *_____

-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete
-----

```

Figure 20. PAYDEPT Rule Definition Panel

The IP Data Update panel would be defined as follows:

```

TNCRULD                Network Center Rule Definition                ACCESS
Date: 01/15/2007      Time: 17:57:06                User: EXAMPLE          Version: 2.0.0

Name . . . . PAYDEPT_                Title Allow_PAY*_LUs_____
Count . *-----*
Action . | TNCIPDT      IP Data Display/Update |
Date. .f |-----|
. . . . | Modify the following data fields. Then Enter. |
Day . . |-----|
Dlu (Plu | IP address  4.*.18.2%%_____ |
. . Adjs | Port Number * _____ |
. . Alia | DNS Name . * _____ |
. . Alia |-----|
. . Hcvn |-----|
. . Hcvt | Enter F1=Help F3=Exit F12=Cancel F16=Save |
. . Neti *-----*
. . Sscp . . * _____ Time. .first 07:00
. . Subarea. * _____ . . . . last 18:00
From . . . . * _____ Session type * _____
Mode . . . . Active_
Olu (Slu) . PAY*_____
. . Adjsscp * _____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 21. PAYDEPT IP Data Update Panel

The next three Rules - LOGAPPL, TCAS, and TSO - show how you can use Access to "pass" a session's access privileges from one application to another:

```

LOGAPPL  TNCRULE PLU=DIRECTOR,
        TYPE=AUTOLOGON, ACTION=ALLOW
TCAS     TNCRULE PLU=TSO,
        TYPE=THIRD-PARTY,
        FROM=DIRECTOR
TSO      TNCRULE PLU=TSO0*,
        TYPE=THIRD-PARTY,
        FROM=TSO

```

The LOGAPPL Rule allows any LU to go into session with a controlling PLU named DIRECTOR. The Rule definition panel would be defined as follows:

```

-----
TNCRULD          Network Center Rule Definition          ACCESS
Date: 01/15/2007   Time: 18:01:27          User: EXAMPLE          Version: 2.0.0

Name . . . . LOGAPPL_                               Title Allow_access_to_Director____
Count . . . .
Action . . . . Allow____          . . Alias . * _____
Date .first * _____          . . Aliasnet * _____
. . . . last * _____          . . Hcvname. * _____
Day . . . . * _____          . . Hcvtype. 0_
Dlu (Plu) . DIRECTOR          . . Netid . * _____
. . Adjsscp * _____          . . Sscp . . * _____
. . Alias . * _____          . . Subarea. * _____
. . Aliasnet * _____          . . IP data. No_
. . Hcvname. * _____          Option . . . None____
. . Hcvtype. 0_          Rule type . Slu-Plu
. . Netid . * _____          Ruleset . . No_          -
. . Sscp . . * _____          Time .first * _____
. . Subarea. * _____          . . . . last * _____
From . . . . * _____          Session type Autologon__
Mode . . . . Active_
Olu (Slu) . * _____
. . Adjsscp * _____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete
-----

```

Figure 22. LOGAPPL Rule Definition Panel

The TCAS Rule allows the Application DIRECTOR to pass ownership of the LU to the "TCAS" application. The Rule definition panel would be defined as follows:

```

TNCRULD                               Network Center Rule Definition                               ACCESS
Date: 01/15/2007                       Time: 18:03:13                               User: EXAMPLE                               Version: 2.0.0

Name . . . . TCAS_____                Title Pass_DIRECTOR_to_TCAS_____
Count . . . .
Action . . . . Allow_____              . . Alias . *_____
Date. .first *_____                    . . Aliasnet *_____
. . . . last *_____                     . . Hcvname. *_____
Day . . . . *_____                       . . Hcvtype. 0_
Dlu (Plu) . TSO_____                     . . Netid . *_____
. . Adjsscp *_____                       . . Sscp . . *_____
. . Alias . *_____                       . . Subarea. *_____
. . Aliasnet *_____                      . . IP data. No_
. . Hcvname. *_____                      Option . . . None_____
. . Hcvtype. 0_                           Rule type . Slu-Plu
. . Netid . *_____                       Ruleset . . No_
. . Sscp . . *_____                       Time. .first *_____
. . Subarea. *_____                       . . . . last *_____
From . . . . DIRECTOR                     Session type Third-party
Mode . . . . Active_
Olu (Slu) . *_____
. . Adjsscp *_____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 23. TCAS Rule Definition Panel

The TSO Rule allows "TCAS" to pass the LU to the created TSO address space. The Rule definition panel would be defined as follows:

```

TNCRULD                               Network Center Rule Definition                               ACCESS
Date: 01/15/2007                       Time: 14:55:47                               User: EXAMPLE                               Version: 2.0.0

Name . . . . TSO_____                  Title LU_from_TCAS_to_TSO_____
Count . . . .
Action . . . . Allow_____              . . Alias . *_____
Date. .first *_____                    . . Aliasnet *_____
. . . . last *_____                     . . Hcvname. *_____
Day . . . . *_____                       . . Hcvtype. 0_
Dlu (Plu) . TSO*_____                     . . Netid . *_____
. . Adjsscp *_____                       . . Sscp . . *_____
. . Alias . *_____                       . . Subarea. *_____
. . Aliasnet *_____                      . . IP data. No_
. . Hcvname. *_____                      Option . . . None_____
. . Hcvtype. 0_                           Rule type . Slu-Plu
. . Netid . *_____                       Ruleset . . No_
. . Sscp . . *_____                       Time. .first *_____
. . Subarea. *_____                       . . . . last *_____
From . . . . TSO_____                     Session type Third-party
Mode . . . . Active_
Olu (Slu) . *_____
. . Adjsscp *_____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 24. TSO Rule Definition Panel

The next three Rules - MYSITE, OUTSIDE, and DIRECTOR - show how you can use Access Rules to control which sessions from within or outside of your network will be approved or denied. (Remember, the types of Rules and conditions you can actually set are virtually limitless):

```

MYSITE      TNCRULE SUBAREA=3,
            PLU=*,ACTION=ALLOW
OUTSIDE     TNCRULE SLU=*,
            PLU=DIRECTOR,ACTION=ALLOW
DIRECTOR    TNCRULE FROM=DIRECTOR,
            TYPE=THIRD-PARTY,ACTION=ALLOW

```

The MYSITE Rule allows any LU from subarea 3 to go into session with any application. The Rule definition panel would be defined as follows:

```

-----
TNCRULD          Network Center Rule Definition          ACCESS
Date: 01/15/2007   Time: 14:57:43   User: EXAMPLE   Version: 2.0.0

Name . . . . MYSITE__          Title Allow_LUs_from_MYSITE_____
Count . . .
Action . . . Allow_____   . . Alias . * _____
Date .first * _____   . . Aliasnet * _____
. . . . last * _____   . . Hcvname. * _____
Day . . . . * _____   . . Hcvtype. 0_
Dlu (Plu) . * _____   . . Netid . * _____
. . Adjsscp * _____   . . Sscp . . * _____
. . Alias . * _____   . . Subarea. 00000003
. . Aliasnet * _____   . . IP data. No_
. . Hcvname. * _____   Option . . . None_____
. . Hcvtype. 0_           Rule type . Slu-Plu
. . Netid . * _____   Ruleset . . No_
. . Sscp . . * _____   Time .first * _____
. . Subarea. * _____   . . . . last * _____
From . . . . * _____   Session type * _____
Mode . . . . Active_
Olu (Slu) . * _____
. . Adjsscp * _____
-----
Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
-----

```

Figure 25. MYSITE Rule Definition Panel

If the session request is not matched by the MYSITE Rule, the request is passed to the OUTSIDE Rule, which allows requesting sessions from outside of Subarea 3 with access to the DIRECTOR application, only. The Rule definition panel would be defined as follows:

```

TNCRULD                               Network Center Rule Definition                               ACCESS
Date: 01/15/2007                       Time: 15:01:01                               User: EXAMPLE                               Version: 2.0.0

Name . . . . OUTSIDE_                               Title Allow_DIRECTOR_access_only__
Count . . . .
Action . . . Allow_____ . . Alias . *_____
Date .first *_____ . . Aliasnet *_____
. . . . last *_____ . . Hcvname. *_____
Day . . . . *_____ . . Hcvtype. 0_
Dlu (Plu) . DIRECTOR . . Netid . *_____
. . Adjsscp *_____ . . Sscp . . *_____
. . Alias . *_____ . . Subarea. *_____
. . Aliasnet *_____ . . IP data. No_
. . Hcvname. *_____ Option . . . None_____
. . Hcvtype. 0_ Rule type . Slu-Plu
. . Netid . *_____ Ruleset . . No_
. . Sscp . . *_____ Time .first *_____
. . Subarea. *_____ . . . . last *_____
From . . . . *_____ Session type *_____
Mode . . . . Active_
Olu (Slu) . *_____
. . Adjsscp *_____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 26. OUTSIDE Rule Definition Panel

The DIRECTOR Rule allows the DIRECTOR application to forward the device to any application it chooses. The Rule definition panel would be defined as follows:

```

TNCRULD                      Network Center Rule Definition                      ACCESS
Date: 01/15/2007             Time: 15:02:13                      User: EXAMPLE                      Version: 2.0.0

