ACCESS

Document Number TNC-0005-9

The Network Center

North Ridge Software, Inc.

Copyright

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

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

List of Illustrations

Preface

This document provides general information about the Network Center's Access Component. Topics include:

- Introduction to Access
- Using Rules to control session establishment
- How to create Rules quickly and efficiently
- Rule planning aids and example Rules
- Implementing Access
- Tracking session activity
- Access Administration Menu choices
- Access Messages

Who Should Read this Document

This document is for individuals who utilize Access at their installation. It provides information on using Access to implement Rules that protect a VTAM domain from being misused by programs, devices, and terminal operators.

You might use the information in this book if you:

- Plan to administer or utilize Access at your installation
- Plan to install and/or maintain the Network Center and Access. This role is referred to as the "Network Administrator".

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, visit www.North-Ridge.com on the World Wide Web.

How this Document is Organized

The Network Center's *Access* manual is organized into two parts called the **Access Guide** and **Access Reference**.

The Access Guide

The Guide contains the following chapters:

Chapter 1: "Introduction to Access" briefly explains what Access does, and how it works within your network.

Chapter 2: "Using Rules Control Session Establishment" introduces the Access Rule: the tool that allows you to approve or deny VTAM sessions within the local domain. It includes sections describing Rule operands, Ruleset Rules, Rule Groups, and Rule processing.

Chapter 3: "Techniques for Creating Efficient Rules Faster" explains techniques and tools that can help you to define Rules quickly and for maximum processing efficiency.

Chapter 4: "Planning for Access Implementation" provides useful hints, examples and worksheets for establishing Rules, Rulesets, and Groups before you implement them.

Chapter 5: "Implementing Access" guides you in defining and activating Rules online, as well as testing them to ensure that they are effective.

Chapter 6: "Tracking Session Approval and Denial" includes guidance on using tools that allow you to view session statistics, Rule messages, and other Rule activity resources. It also describes how to activate the accounting option for recording specific Network Center or Access messages.

Access Reference

Access Reference includes:

Chapter 7: "Access Component Administration Menu Choices" provides concise, detailed procedures for the Access menu functions.

Chapter 8: "Messages" describes Access messages and the expected system, operator, and Network Administrator responses.[1]

How to Send Your Comments to North Ridge Software

We welcome comments and suggestions that might help us 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 publication, the publication version, and the page, section, or topic you are commenting on.

---

[1] The Network Administrator is the person responsible for installing and maintaining the Network Center and, normally, Access.

Part One: The Access Guide

Chapter 1. Introduction to Access

This chapter provides basic information on the Access Component. Topics cover the following questions:

- "What Does Access Do?".
- "How Does Access Work?".

What Does Access Do?

Access is a member of the Network Center, a family of software components that operate independently or together in the z/OS and z/VM environments to provide you with the power to manage, monitor, and control VTAM based networks. (See the *General Information* manual, TNC-0001, for more information).

Access provides absolute control over session approval and denial in a local VTAM[2] domain, allowing you to protect it from misuse by programs, devices, and terminal operators that are inside or outside of the domain or network.

Access provides this security through Rules that you can set to meet various session establishment conditions. Using Access, you can dynamically maintain session Rules, detect session violations, produce session audit trail information, and interactively view sessions being processed by VTAM.

How Does Access Work?

During execution, VTAM processes requests for sessions between two LUs (logical units). These sessions allow information to be transferred between a terminal device and a processing subsystem - such as CICS, TSO, VSCS, IMS, ROSCOE, IDMS, MODEL204, and NETVIEW - or between two programs. Session establishment is subject to the approval or denial of an optional VTAM installation exit called ISTEXCAA.

Access resides in ISTEXCAA. As each VTAM session request travels through this Session Management Exit (SME), Access extracts information associated with the proposed session, compares the information against the active Access Rules, and allows or denies the session accordingly. (Access does not rely on security procedures implemented in other nodes to assure that the domain is used properly).