Name . . . . DIRECTOR                      Title Allow_DIRECTOR_to_forward_LU
Count . . . .
Action . . . . Allow_____ . . Alias . *_____
Date .first *_____ . . Aliasnet *_____
. . . . last *_____ . . Hcvname. *_____
Day . . . . *_____ . . Hcvtype. 0_
Dlu (Plu) . *_____ . . Netid . *_____
. . Adjsscp *_____ . . Sscp . . *_____
. . Alias . *_____ . . Subarea. *_____
. . Aliasnet *_____ . . IP data. No_
. . Hcvname. *_____ Option . . . None_____
. . Hcvtype. 0_ Rule type . Slu-Plu
. . Netid . *_____ Ruleset . . No_
. . Sscp . . *_____ Time. .first *_____
. . Subarea. *_____ . . . . last *_____
From . . . . DIRECTOR Session type Third-party
Mode . . . . Active_
Olu (Slu) . *_____
. . Adjsscp *_____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 27. DIRECTOR Rule Definition Panel

Alias

Alias allows you to set flexible, timesaving Rules over alias name assignment in the gateway SSCP. Capabilities include:

- Dynamically assigning alias names from a "pool" (or range) of predefined aliases
- Assigning alias names from a group that contains a set of specific alias assignments
- Assigning names on a one to one basis

If no Rule exists mapping the connection, Alias allows the connection to function with the originating name.

Each time VTAM needs to obtain an Alias name for a logical unit, it travels through the Alias nucleus code residing in the Session Management Exit location. Alias then extracts the appropriate information for the connection being established, compares the information against the active Rules, and assigns an alias name, if required.

The following figure illustrates the basic Alias placement within a network:

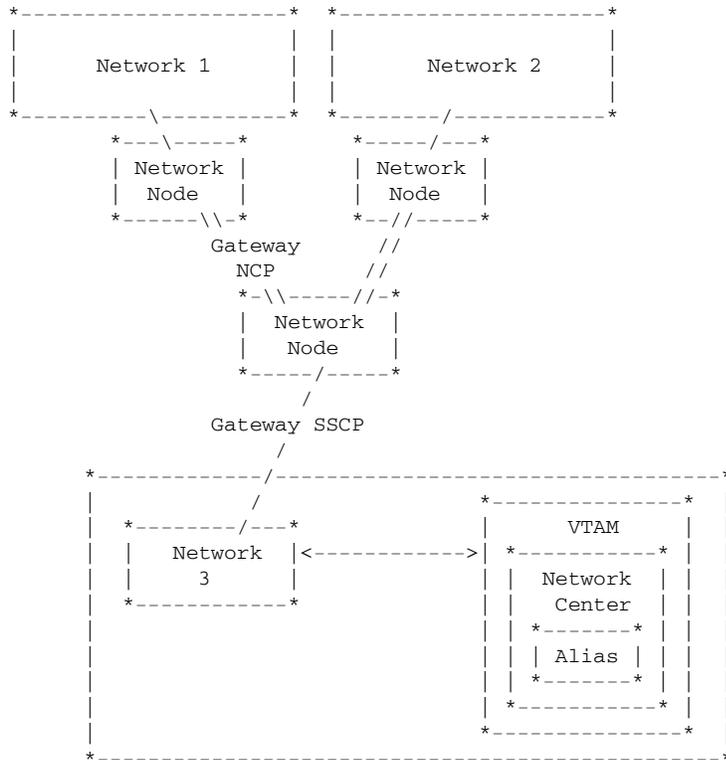


Figure 28. General Alias Network Structure

While Alias operates, it produces messages that indicate which Rules are being matched into a standard Network Center LOG. You can also use the Network Center's standard Accounting mechanism to record session information. You can view recent LOG information online using the Message Queue.

Session Characteristics

As each session is being processed by VTAM, Alias receives control and collects the following characteristics that describe the session under evaluation:²

Adjsscp	Identifies the name of the SSCP adjacent to the current node in the direction of the requesting LU (normally, the SLU).
Alias	Identifies the LU's alias, if alias assignment has been made.
Aliasnet	Identifies the Network id where the LU's ALIAS is known.
COS name	Establishes the Class of Service name to be used if a COS name translation is requested.
Day	Identifies the day(s) of the week the Rule will be effective. Ranges and groupings of days are valid.
Date	Identifies the calendar date range that the Rule will be effective.
Dlu	Identifies the destination logical unit (typically the requested application or PLU).
Dlu alias	Establishes the Alias name, Alias mask, or Alias group describing how an alias name will be returned to VTAM if a DLU name is to be translated.
From	Identifies the PLU (for instance, a controlling application) initiating the session.
Hcvname	Identifies the name of the major or minor node within VTAMLST that defines the LU.
Hcvtype	Establishes the type of major or minor node for the LU that is acceptable.
Logmode	Identifies the translated logon mode name to be used if VTAM requests a logmode name translation.
Netid	Identifies the home network of the LU.
Olu	Identifies the originating logical unit (typically the terminal or SLU).
Olu alias	Establishes the Alias name, Alias mask, or Alias group describing how an alias name will be returned to VTAM if a OLU name is to be translated.
Rule type	Establishes the type of Rule matching that will occur when the Rule is evaluated (can be set to OLU-DLU, SLU-PLU, or DUAL).
Session type	Identifies the type of session initiation, such as PLU requested, SLU requested, Autologon, Third Party, Inquire or Resource Directed Search.
Sscp	Identifies the SSCP for the domain that manages the LU.
Subarea	Identifies the subarea associated with the LU's domain.
Time	Identifies the time range that the Rule will be effective.

² Adjsscp, Alias, Aliasnet, Hcvname, Hcvtype, Netid, Sscp, and Subarea are collected for both the OLU (SLU) and PLU (DLU).

To-Network identifies the Network id of the destination network to which this alias translation request applies.

Rule Processing

As Alias collects the session characteristics, it compares them against a set of active Alias Rules. The Rules are identified by **NAME** and **TITLE** and may be written to **TRANSLATE** or **BYPASS** the supplied alias translation request. Rule status may be **ACTIVE**, **DORMANT**, or **WARN**, where **WARN** produces an audit of Rule processing, but aliases are not assigned.

In the following Alias Rules, one to one alias name translation has been defined:

```
T31001 TNCRULE SLU=T31001,OLUALIAS=OTHER01,
          NETID=OTHER,TO-NETWORK=NRS
T31002 TNCRULE SLU=T31002,OLUALIAS=OTHER02,
          NETID=OTHER,TO-NETWORK=NRS
```

Each of the preceding Rules simply translates the name of the incoming device, T31001 and T31002, from the OTHER Network to an LU name that begins with the character string "OTHER" within the local network, NRS.³ The Rule definition panel for T31001 would be defined as follows:

```
-----
TNCRUULD          Network Center Rule Definition          ALIAS
Date: 01/15/2007   Time: 15:05:54           User: EXAMPLE      Version: 2.0.0

Name . . . . T31001__          Title Translation_for_T31001_____
Count . . . .
Action . . . Translate . . Alias . *_____ To Network . *_____
Date. .first *_____ . . Aliasnet *_____ Alias translations
. . . . last *_____ . . Hcvname. *_____ Alias (DLU) _____
Day . . . . *_____ . . Hcvtype. 0_ . . . (OLU) OTHER01_
Dlu (Plu) . *_____ . . Netid . OTHER__ Netview . . No_
. . Adjsscp *_____ . . Sscp . . *_____ To COSname . *_____
. . Alias . *_____ . . Subarea. *_____ To Logmode . *_____
. . Aliasnet *_____ . . IP data. _____
. . Hcvname. *_____ Option . . . None_____
. . Hcvtype. 0_ Rule type . Slu-Plu
. . Netid . *_____ Ruleset . . No_
. . Sscp . . *_____ Time. .first *_____
. . Subarea. *_____ . . . . last *_____
From . . . . *_____ Session type *_____
Mode . . . . Active_ Alias selections
Olu (Slu) . T31001__ From COSname *_____
. . Adjsscp *_____ From Logmode *_____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete
-----
```

Figure 29. T31001 Rule Definition Panel

As you can see, one to one translation provides a simple approach to assigning alias names, but requires that you establish a Rule for every device that might contact the system.

³ The TO NETWORK operand must be specified to ensure that translation into our network (NRS) occurs properly.

Now, let's assume that you would like to define a more general Rule that would allow any device originating from the OTHER network to receive a local Alias translation.

With this Rule, any device from the OTHER network whose LU name begins with "T" will be assigned a name from an Alias Pool, which is defined by the Alias Mask 'OTHER%%': the first device from the OTHER network will be assigned the name OTHER01, the second device will be assigned the name OTHER02 up to OTHER99.

```
OTHER TNCRULE SLU=T*,NETID=OTHER,OLUALIAS=OTHER%%,TO-NETWORK=NRS
```

The OTHER Rule definition panel would be defined as follows:

```

TNCRULD                      Network Center Rule Definition                      ALIAS
Date: 01/15/2007             Time: 15:41:56                      User: EXAMPLE                Version: 2.0.0

Name . . . . OTHER_____          Title Translation_for_all_OTHER_____
Count . . .
Action . . . Translate           . . Alias . *_____          To Network . NRS_____
Date .first *_____             . . Aliasnet *_____        Alias translations
. . . . last *_____           . . Hcvname. *_____        Alias (DLU) _____
Day . . . . *_____             . . Hcvtype. 0_             . . . (OLU) OTHER%%_
Dlu (Plu) . *_____            . . Netid . OTHER_____     Netview . . No_
. . Adjsscp *_____            . . Sscp . . *_____        To COSname . *_____
. . Alias . *_____             . . Subarea. *_____        To Logmode . *_____
. . Aliasnet *_____            . . IP data. _____
. . Hcvname. *_____            Option . . . None_____
. . Hcvtype. 0_                 Rule type . Slu-Plu
. . Netid . *_____            Ruleset . . No_
. . Sscp . . *_____            Time. .first *_____
. . Subarea. *_____           . . . . last *_____
From . . . . *_____            Session type *_____
Mode . . . . Active_            Alias selections
Olu (Slu) . T*_____            From COSname *_____
. . Adjsscp *_____            From Logmode *_____
-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 30. OTHER Rule Definition Panel

You can further enhance a Rule's capabilities by using Value Groups. For example, assume that you want to allow name translation for three different networks named CREDIT, BANK, and CLIENT:

```

USERS  TNCRULE VALUES=(CREDIT,BANK,CLIENT)
NORMAL TNCRULE NETID=&USERS,TO-NETWORK=NRS,OLUALIAS=USERS%%%
```

You would first define the Network ids into a Value Group, as follows (see "Value Groups" on page 27):

```

TNCGRPD          Group Definition          ALIAS
Date: 01/15/2007  Time: 15:08:53          User: EXAMPLE    Version: 2.0.0

Type the desired values in the listed entry fields. Then Enter.

Name . . . . &USERS__          Title NETIDs_for_NORMAL_Rule_____

 1. CREDIT__          16. _____          31. _____          46. _____
 2. BANK__            17. _____          32. _____          47. _____
 3. CLIENT__          18. _____          33. _____          48. _____
 4. _____          19. _____          34. _____          49. _____
 5. _____          20. _____          35. _____          50. _____
 6. _____          21. _____          36. _____          51. _____
 7. _____          22. _____          37. _____          52. _____
 8. _____          23. _____          38. _____          53. _____
 9. _____          24. _____          39. _____          54. _____
10. _____          25. _____          40. _____          55. _____
11. _____          26. _____          41. _____          56. _____
12. _____          27. _____          42. _____          57. _____
13. _____          28. _____          43. _____          58. _____
14. _____          29. _____          44. _____          59. _____
15. _____          30. _____          45. _____          60. _____

-----
Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 31. USERS Value Group Definition Panel

The Rule Definition panel, which includes the Value Group name in the Netid field, would appear as follows:

TNCRULD	Network Center Rule Definition	ALIAS
Date: 01/15/2007	Time: 15:10:14	User: EXAMPLE
		Version: 2.0.0

Name	NORMAL__	Title Trans_for_CREDIT_BANK_CLIENT
Count		
Action	Translate	. . Alias . *
Date .first *	_____	. . Aliasnet *
. . . . last *	_____	. . Hcvname. *
Day *	_____	. . Hcvtype. 0_
Dlu (Plu) . *	_____	. . Netid . &USERS__
. . Adjsscp *	_____	. . Sscp . . *
. . Alias . *	_____	. . Subarea. *
. . Aliasnet *	_____	. . IP data. ____
. . Hcvname. *	_____	Option . . . None_____
. . Hcvtype. 0_	_____	Rule type . Slu-Plu
. . Netid . *	_____	Ruleset . . No_
. . Sscp . . *	_____	Time .first *_____
. . Subarea. *	_____ last *_____
From *	_____	Session type *_____
Mode	Active_	Alias selections
Olu (Slu) . *	_____	From COSname *_____
. . Adjsscp *	_____	From Logmode *_____

Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

Figure 32. NORMAL Rule Definition Panel

The Query Menu

The Query Menu provides the anchor point for Query requests and displays:

```
Options  Exit  Help
-----
A01TNC                                     Query Menu

Select one of the following choices by typing the number, or make a selection
by positioning the cursor at your choice. Then Enter.

___  1. Application program blocks
     2. Buffer pool directory
     3. Buffer pool start options
     4. Configuration table
     5. Resource definition table
     6. Session information blocks
     7. Symbolic resolution table
     8. System/user logmode tables
     9. Vector table
    10. Virtual route blocks
    11. Vtam start options

-----
Enter  F1=Help  F3=Exit  F10=Actions  F12=Cancel  F13=Keys  F21=Command
```

Figure 34. Query Selection List

The choices provide access to the following VTAM control blocks and related information:

Menu Choice	Available VTAM Control Block(s)
Application program blocks	ACDEB/FMCB/LUCB/MPST/PST
Buffer pool directory	BPPTY, BPENT, PXB
Buffer pool start options	SBFA
Configuration table	CONF
Resource definition table	RDT, RDTE, RAP, RCC, RCDRM, RCDRS, RCPRE, RGP, RIN, RLN, RLU, RPRE, RPU, RRN, RLS, RSW, PAB, DYPAB, NCB, LDNCB, XCNCB
Session information blocks	SIB
Symbolic resolution table	SRT
System logmode table	LOGMODE
Communications Vector Table	ATCVT
Virtual route blocks	VRBLK
Start options	Accumulated from various locations

Figure 35. Query Menu Overview

Control Block Display and Interpretation

Query requests are displayed in selection list format, simple hexadecimal storage dump, or interpreted format. Individual fields within these displays may lead to another control block or to bit settings in individual control block fields. Control block fields that contain individual bit settings may also produce extended interpretation via a pop up window.

The following example shows an unformatted (hexadecimal) dump of a Session Information Block (SIB):

TNQDUMP	A06TSO1	VTAM Storage - SIB				More:	+

SIB	Session information block						
0000	9800FC00	00000000	E85B1C91	D80684EA	q.....Y\$.jQ.d.	12F39010	
0010	40404040	40404040	C9D5E3C5	D9C1C3E3	INTERACT	12F39020	
0020	C9D5E3C5	D9C1C3E3	BCB72EF3	C3AC9400	INTERACT...3C.m.	12F39030	
0030	12F39300	00000000	00000000	00000000	.3l.....	12F39040	
0040	00000000	12F39120	12F390C0	12F340143j..3.{.3 .	12F39050	
0050	50311400	00000008	00000000	00000000	&.....	12F39060	
0060	00000000	00000000	00000000	00000000	12F39070	
0070	80000000	00000000	00000000	00000000	12F39080	
0080	00000000	00000000	00000000	00000000	12F39090	
0090	00000000	00000000	00000000	00000000	12F390A0	
00A0	00000000	00000000	00000000	00000000	12F390B0	
00B0	00000000	00000000	C1F0F6E3	E2D6F140A06TSO1	12F390C0	
00C0	D7F3F9F0	40404040	00000000	12F499D4	P3904rM	12F390D0	
00D0	00000000	00107380	68048100	00000004a.....	12F390E0	
00E0	3C000005	00000000	00000000	00000000	12F390F0	
00F0	00000000	00060139	00000000	00000000	12F39100	
0100	00000000	00000000	00000000	00000000	12F39110	
0110	00000000	00000000	C1F0F6E9	D6E24040A06ZOS	12F39120	
0120	D7F3F9F0	40404040	00000000	12F498B0	P3904q.	12F39130	

Enter	F1=Help	F3=Exit	F7=Bkwd	F8=Fwd	F11=Format	F12=Cancel	F21=Command

Figure 36. Query Hexadecimal Display

The control block can be interpreted by switching to FORMAT mode, as shown in the following figure:

```

SIBVE51M A06TSO1                Session Information Block                More:  +
-----
The highlighted values may be selected by positioning the cursor. Then Enter.

Sibcbid   : 98                      Flags      : 50
Reserved  : 00                      :          : 31
Sibfsmin  : FC                      :          : 14
Sibfsmtm  : 00                      Sibbsawc   : 00
Sibfsens  : 00000000                Sibbvrtip  : 00
Sibpcid   : E85B1C91D80684EA        Sibberfl   : 00
Sibbcosn  : *-*                     Sibbreri   : 00
Sibblgmd  : INTERACT                Flags      : 08
Sibddlmd  : INTERACT                Sibbprbq   : 00000000
Sibbtime  : BCB72EF3C3AC9400        Sibbsebq   : 00000000
Sibbfwd   : 12F39300                Reserved   : 0000000000000000
Sibbbwd   : 00000000                :          : 0000000000000000
Sibbpriq  : 00000000                :          : 8000000000000000
Sibbsecq  : 00000000                :          : 0000000000000000
Sibbiptr  : 00000000                :          : 0000000000000000
Sibbpptr  : 12F39120                Sibttmcd   : 00
Sibbsptr  : 12F390C0                Flags      : 00
Sibbfqpc  : 12F34014                Sibtsese   : 00
-----
Enter F1=Help F3=Exit F7=Bkwd F8=Fwd F11=Dump F12=Cancel F21=Command

```

Figure 37. Query Formatted Display

You can get descriptions of displayed control blocks by accessing the wide range of Query HELP panels or by referencing appropriate IBM publications including the *SNA Reference Summary*, *VTAM Diagnosis Reference*, *VTAM Programming*, and *VTAM Reference Summary* (LY30-5600).