---

[2] VTAM is a key component of a SNA based network and handles a wide variety of tasks associated with an operating network of devices, users, and applications. The Network Administrator at each installation controls the type of processing undertaken by VTAM via a series of definitions and activities within VTAM (VTAMLST definitions, etc.).

The following figure illustrates the basic Access architecture:

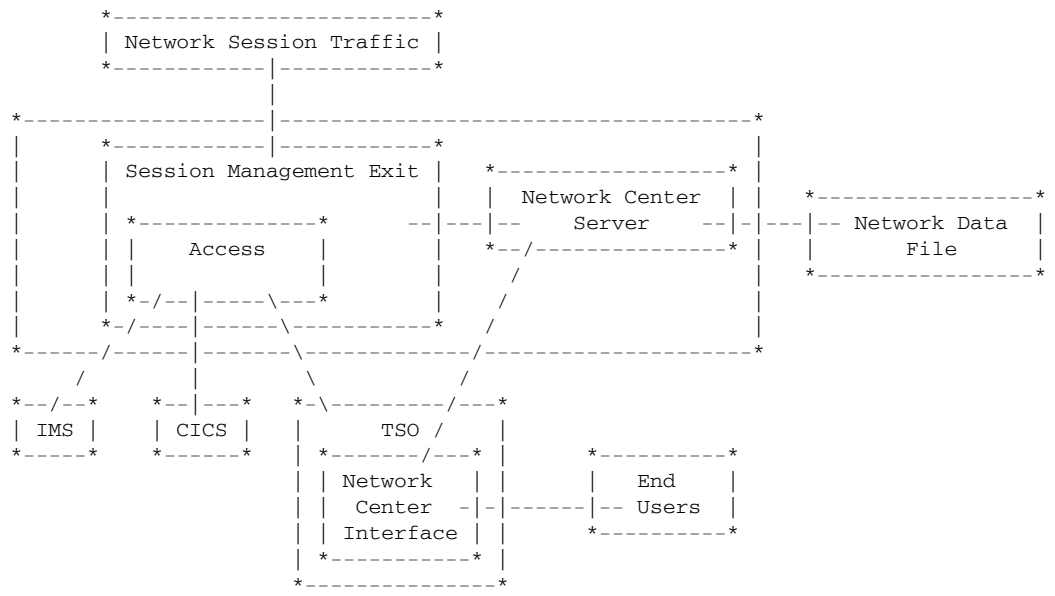

Figure 1. General Access Architecture

Chapter 2. Using Rules to Control Session Establishment

Access allows you to define Rules that control approval and denial of VTAM Sessions within your local domain. This Chapter describes the Access Rule and the various structures that allow you to define, organize, and process Rules. Topics include:

Rules

Access compares session requests against **Rules** that determine whether the session will be allowed or denied. You can define Rules using the "Rule definition" panel. Each Rule panel allows you to create one Rule:

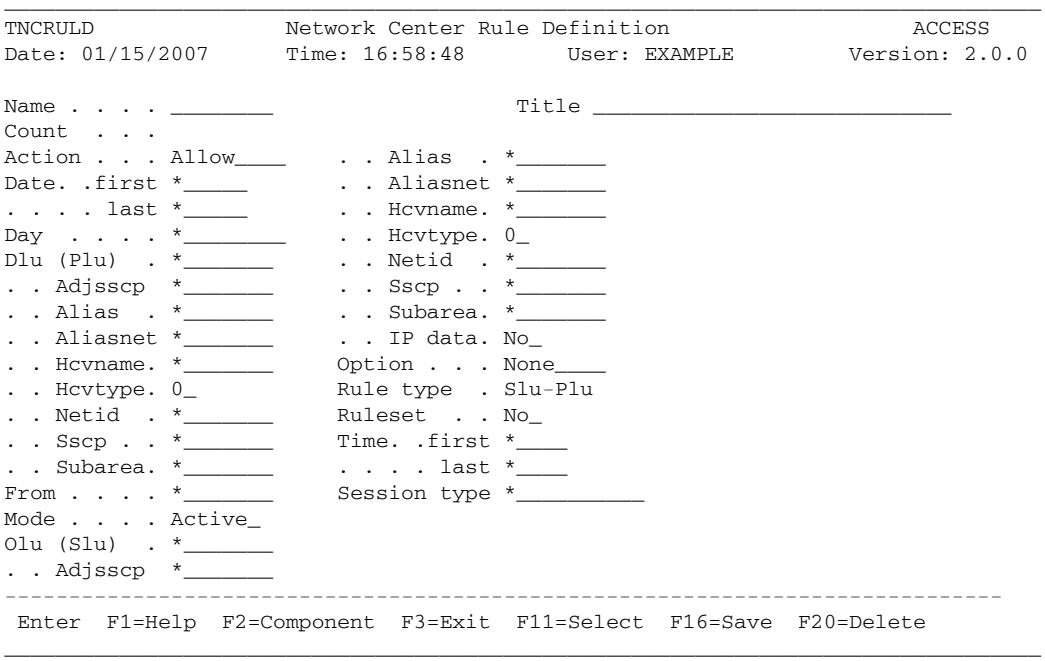

Figure 2. Rule Definition Panel (TNCRULD)

The Rule panel contains definable **operands**, called "fields". These fields determine the conditions that allow or deny a session between particular network resources. For example, you can use the operands to specify the names of the session partners, the name and title of the Rule, the time of day the Rule will operate, and whether or not the session will be granted access.

Many of the fields default to an asterisk (*****). This is a pattern matching character, which allows any applicable value to match the field operand. See "Chapter 3. Techniques for Creating Efficient Rules Faster" on page 27 for more information.

You can set the order in which the Rules are compared to the sessions by organizing them into Rulesets and/or Groups. This Rule priority order is also called the "processing order". See "Ruleset Rules" on page 22 and "Rule Groups" on page 25 for more information.

Rule Operand Definitions

As discussed in "Rules" on page 9, **operands** are the fields in the Rule Definition panel that you can set to allow or deny establishment for a particular session. The remainder of this section defines each operand in alphabetical order.

Most of the operand values default to an asterisk pattern character (*****) (see "Pattern Matching: Creating Rule Operand Masks" on page 27). Operands that do not default to the asterisk are underlined in the following definitions. Many of the operands also accept a Value Group specification, as noted in the operand's definition (see "Value Groups: Creating Symbolic Rule Operand Values" on page 29 for more information).

Action

The **Action** operand establishes the action that Access will take when a session matches the Rule. You may use one of the following settings:

Setting	*Function*
ALLOW	Permits the session to continue as normal
DENY	Access will reject the session

Date

The **Date** operand establishes the first and last calendar date that the Rule will be effective. The dates are inclusive.

To define the date field, enter the first calendar date in the YYMMDD format in the "first" field; Enter the last calendar date in the YYMMDD format in the "last" field.

Day

The **Day** operand establishes the day(s) of the week that the Rule will be effective.

To define the field, enter MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, or SUNDAY or use one of the following special groupings:

Grouping	*Includes*
MIDWEEK	TUESDAY, WEDNESDAY, and THURSDAY
WEEKDAYS	MONDAY, TUESDAY, WEDNESDAY, THURSDAY, and FRIDAY
WEEKENDS	SATURDAY and SUNDAY

Dlu (Plu)

The **Dlu** or **(Plu)** operand identifies the Destination Logical Unit (DLU), which is normally also the Primary Logical Unit (PLU). Most often, this is the name of the application or subsystem associated with the session.

To define the field, enter the eight-character LU name for the Dlu/Plu.

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you may display or define the Value Group by placing the cursor on the field and using the F11=Select action.

| The Network Center derives the Dlu/Plu value from the Resource Identifier Control Vector (RIC) that is passed to the Session Management Exit (SME) by VTAM.

Adjsscp

The **Adjsscp** (Adjacent SSCP) operand identifies the eight-character name of the System Services Control Point (SSCP) that is in the direction of the DLU. This value is normally the name of the VTAM domain adjacent to the processor that the Network Center is operating on. However, this is not necessarily the "home domain" of the Dlu/Plu.