Select

Select allows you to manipulate the contents of the following lists, which are used by VTAM during processing:

- Gateway Path
- Adjacent Link Station
- Adjacent SSCP
- Network Virtual Route

By setting Select Rules, you can dynamically prioritize, define, and monitor contacts with other domains and networks for optimal load balancing efficiency and increased control over cross-network activities.

For example, you can restrict certain cross-domain and cross-network activities, control selection of logical connection between hosts, and set and adjust processing orders.

Select operates in the following manner: Each time VTAM needs to determine if a particular List of items is appropriate, it calls the Select routine residing in the Session Management Exit (SME). Select then extracts data associated with the connection being established, compares the data against the active Rules, and assigns or manipulates a Select List, as required.

Session Characteristics

You can structure Select Rules to control a wide variety of VTAM session characteristics:⁴

Adjsscp	Identifies the name of the SSCP adjacent to the current node in the direction of the requesting LU (normally, the SLU).
Alias	Identifies the LU's alias if alias assignment has been made.
Aliasnet	Identifies the Network id where the LU's ALIAS is known.
Day	Identifies the day(s) of the week the Rule will be effective. Ranges and groupings of days are valid.
Date	Identifies the calendar date range that the Rule will be effective.
Dlu	Identifies the destination logical unit (typically the requested application or PLU).
From	Identifies the PLU (for instance, a controlling application) forwarding the session.
Hcvname	Identifies the name of the major or minor node within VTAMLST that defines the LU.
Hcvtype	Establishes the acceptable type of major or minor node for the LU.
Netid	Identifies the home network of the LU.
Olu	Identifies the originating logical unit (typically the terminal device or SLU).
Rule type	Establishes the type of Rule matching that will occur when the Rule is evaluated (can be set to OLU-DLU, SLU-PLU, or DUAL).
Select list	Identifies a list of resource names and optional weighting factors to be utilized for the Select exit point logic.
Session type	Identifies the type of session initiation, such as PLU requested, SLU requested, Autologon, Third Party, Inquire, or Resource Directed Search.
Sscp	Identifies the SSCP for the domain that manages the LU.
Subarea	Identifies the subarea associated with the domain.
Time	Identifies the time range that the Rule will be effective.

⁴ Adjsscp, Alias, Aliasnet, Hcvname, Hcvtype, Netid, Sscp, and Subarea can be specified for both the OLU (SLU) and DLU (PLU).

Rule Processing

Select Rules are identified by **NAME** and **TITLE** and may be written to **SELECT**, **REPLACE**, or **BYPASS** associated lists. Rule status may be **ACTIVE**, **DORMANT**, or **WARN**, where **WARN** produces an audit of Rule processing, but lists are not actually modified.

You can use Select to balance the workload across the desired routes. Whenever VTAM asks Select to select a route, it will evaluate the number of sessions that are in operation across the identified routes. It then chooses the route that is the farthest below the desired weighting ratio and orders the list for VTAM, placing the desired route first in the list.

For example, let's say that you wish to assign a load balancing factor to two routes, VR1TP1 and VR2TP1, within the network TODC2. You want the high speed route, VR1TP1, to receive 65% of all session traffic, and VR2TP1 to receive the remainder at 35% of session traffic. You would need to define a Select List (TWOPATHS) and a Select Rule (TODC2):

```
TWOPATHS TNCRULE LIST=(VR1TP1,65,VR2TP1,35)
TODC2 TNCRULE ACTION=SELECT,SLU=*,NETID=TODC2,SELECT=TWOPATHS
```

The Select List would appear as follows:

TNCGRPD	Select List Definition	SELECT
Date: 01/15/2007	Time: 15:25:09	User: EXAMPLE
		Version: 2.0.0

Type the desired values in the listed entry fields. Then Enter.

Name TWOPATHS	Title Select_list_for_T0DC2_____
1. VR1TP1__ 65	16. _____
2. VR2TP1__ 35	17. _____
3. _____	18. _____
4. _____	19. _____
5. _____	20. _____
6. _____	21. _____
7. _____	22. _____
8. _____	23. _____
9. _____	24. _____
10. _____	25. _____
11. _____	26. _____
12. _____	27. _____
13. _____	28. _____
14. _____	29. _____
15. _____	30. _____
	31. _____
	32. _____
	33. _____
	34. _____
	35. _____
	36. _____
	37. _____
	38. _____
	39. _____
	40. _____
	41. _____
	42. _____
	43. _____
	44. _____
	45. _____
	46. _____
	47. _____
	48. _____
	49. _____
	50. _____
	51. _____
	52. _____
	53. _____
	54. _____
	55. _____
	56. _____
	57. _____
	58. _____
	59. _____
	60. _____

Enter F1=Help F3=Exit F7=Bkwd F8=Fwd F11=Select F16=Save F20=Delete

Figure 39. TWOPATHS Select List Panel

The TODC2 Rule would appear as follows (the "Select list" field notes that the Rule relates to the "TWOPATHS" Select List):

```

TNCRULD                               Network Center Rule Definition                               SELECT
Date: 01/15/2007                       Time: 15:26:53                               User: EXAMPLE                               Version: 2.0.0

Name . . . . TODC2__                               Title Load_balance_for_TODC2_____
Count . . . .
Action . . . . Select__                               . . Alias . *_____
Date .first *_____                               . . Aliasnet *_____
. . . . last *_____                               . . Hcvname. *_____
Day . . . . *_____                               . . Hcvtype. 0_
Dlu (Plu) . *_____                               . . Netid . TODC2__
. . Adjsscp *_____                               . . Sscp . . *_____
. . Alias . *_____                               . . Subarea. *_____
. . Aliasnet *_____                               . . IP data. ____
. . Hcvname. *_____                               Option . . . None__
. . Hcvtype. 0_                               Rule type . Slu-Plu
. . Netid . *_____                               Ruleset . . No_
. . Sscp . . *_____                               Time .first *_____
. . Subarea. *_____                               . . . . last *_____
From . . . . *_____                               Session type *_____
Mode . . . . Active_                               Select processing
Olu (Slu) . *_____                               Select list TWOPATHS
. . Adjsscp *_____

-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 40. TODC2 Rule Definition Panel

Now, let's say you want to enhance the load balancing by prioritizing 90% of CICS work across the higher capacity link, VR1TP1, the remaining 10% of CICS traffic to the link VR2TP1, and all other traffic according to the TWOPATHS Rule.

You would do this by creating a Select List for the new criteria (CICSPATH) and a Rule that assigns the CICS work to the Select List (CICS). Your Rule structure would then be in the following processing order:

```

CICSPATH TNCRULE LIST=(VR1TP1,90,VR2TP1,10)
TWOPATHS TNCRULE LIST=(VR1TP1,65,VR2TP1,35)
CICS     TNCRULE ACTION=SELECT,PLU=CICS*,NETID=TODC2,SELECT=CICSPATH
TODC2   TNCRULE ACTION=SELECT,SLU=*,NETID=TODC2,SELECT=TWOPATHS

```

The CICSPATH Select List would appear as follows:

```

TNCGRPD                               Select List Definition                               SELECT
Date: 01/15/2007                       Time: 15:29:03                               User: EXAMPLE                               Version: 2.0.0

Type the desired values in the listed entry fields. Then Enter.

Name . . . . CICSPATH                               Title Select_list_for_CICSPATH_____

  1. VR1TP1__ 90      16. _____ 31. _____ 46. _____
  2. VR2TP1__ 10      17. _____ 32. _____ 47. _____
  3. _____      18. _____ 33. _____ 48. _____
  4. _____      19. _____ 34. _____ 49. _____
  5. _____      20. _____ 35. _____ 50. _____
  6. _____      21. _____ 36. _____ 51. _____
  7. _____      22. _____ 37. _____ 52. _____
  8. _____      23. _____ 38. _____ 53. _____
  9. _____      24. _____ 39. _____ 54. _____
 10. _____      25. _____ 40. _____ 55. _____
 11. _____      26. _____ 41. _____ 56. _____
 12. _____      27. _____ 42. _____ 57. _____
 13. _____      28. _____ 43. _____ 58. _____
 14. _____      29. _____ 44. _____ 59. _____
 15. _____      30. _____ 45. _____ 60. _____

-----
Enter F1=Help F3=Exit F7=Bkwd F8=Fwd F11=Select F16=Save F20=Delete

```

Figure 41. CICSPATH Select List Panel

The CICS Rule would appear as follows:

```

TNCRULD                               Network Center Rule Definition                               SELECT
Date: 01/15/2007                       Time: 15:30:40                               User: EXAMPLE                               Version: 2.0.0

Name . . . . CICS_____                               Title Load_balancing_for_CICS_____
Count . . .
Action . . . Select_____
Date .first *_____ . . Alias . *_____
. . . . last *_____ . . Aliasnet *_____
Day . . . . *_____ . . Hcvname. *_____
Dlu (Plu) . CICS*_____ . . Hcvtype. 0_
. . Adjsscp *_____ . . Netid . *_____
. . Alias . *_____ . . Sscp . . *_____
. . Aliasnet *_____ . . Subarea. *_____
. . Hcvname. *_____ . . IP data. _____
. . Hcvtype. 0_ Option . . . None_____
. . Netid . TODC2_____ Rule type . Slu-Plu
. . Sscp . . *_____ Ruleset . . No_
. . Subarea. *_____ Time .first *_____
From . . . . *_____ . . . . last *_____
Mode . . . . Active_ Session type *_____
Olu (Slu) . *_____ Select processing
. . Adjsscp *_____ Select list CICSPATH

-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 42. CICS Rule Definition Panel

For more information on setting the Rule processing order or on Select in general, see the *Select* guide.

Session Characteristics

You can set Timeout Rules to disconnect LUs based on the following session characteristics:⁵

Adjsscp	Identifies the name of the SSCP adjacent to the current node in the direction of the requesting LU (normally, the SLU).
Alias	Identifies the LU's alias if alias assignment has been made.
Aliasnet	Identifies the Network id where the LU's ALIAS is known.
Connect time	Establishes the maximum interval that the session may last. Any session exceeding this value will be terminated.
Day	Identifies the day(s) of the week the Rule will be effective. Ranges and groupings of days are valid.
Date	Identifies the calendar date range that the Rule will be effective.
Dlu	Identifies the destination logical unit (typically the requested application or PLU).
From	Identifies the PLU (for instance, a controlling application) forwarding the session.
Hcvname	Identifies the name of the major or minor node within VTAMLST that defines the LU.
Hcvtype	Establishes the acceptable type of major or minor node for the LU.
Hours	Establishes the time of day that a session can continue. Timeout will terminate sessions Sessions that exist outside of this interval.
Inactivity	Establishes an acceptable idle interval. Inactive intervals greater than this value will have their session terminated.
IP data	Identifies the IP data address, and/or Port Number, and/or DNS name of the Olu(Slu) associated with the session.
Netid	Identifies the home network of the LU.
Olu	Identifies the originating logical unit (typically the terminal device or SLU).
Rule type	Establishes the type of Rule matching that will occur when the Rule is evaluated (can be set to OLU-DLU, SLU-PLU, or DUAL).
Session type	Identifies the type of session initiation, such as PLU requested, SLU requested, Autologon, Third Party, or Resource Directed Search.
Sscp	Identifies the SSCP for the domain that manages the LU.
Subarea	Identifies the subarea associated with the domain.
Time	Identifies the time range that the Rule will be effective.

⁵ Adjsscp, Alias, Aliasnet, Hcvname, Hcvtype, Netid, Sscp, and Subarea can be specified for both the OLU (SLU) and DLU (PLU).

Rule Processing

Timeout Rules are identified by **NAME** and **TITLE**. Rule status may be **ACTIVE**, **DORMANT**, or **WARN**, where **WARN** produces an audit of Rule processing but sessions are not actually terminated.

For example, the following Rule establishes a five minute idle session time interval for any LU starting with the letters "NY" in the NRS network that has an IP address of "4.*.18.2%% ". If the idle interval exceeds 5 minutes, the session will be terminated:

```

LOCALS      TNCRULE SLU=NY*,NETID=NRS,IPDATA=YES
            INACTIVITY=5M
  
```

The Rule definition panel would appear as follows:

```

-----
TNCRULD      Network Center Rule Definition      TIMEOUT
Date: 01/15/2007      Time: 15:32:33      User: EXAMPLE      Version: 2.0.0

Name . . . . LOCALS__      Title Timeout_for_NY_____
Count . . . .
Action . . . Monitor__      . . Alias . * _____      Hour. .first * _____
Date. .first * _____      . . Aliasnet * _____      . . . . last * _____
. . . . last * _____      . . Hcvname. * _____      Inactivity . 5M_____
Day . . . . * _____      . . Hcvtype. 0_      Period start * _____
Dlu (Plu) . * _____      . . Netid . * _____      . . . . end * _____
. . Adjsscp * _____      . . Sscp . . * _____      Weekday . . * _____
. . Alias . * _____      . . Subarea. 00000003
. . Aliasnet * _____      . . IP data. Yes
. . Hcvname. * _____      Option . . . None_____
. . Hcvtype. 0_      Rule type . Slu-Plu
. . Netid . * _____      Ruleset . . No_
. . Sscp . . * _____      Time. .first * _____
. . Subarea. * _____      . . . . last * _____
From . . . . * _____      Session type * _____
Mode . . . . Active_      Timeout conditions
Olu (Slu) . NY*_____      Connect time 0_____
. . Adjsscp * _____      Force . . . No_

-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete
  
```

Figure 44. LOCALS Rule Definition Panel

The IP Data Update panel would appear as follows:

```

TNCRULD                      Network Center Rule Definition                      TIMEOUT
Date: 01/15/2007             Time: 15:32:33                       User: EXAMPLE                 Version: 2.0.0

Name . . . . LOCALS__          Title Timeout_for_NY_____
Count . *-----*
Action . | TNCIPDT      IP Data Display/Update | first * ____
Date. .f |-----| last * ____
. . . . | Modify the following data fields. Then Enter. | ty . 5M ____
Day . . |-----| tart * ____
Dlu (Plu | IP address 4.*.18.2%%_____ | end * ____
. . Adjs | Port Number * _____ | . . * ____
. . Alia | DNS Name . * _____ |
. . Alia |-----|
. . Hcvn |-----|
. . Hcvt | Enter F1=Help F3=Exit F12=Cancel F16=Save |
. . Neti *-----*
. . Sscp . . * _____ Time. .first * ____
. . Subarea. * _____ . . . . last * ____
From . . . . * _____ Session type * _____
Mode . . . . Active_      Timeout conditions
Olu (Slu) . NY* _____ Connect time 0 _____
. . Adjsscp * _____ Force . . . No_

-----
Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

```

Figure 45. LOCALS IP Data Update panel

You can also create Rules that set an idle time interval with a time parameter as well. For example, the PAYDEPT Rule sets a 1 minute idle interval for any LU beginning with "PAY" from SUBAREA "3" when in session with "DBDCCICS" between 7:00am and 6:00pm Monday through Friday. Any other LU's, or those LU's outside of the time and day interval will not have their sessions subject to Timeout idle time checking:

```

PAYDEPT  TNCRULE SLU=PAY*,SUBAREA=3,
          PLU=DBDCCICS,INACTIVITY=1M
          TIME=(0700,1800),DAY=WEEKDAYS,
          ACTION=MONITOR

```

The Rule definition panel would appear as follows:

TNCRULD	Network Center Rule Definition		TIMEOUT
Date: 01/15/2007	Time: 15:35:39	User: EXAMPLE	Version: 2.0.0
Name PAYDEPT_	Title TIMEOUT_for_PAY_____		
Count			
Action Monitor__	. . Alias . . *_____	Hour. .first 07:00	
Date. .first *_____	. . Aliasnet *_____ last 18:00	
. . . . last *_____	. . Hcvname. *_____	Inactivity . 1M_____	
Day Weekday__	. . Hcvtype. 0_	Period start *_____	
Dlu (Plu) . DBDCCICS	. . Netid . *_____ end *_____	
. . Adjsscp *_____	. . Sscp . . *_____	Weekday . . *_____	
. . Alias . *_____	. . Subarea. 00000003		
. . Aliasnet *_____	. . IP data. No_		
. . Hcvname. *_____	Option . . . None_____		
. . Hcvtype. 0_	Rule type . Slu-Plu		
. . Netid . *_____	Ruleset . . No_		
. . Sscp . . *_____	Time. .first *_____		
. . Subarea. *_____ last *_____		
From *_____	Session type *_____		
Mode Active_	Timeout conditions		
Olu (Slu) . PAY*_____	Connect time 0_____		
. . Adjsscp *_____	Force . . . No_		

Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete			

Figure 46. PAYDEPT Rule Definition Panel

As another example, the following Rule would terminate any session initiated by LU devices starting with "DIAL" outside of an 8 am to 5 pm time range; any session that establishes within the defined HOURS will be subject to a 30-minute inactivity timer:

DAYS	TNCRULE SLU=DIAL*, ACTION=MONITOR,
	HOURS=(0800,1700), INACTIVITY=30M

The Rule definition panel would appear as follows:

TNCRULD	Network Center Rule Definition	TIMEOUT
Date: 01/15/2007	Time: 15:37:46	User: EXAMPLE
		Version: 2.0.0

Name DAYS_____		Title Timeout_for_DIAL_____
Count		
Action Monitor__	. . Alias . *	Hour .first 08:00
Date .first *_____	. . Aliasnet *_____ last 17:00
. . . . last *_____	. . Hcvname. *_____	Inactivity . 30M_____
Day *_____	. . Hcvtype. 0_	Period start *_____
Dlu (Plu) . *_____	. . Netid . *_____ end *_____
. . Adjsscp *_____	. . Sscp . . *_____	Weekday . . *_____
. . Alias . *_____	. . Subarea. *_____	
. . Aliasnet *_____	. . IP data. No_	
. . Hcvname. *_____	Option . . . None_____	
. . Hcvtype. 0_	Rule type . Slu-Plu	
. . Netid . *_____	Ruleset . . No_	
. . Sscp . . *_____	Time .first *_____	
. . Subarea. *_____ last *_____	
From *_____	Session type *_____	
Mode Active_	Timeout conditions	
Olu (Slu) . DIAL*_____	Connect time 0_____	
. . Adjsscp *_____	Force . . . No_	