For INIT OTHER CD processing the Adjsscp is the name of the SSCP in the direction of the SLU.

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you may display or define the Value Group by placing the cursor on this field and using the F11=Select action.

Alias

The **Alias** operand identifies the alias name assigned to the Dlu/Plu (if an alias assignment has been made).

To define the field, enter the eight-character alias name of the Dlu/Plu, which is derived from the PLU Resource Identifier Control vector (RIC).

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you may display or define the Value Group by placing the cursor on the field and using the F11=Select action.

You may also specify an equal sign ("=") in the Dlu (Plu) Alias field to cause the Network Center to match or select the Rule if the corresponding "Name" or "Alias" field value matches the pattern in the corresponding Name field. This allows you to specify the LU name only once (in the Name field) and have the corresponding Rule apply whether the LU's name is the real name or the Alias name.

Aliasnet

The **Aliasnet** operand identifies the eight-character network id for the network in which the assigned alias name (LU) is known. This value is derived from the Resource Identifier Control Vector (RIC).

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you can display or define the Value Group by placing the cursor on the field and using the F11=Select action.

Hcvname

The **Hcvname** operand identifies the name of a resource that has been defined as a part of the upper level hierarchy for the LU (as defined within the Hierarchy Control Vector).

To define this field, enter the one to eight-character name of the Dlu/Plu's VTAMLST definition entry. You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you can display or define the Value Group by placing the cursor on the field and using the F11=Select action.

Hcvtype

The **Hcvtype** operand establishes the type of VTAM defined resource that is operating as the Dlu/Plu. (In other words, it has been defined as a part of the upper level hierarchy for this LU, as defined within the Hierarchy Control Vector.)

The values for this field are as follows:

1	Communication controller
2	APPL major node
3	Local non-SNA major node
4	Switched major node
5	Local SNA major node
6	CDRM major node
7	CDRSC major node
8	CA major node
10	CDRM
12	GROUP
14	LINE
15	Direct attachment node
16	APPL
18	PU
22	LU
23	Link station
24	CDRSC
28	LAN major node
29	Packet major node
30	XCA major node

Figure 3. Hierarchy Control Vector Assignments

The Hierarchy Control Vector may contain several elements for a single LU, depending on the definition hierarchy used at your installation. You can determine the HCV contents by activating The Network Center's trace level messages.

Note: These values are reproduced here for convenience only. You should obtain the currently defined values from the VTAM Customization publication that applies to your version of VTAM.

Netid

The **Netid** field identifies the eight-character network name for the home network of the Dlu/Plu. This value is derived from the Resource Identifier Control Vector (RIC).

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you may display or define the Value Group by placing the cursor on the field and using the F11=Select action.

Sscp

The **Sscp** operand identifies the eight-character logical unit name for the system services control point (SSCP) for the domain that controls the Dlu/Plu. This value is derived from the Resource Identifier Control Vector.

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you may display or define the Value Group by placing the cursor on this field and using the F11=Select action.

Subarea

The **Subarea** operand identifies the numeric value of the subarea associated with the domain that controls the Dlu/Plu. This value is derived from the Resource Identifier Control Vector (RIC).

You may use pattern matching or a Value Group in this field. If you enter a Value Group value, you can display or define the Value Group by placing the cursor on the field and using the F11=Select action.

From

The **From** operand identifies the PLU (application or subsystem) that last went into session with the device.

This field is typically used in conjunction with allowing LOGAPPL type applications to forward a device to any desired subsystem. It also applies to subsystems that create additional sessions in order to service the actual subsystem requests (for example, TSO).

You may use pattern matching or a Value Group in this field. If you define a Value Group value, you may display or define the Value Group by placing the cursor on the field and using the F11=Select action.

Note: The Network Center uses the ILU (Initiating Logical Unit) identifier to establish the FROM value.