Enter F1=Help F2=Component F3=Exit F11=Select F16=Save F20=Delete

Figure 47. DAYS Rule Definition Panel

Technical Information

This chapter addresses the software and hardware technicalities of the Network Center and its Components. It also contains packaging, licensing, and ordering information. Topics include the following:

- Supported Systems
- Software Characteristics
- Packaging
- Publications
- Licensing
- Ordering Network Center Trials

Supported Systems

The Network Center supports z/OS and z/VM environments that operate VTAM 3.1.1 and subsequent releases. The following Network Center releases are operational for the listed environment:

Network Center Release	Operating System and VTAM Version (MVS, OS/390, and z/OS are interchangeable terms as are VM and z/VM. The VTAM version is noted in parenthesis.)
1.7.5	MVS(3.1.1), MVS(3.2), MVS(3.4.0), MVS(3.4.1), MVS(4.1), MVS(4.2), MVS(4.3), VM(3.4), VM(4.2), OS390(4.4), OS390(4.5)
1.8.2	MVS(3.1.1), MVS(3.2), MVS(3.4.0), MVS(3.4.1), MVS(4.1), MVS(4.2), MVS(4.3), VM(3.4), VM(4.2), OS390(4.4), OS390(4.5), OS390(4.6), OS390(4.7), OS390(4.8)
2.0.0	MVS(3.1.1), MVS(3.2), MVS(3.4.0), MVS(3.4.1), MVS(4.1), MVS(4.2), MVS(4.3), VM(3.4), VM(4.2), OS390(4.4), OS390(4.5), OS390(4.6), OS390(4.7), OS390(4.8), z/VM(4.2), z/OS(5.1), z/OS(6.1)

Figure 48. Supported Systems

Software Characteristics

The following technical characteristics apply to all Network Center routines and Components.

- All routines are fully re-entrant z/Series Assembler code.
- The Network Center is fully compatible with all software products that are generally available within SNA networks.
- Defined subsystem interfaces are strictly adhered to.
- The Network Center provides support for z/OS and z/VM operating systems and provides teleprocessing system support within CMS and TSO.
- SNA and VTAM native terms can be used interchangeably.
- Assembly of routines is generally not required at installation.
- The Network Center does not provide SVCs or operating system service routines that require a nucleus generation or IPL.
- The Network Center complies with Systems Application Architecture (SAA) and Common User Access (CUA) concepts.
- The Network Center supports VTAM Version 3.1.1 and up; VM/SP Release 5.0, VM/XA, VM/ESA, z/VM and up; and all IBM supported releases of MVS/SP, MVS/XA, MVS/ESA, OS/390, and z/OS.
- The Network Center operates in 24-bit PSW mode or 31-bit mode.
- The Network Center can use OS Dynamic Allocation to eliminate VTAM JCL changes, if desired.
- Working set requirements for the Network Center Interface and Network Center Server routines relate directly to the installed Components and the issued operational requests. CPU overhead remains minimal until a request is issued, at which point it becomes a function of the Component and the requested function.

Packaging

The Network Center is distributed on magnetic tape media or via the Internet. You can request the desired media using the *Product Order* form or the *Trial Agreement* form. Other distribution media and formats are available by request.

z/OS Systems

z/OS installations utilize two z/OS Partitioned Data Sets (PDS). The datasets contain:

Contents	Purpose
DATA	a Partitioned Data Set containing miscellaneous 80 character members that contain miscellaneous source code, sample JCL, and other support items
LOAD	a Partitioned Data Set containing the executable and link-edited modules that make up The Network Center and the Components ordered by your installation

Figure 49. z/OS Distribution Files

z/VM Systems

z/VM operating systems support consists of a single CMS Mini-disk (tape media file 3 in VMFPLC2 format). The z/VM distribution files include:

Contents	Purpose
Product Files	TEXT, MODULE, LOADLIBs, EXECs, and other miscellaneous files necessary to support The Network Center in VM environments

Figure 50. z/VM Distribution Files

Publications

The Network Center's documentation library contains a set of standard manuals (the "base set") and individual manuals for each Component. The documentation is available in hardcopy (paper), Acrobat Reader (PDF), or Softcopy Reader - BookManager/READ format (see www.north-ridge.com).

Base Set

The base manual set provides general information on The Network Center, including Component installation. It includes the following publications:

- General Information, TNC-0001
- User's Guide, TNC-0002
- Installation & Operations, TNC-0003
- Query, TNC-0006

The base manuals should be available to any processor operating the Network Center Server or one or more implementations of the Network Center Interface.

Optional Components

The Optional Component manuals provide detailed information on utilizing each Component and are distributed to clients according to Component licensing. Optional publications include the following:

- Access, TNC-0005
- Timeout, TNC-0007
- Alias, TNC-0027
- Select, TNC-0039

Licensing

The Network Center is licensed under standard NRS licensing arrangements. Each Network Center Server with associated Components and each Network Center Interface is licensed for use on an individual CPU under one of two basic arrangements:

Enterprise Licenses are available in increments of 3 or 5, which may be moved freely about a business operation and may operate on any processor without regard for hardware capacity.

Tiered Licenses are provided for each processor that will operate the software. The license fee is established based upon the relative size of the machine.

License fees are related to the number of licenses, number of Components, and CPU model of the licensed processor. DSLO and Volume Discounts may apply for Tiered Licenses.

Rental and lease purchase options are also available. Contact NRS for additional information (see "Copyright" on page ii for the NRS address, phone number, etc.).

Ordering Network Center Trials

North Ridge Software, Inc. offers free trial periods for The Network Center and each Component. Simply complete a NRS *Trial Agreement* ("Appendix A. Network Center Trial Agreement" on page 69) and mail or FAX it to NRS to initiate a trial. Be sure to specify your Operating System and VTAM Version and the Components that you are interested in trying.

Appendix A. Network Center Trial Agreement

This Trial Agreement is entered into on the _____ day of _____, _____, by North Ridge Software, Inc. and the Client identified as follows:

Name	
Title	
Organization/Company	
Street Address	
Department or Mail Stop	
City, State/Province	
Zip/Postal Code, Country	
Phone, FAX	
Signature	

North Ridge Software, Inc. hereby grants a revocable license to the Client to utilize the current release of **The Network Center** on the computer system at the location listed above for a Trial Period of thirty (30) days beginning _____, _____. No license fee is due from the Client for this license.

This license is granted for the sole and specific purpose of evaluating the capability of The Network Center to meet the Client's requirements. No other use shall be made of The Network Center. The Client hereby agrees to return all manuals, documents, and software related to The Network Center to North Ridge Software, Inc. and delete all copies of The Network Center from Client's systems and backups **or** to negotiate a License Agreement by the end of the Trial Period. This license shall automatically be revoked on the last day of the Trial Period without further notice to the Client.

The Client recognizes that **The Network Center** is proprietary to North Ridge Software, Inc. The Client agrees not to use, copy, modify, or transfer The Network Center or any copy, modification, or merged portion, in whole or in part, except as expressly provided for in this Trial Agreement without the express written consent of North Ridge Software, Inc.

North Ridge Software, Inc. makes no warranties, express or implied, related to The Network Center. In no event will North Ridge Software, Inc. be liable to the Client for any damages, including any lost profits, lost savings or other incidental or consequential damages arising from the use of The Network Center during the Trial Period.

| Return this completed Trial Agreement to NRS via the U.S. Mail or FAX (numbers listed under
| "Copyright" on page ii). The trial package will be returned via standard shipping channels to the
address you have listed.

You can also request trial materials via Email (sales@north-ridge.com) or via the Trial Agreement on the NRS website (www.north-ridge.com).

Glossary

The following definitions are intended to aid the reader in clarifying terminology as it is used in this publication and in regards to the Network Center suite of software Components. Some definitions are based on descriptions and entries in *Common User Access Panel Design and User Interaction*, IBM publication SC26-4351.

Access: A Network Center Component that allows authorized users to control and monitor session establishment and denial within a VTAM domain.

Account: A VM facility available from CP DIAGNOSE that allows a virtual machine to record statistical and accounting data for future processing.

action bar: In CUA terminology, the area at the top of a panel that displays the currently available keyword actions.

Adjacent Link Station (ALS): A link station partner in an adjacent node.

Adjacent SSCP: A System Service Control Point (SSCP) that VTAM can be in session with or that VTAM can use to reach destination SSCPs in the same or in other networks.

advanced program to program communication (APPC): The general facility characterizing the LU 6.2 architecture and its various implementations in products.

Alias: A Network Center Component that provides resource name assignment from within the VTAM session management exit (SME).

alias name: A name used within a local host to identify a logical unit (etc.) in another

network, guaranteeing that values remain unique amongst network nodes.

APPC: See *advanced program to program communications*.

central processing unit (CPU): The part of a host that, under the control of an operating system, executes instructions to perform a designated function.

CICS: See *Customer Information Control System*.

CMS: See *conversational monitor system*.

Common User Access (CUA) architecture: IBM guidelines for the dialog between an end user and a computing system. CUA is based from Systems Application Architecture (SAA).

Component: An individual facility within the Network Center product suite. For example, Access, Alias, Query, Select, and Timeout are all Network Center Components.

conversational monitor system (CMS): The portion of the virtual machine (VM) operating system that provides general interactive time sharing capabilities.

CPU: See *central processing unit*.

cross-domain: An action or activity that occurs between more than one domain. For example, in a cross-domain session, different VTAM domains own the PLU and SLU.

cross-network: An action or activity that occurs between two or more SNA networks. For example, in a cross-network session different SNA networks own the PLU and SLU.

CUA: see *Common User Access*.

Customer Information Control System (CICS): A widely used IBM subsystem, which provides online transaction processing services and application management.

destination logical unit (DLU): A logical unit that is the target of a session initiation request. Normally, the DLU is an application subsystem residing in a host. See also *primary logical unit* and *origin logical unit*.

device: A mechanical, electrical, or electronic contrivance with a specific purpose.

DLU: See *destination logical unit*.

domain: The part of a network where the data processing resources (hardware and software) are under the common control of VTAM.

element: In SNA, the particular resource within a subarea that is identified by an element address.

entry field: In CUA, a designated area on the panel into which a user types or places text information or field values.

ESA: Extended Systems Architecture. An advancement in the extended architecture (XA) support for operating systems that extends addressability for system, subsystem, and application functions.

extended architecture (XA): Denotes that the underlying address range of the CPU is built around a 31 bit address instead of a 24 bit address.

field: An identifiable area in a window, e.g., an *entry field* or a *selection field*.

function key area: The area at the bottom of a Network Center panel that displays function key assignments. To aid users, the most commonly used of the currently available function keys are displayed for each particular panel.

gateway: The combination of machines and programs that provide address translation, name translation, and SSCP rerouting between independent SNA networks.

GCS: See *group control system*.

Group: A defined collection of Rules, Rulesets, and/or other Groups that controls how a particular Network Center resource or Component should operate.

group control system (GCS): A component of VM that provides multiprogramming and shared memory support to virtual machines in the execution of VTAM.

host: A computer, such as a mainframe, that provides centralized control of the network.

IMS: See *Information Management System*.

Information Management System (IMS): A data/database communication system that can manage complex databases and networks.

initial program load (IPL): 1.) The process of loading system programs and preparing VTAM to run jobs. 2.) The initialization procedure that causes an operating system to commence operation.

Internet Protocol (IP): In the Internet suite of protocols, a connectionless protocol that routes data through a network or interconnected networks and acts as an intermediary between the higher protocol layers and the physical network.

inter user communication vehicle (IUCV): A VM facility that provides communication between virtual machines and VM components.

IP: See *Internet Protocol*

IPL: See *initial program load*.

ISTEXCAA: See *session management exit*.

IUCV: See *inter user communication vehicle*.

logical unit (LU): An end point (e.g. a terminal or program) in an SNA session. LUs are a type of network accessible unit that enable users to gain access to network resources and to communicate with each other.

LU: See *logical unit*.

major node: In VTAM, a set of resources that can be activated or deactivated as a group. See also *minor node*.

Message Queue: A Network Center facility that allows the Network Administrator to display messages issued during execution by the Network Center Components, the Network Center Server, and VTAM.

minor node: In VTAM, a uniquely defined resource within a major node.

MVS: Multiple Virtual Storage. A variation of IBM's OS operating system, which includes MVS/390, MVS/XA, MVS/ESA, and the MVS element of OS/390.

NCP: See *Network Control Program*.

NETID: Network id or network identifier. A 1- to 8-byte name that identifies one or more domains operating as a single SNA network.

Netview: A Tivoli product (originally introduced by IBM) that provides VTAM based network management.

network: The combination of hardware, software, and interconnection techniques that allow people to access information stored on one or more CPUs.

Network Center: North Ridge Software's suite of software components that provide increased control over the VTAM network activities.

Network Center Interface: The portion of the Network Center that executes in the host subsystem to manage communication between a Network Center workstation, the end user, and the Network Center Server

Network Center Server: The portion of the Network Center that executes within the VTAM address space or virtual machine and services requests that originate from the network or the Network Center Interface.

Network Control Program (NCP): An IBM program that provides communication controller support for single domain, multiple domain, and interconnected network capability.

Network Data File: The information stored on disk that supports installed Network Center Components. The Network Center uses the BSAM access method to access the information.

Network id: See *NETID*.

network identifier: See *NETID*.

node: An endpoint of a link common to two or more links in a network. Nodes can be processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities.

OLU: See *origin logical unit*.

operating system: The software that manages the physical resources of the host computer (zOS, zVM, and DOS are the prevalent IBM offerings).

origin logical unit (OLU): A logical unit that is the requesting side of a session initiation sequence (e.g. a user at a terminal). See also *destination logical unit* and *secondary logical unit*.

OS: Pertaining to the IBM operating systems that include OS/390, OS/VS, OS/VS1, and z/OS.

OS/390: The IBM operating system that includes and integrates functions previously provided by many IBM software products, including the MVS operating system.

panel: In CUA, the formatted display of information that appears on a display screen.

panel body: In CUA, the portion of the panel not occupied by the action bar or function key area.

panel element: In CUA, the smallest portion of a panel (e.g. entry fields, leader dots, and panel titles).

panel id: In CUA, a panel element that displays the panel's identification in the upper left corner of the panel body.

pattern matching character: The special characters, which include the asterisk (*) or percent sign (%), that can be used to represent one or more characters in the comparison of character strings. Any character or set of characters can replace a pattern matching character.

physical unit (PU): One of three types of network addressable units (NAU): a logical

unit, a physical unit (PU), or a system services control point (SSCP).

PLU: See *primary logical unit*.

pop up window: In CUA, an additional, smaller panel that supplies information related to the currently displayed panel.

primary logical unit (PLU): In SNA, the logical unit (LU) that sends the BIND to activate a session with its partner LU. The PLU identifies one side of a session and is typically an application subsystem (e.g. the Network Center Server operates as a PLU to the Network Center Interface in TSO). Contrast with *secondary logical unit*.

PTF: Program Temporary Fix. A temporary solution of a problem diagnosed by North Ridge Software in a current unaltered release of the program.

PU: See *physical unit*.

Query: A Network Center Component that provides extensive panels for the display and diagnosis of VTAM internal operations.

request/response unit (RU): A message unit that contains control information associated with a transmission.

resource: Any VTAM network element (e.g. Logical Unit (LU), application, or device) that is managed by VTAM.

RU: See *request/response unit*.

Rule: A set of criteria that establishes the operational characteristics of a portion of the VTAM network in relation to one of the Network Center's Components.

Ruleset: A Rule that defines a set of Rules. During processing, the Component will bypass the Rules defined in the Ruleset unless the session matches the criteria defined in the Ruleset. Ruleset Rules help to decrease processing time.

SDLC: See *Synchronous Data Link Control*.

secondary logical unit (SLU): In SNA, the logical unit (LU) that contains the secondary half session of a particular LU-LU session. The SLU identifies one side of a session and

is typically a terminal device, but may also be a processing program (e.g. the Network Center Interface for TSO operates as a SLU). Contrast with *primary logical unit*.

Select: A Network Center Component that allows a local installation to control the sequence in which VTAM assigns or evaluates the usage of other network elements.

selection field: In Network Center Components, a special type of entry field that allows users to select a menu list item for display.

session: In SNA, the communications between two logical units; for example, a session exists between a terminal device and a subsystem.

session management exit (SME): An exit point within VTAM that provides the local installation with control over the actions of VTAM. This routine is also known as ISTECCA.

SLU: See *secondary logical unit*.

SME: See *session management exit*.

SMF: See *System Management Facility*.

SNA: See *Systems Network Architecture*.

SNA network interconnection (SNI): The connection, by gateways, of two or more independent SNA networks to allow communication between logical units in these networks. Each SNA network retains its independence.

SNI: See *SNA Network Interconnection*.

SSCP: See *System Services Control Point*.

subarea: Within an SNA network, the value that represents a unique processing location (host or front end processor).

subsystem: A VTAM processing APPLICATION, such as CICS, TSO, CMS, or Netview. These subordinate systems are capable of operating independently of, or asynchronously with, VTAM.

Synchronous Data Link Control (SDLC): The communications procedures, which

conform to specific industry standards, between two teleprocessing end points.

System Management Facility (SMF): An OS feature that collects and records a variety of statistical and accounting data for later processing.

System Services Control Point (SSCP): The key processing point within a VTAM domain that manages session initiation and termination.

Systems Network Architecture (SNA): The definition of work flow and corresponding work units between two end points in a teleprocessing connection.

TCAS: See *terminal control address space*.

TCU: See *transmission control unit*.

teleprocessing: In a network, the communication between two end points that allows information to be utilized across transmission connections.

terminal: A device, usually equipped with a keyboard and monitor, that allows end users to access the network and process information.

terminal control address space (TCAS): The part of TSO/VTAM that provides logon services for TSO/VTAM users.

The Network Center: See *Network Center*.

Timeout: A Network Center Component that provides a domain wide inactivity timer for idle terminal sessions. Timeout also allows for session time limits.

Time Sharing Option (TSO): A portion of the MVS operating system that provides interactive time sharing capabilities.

transmission control unit (TCU): A communication control unit whose operations are controlled solely by programmed instructions from the computing system to which the unit is attached. No program is stored or executed in the unit. Examples are the IBM 2702 and 2703 Transmission Controls.

TSO: See *Time Sharing Option*.

user: Any person who may issue or receive commands and messages to or from the information or terminal processing system.

Value Group: In the Network Center, a collection of values that are referenced from an operand as a single entity. For example, users simplify Rule definition by creating one symbolic value that references a group of values.

virtual machine (VM): 1.) An IBM operating system that provides time sharing type services. 2.) A virtual data processing system that appears to be at the exclusive disposal of any particular end user, but the functions are actually accomplished by sharing the resources of an actual data processing system.

Virtual Telecommunications Access Method (VTAM): An IBM software product that provides network support services to the operating system, including controlling communication and the flow of data in an SNA network. VTAM provides the SNA application programming interfaces and SNA networking functions.

Note: Beginning with Release 5 of the OS/390 operating system, the VTAM for MVS/ESA function was included in Communications Server for OS/390. Subsequently, in z/OS VTAM was included in the z/OS Communications Server.

VM: See *virtual machine*.

VTAM: *Virtual Telecommunications Access Method*.

window: In CUA, an area of the terminal screen with visible boundaries that displays a panel or a portion of a panel.

workstation: A terminal that is connected to a mainframe at which a user can perform applications.

XA: See *extended architecture*.

z/OS: An IBM mainframe operating system that provides extended services to meet the demands of enterprise businesses using open software technologies, including distributed IP networking. z/OS includes and integrates

functions previously provided by other IBM products including MVS operating systems.

z/VM: IBM's VM operating system that is based on 64-bit architecture and that provides

extended services to meet the demands of enterprise businesses desiring a broad support for operating system environments including z/OS, OS/390, TPF, VS/ESA, CMS, and Linux.

Index

A

Access 30
 defined 71
Access Rules 32
ACCOUNT
 defined 71
ACDEBS 47
action bar 20
 defined 71
ADD 21
Adjacent Link Station 50
 defined 71
Adjacent SSCP 50
 defined 71
Adjsscp 31, 41, 52, 57
administrative issues 63
advanced program to program communication
 defined 71
Alias 31, 40, 41, 52, 57
 defined 71
alias name
 defined 71
Alias Rules 42
Aliasnet 31, 41, 52, 57
APPC
 defined 71
Application program blocks 47
Applied PTFs 23
ATCVT 47
AUTHORIZATION 21, 23

B

base manual set 66
base manuals 66
BPDTY 47
BSAM 21
Buffer pool directory 47

Buffer pool start options 47

C

Center options 23
central processing unit
 defined 71
CICS 4
 defined 71
CLEAR 21
Close TNCLOG 23
CMS 4
 defined 71
Common User Access 20
Common User Access (CUA) architecture
 defined 71
communication paths 9
Communications Vector Table 47
Component
 defined 71
Configuration table 47
CONFT 47
Connect 57
CONSOLE 21
control block display 48
conversational monitoring system (CMS)
 defined 71
COS name 41
CPU
 defined 71
cross-domain
 defined 71
cross-network
 defined 71
CUA 20
 defined 71
Customer Information Control System (CICS)
 defined 72

D

DASD 4
Date 31, 41, 52, 57
Day 31, 41, 52, 57
DELETE 21
destination logical unit (DLU)
 defined 72
device
 defined 72
dial up 4
DISPLAY 46
displaying control blocks 48
Dlu 31, 41, 52, 57
 defined 72
Dlu alias 41
documentation 66
domain
 defined 72

E

element
 element 72
Email address ii
entry field
 defined 72
ESA
 defined 72
EXPORT 21
extended architecture
 defined 72

F

FAX ii
fiber optic 4
field
 defined 72
FORCE 21
FORMAT 21
From 31, 41, 52, 57
function key area 20
 defined 72

G

gateway
 defined 72
Gateway Path 50
GCS
 defined 72
Group
 defined 72
group control system
 defined 72
grouping Rules 26

H

Hcvname 31, 41, 52, 57
Hcvtype 31, 41, 52, 57
host
 defined 72
Hours 57

I

ID 21
IMS 4
 defined 72
Inactivity 57
Information Management System
 defined 72
INIT 21
initial program load
 defined 72
INSTALL 21
Install a component 23
installing the Network Data File 21
inter user communication vehicle
 defined 72
interactive administration 23
Internet Protocol
 defined 72
IP
 defined 72
IP data 31, 57
IPL
 defined 72
ISTEXCAA 46
 defined 72
IUCV
 defined 72

L

LAN 4
LANGUAGE 22
leased lines 4
licensing 67
line monitors 4
LOAD 22
load balancing 53
LOG 22
logical unit
 defined 72
LOGMAX 22
Logmode 41, 47
LOGSIZE 22
LU
 defined 72

M

maintaining the Network Data File 21
major node
 defined 72
manual set 66
manuals 66
media 65
Message queue 23
 defined 72
minor node
 minor node 73
MVS
 defined 73

N

NCP 4
 defined 73
Netid 31, 41, 52, 57
 defined 73
Netview 4
 defined 73
network
 defined 73
Network Center
 defined 73
Network Center Interface
 defined 73
Network Center Server
 defined 73
Network Control Program

 defined 73
Network Data File 21, 24
 defined 73
Network id
 defined 73
network identifier
 defined 73
Network Virtual Route 50
node
 defined 73

O

Olu 31, 41, 52, 57
 defined 73
Olu alias 41
OLU-DLU 31, 41, 52, 57
operating system
 defined 73
optional publications 66
origin logical unit
 defined 73
OS
 defined 73
OS SMF account records 30, 40, 51, 56
OS/390
 defined 73

P

packaging 65
panel
 defined 73
panel body 20
 defined 73
panel element
 defined 73
panel id
 defined 73
PASSWORD 22
patch cords 4
path 9
path priorities 54
pattern matching 26
pattern matching character
 defined 73
physical unit
 defined 73
PLU
 defined 74
pop up window

- defined 74
- primary logical unit
 - defined 74
- PRINT 22
- protocol convertors 4
- PTF
 - defined 74
- PTFs 23
- PU
 - defined 74
- publications 66

Q

- Query 46
 - defined 74

R

- RDT 47
- Reload data file 24
- REMOVE 22
- Remove a component 24
- request/response unit
 - defined 74
- reset anchor blocks 24
- resource
 - defined 74
- Resource definition table 47
- rotors 4
- RU
 - defined 74
- Rule
 - defined 74
- Rule grouping 26
- Rule processing 24
- Rule type 31, 41, 52, 57
- Rules for Access 32
- Rules for Alias 42
- Ruleset
 - defined 74
- Rulesets 26

S

- SAA user interface 20
- SBFA 47
- SDLC
 - defined 74
- secondary logical unit
 - defined 74
- Select 50
 - defined 74
- Select list 52
- selection field
 - defined 74
- SERVER 22
- session
 - defined 74
- session characteristics 31, 41
- Session information blocks 47
- Session Management Exit 46
 - defined 74
- session termination 56
- Session type 31, 41, 52, 57
- SIB 47
- SLU
 - defined 74
- SLU-PLU 31, 41, 52, 57
- SME
 - defined 74
- SMF
 - defined 74
- SNA 75
 - defined 74
- SNA network interconnection
 - defined 74
- SNI 30
 - defined 74
- SOPT 47
- SRT 47
- SSCP 22, 31, 41, 52, 57
 - defined 74
- Start options 47
- Status output log 24
- Storage usage 24
- Subarea 31, 41, 52, 57
 - defined 74
- subsystem
 - defined 74
- support email ii
- Swap output log 24
- Symbolic resolution table 47
- Synchronous Data Link Control
 - defined 74
- SYSOUT 30, 40, 51, 56

System logmode table 47
System Management Facility
 defined 75
System Services Control Point
 defined 75
Systems Network Architecture
 defined 75

T

tape media 65
TCAS
 defined 75
TCU 4
 defined 75
teleprocessing
 defined 75
terminal
 defined 75
terminal control address space
 defined 75
The Network Center
 defined 75
Time 31, 41, 52, 57
Time Sharing Option
 defined 75
Timeout 56
 defined 75
TNCADMN panel 23
TNCUTIL 21
To-Network 42
transmission control unit
 defined 75
trial 65, 67
TSO 4
 defined 75

U

UNLOAD 22
user
 defined 75
user interface 20

V

Value Group 27, 44
 defined 75
virtual machine
 defined 75
virtual printer 30, 40, 51, 56
Virtual route blocks 47
Virtual Telecommunications Access Method
 defined 75
VM
 defined 75
VM account records 30, 40, 51, 56
VMFPLC2 65
VRBLK 47
VTAM
 defined 75

W

website ii
window
 defined 75
workstation
 defined 75
World Wide Web address ii
WTO 22
WTOR 21

X

XA
 defined 75

Z

z/OS
 defined 75
z/VM
 defined 76