Mode

The **Mode** operand establishes the type of enforcement associated with the Rule. You must enter one of the following values (pattern matching is not valid):

Setting	*Function*
Active	The Rule will be used to evaluate sessions; the Component's action depends on the Action operand.
Dormant	The Rule will not be used when evaluating session conditions.
Test	The Rule will be used to evaluate sessions. If it matches, TNC0257 will be issued, but the Component will not perform actions. All messages, including Trace level messages, will be produced. The Test mode differs from the Warn mode in that the Test mode will evaluate the following Rules, while Warn mode will terminate when the Component finds a matching Rule. In this way, Test mode allows you to test a Rule without changing how the currently active Rules operate.
Warn	The Rule will be used to evaluate sessions, but no Component activity will be taken. However, messages and accounting will continue to operate as if in Active mode.

Name

The **Name** operand establishes the Rule's name. This name is used in the output log and associated accounting and maintenance processes. To define this field, enter a one to eight-character name to uniquely identify the Rule. (You cannot use pattern matching or Value Group names in this field.)

Olu (Slu)

The **Olu** or **(Slu)** operand identifies the logical unit name associated with the Origination Logical Unit (OLU), which is also normally the Secondary Logical Unit (SLU). Most often, this is the logical name of the terminal that is associated with the session. You may use pattern matching or a Value Group in this field.

Adjsscp

The **Adjsscp** (Adjacent SSCP) operand identifies the eight-character name of the System Services Control Point (SSCP) that is in the direction of the Olu. This value is normally the name of the VTAM domain adjacent to the processor that the Network Center is operating on. However, this is not necessarily the "home domain" for the Olu/Slu. For INIT OTHER CD processing the Adjsscp is the name of the SSCP in the direction of the ILU. You may use pattern matching or a Value Group in this field.

Alias

The **Alias** operand identifies the alias name assigned to the Olu/Slu (if an alias assignment has been made). To define this field, enter the eight-character alias name of the Olu/Slu, which is derived from the SLU Resource Identifier vector (RIC).

You may use pattern matching or a Value Group in this field. You may also specify an equal sign ("=") in the Olu(Slu) Alias field to cause the Network Center to match or select the Rule if the corresponding "Name" or "Alias" field value matches the pattern in the corresponding Name field. This allows you to specify the LU name only once (in the Name field) and have the corresponding Rule apply whether the LU's name is the real name or the Alias name.

Aliasnet

The **Aliasnet** operand identifies the eight-character network id for the network in which the assigned alias name (LU) is known. This value is derived from the Resource Identifier Control Vector (RIC). You may use pattern matching or a Value Group in this field.

Hcvname

The **Hcvname** operand is the 1 to 8 character name of a resource that has been defined as a part of the upper level hierarchy for the LU (as defined within the Hierarchy Control Vector). To define this field, enter the one to eight-character name of the Olu/Slu's VTAMLST definition entry. You may use pattern matching or a Value Group in this field.

Hcvtype

The **Hcvtype** operand establishes the type of VTAM defined resource that is operating as the Olu/Slu. (In other words, it has been defined as a part of the upper level hierarchy for this LU, as defined within the Hierarchy Control Vector.) The Hcvtype is a single decimal numeric value, with the values as described in Figure 3 on page 13.

The Hierarchy Control Vector may contain several elements for a single LU, depending on the definition hierarchy used at your installation. You can determine the HCV contents by activating The Network Center's trace level messages.

IP data

The **IP data** operand identifies whether the Rule contains IP information about the SLU. You may enter one of the following values:

Setting Function

No The Rule does not contain IP data.

Yes The Rule contains IP data. To define the IP information about the PLU, enter "YES" and use the F11 (Select) action to display the information entry window. You can then enter any of the following types of information:

IP address This field provides a mask value or actual value for the IP address. For example, an actual IP address is usually in the following format:

```
4.33.18.201
```

You could mask this value in the following manner:

```
4.33.18.2%%
```

Port number This field provides a mask value or actual value for the IP port number. For example, an actual port number is usually in the following common format:

```
1320
```

You could mask this value in the following manner:

```
13%%
```

DNS name This field provides a mask value or actual value for the IP DNS name identifier. For example, an actual DNS name is usually in the following common format:

```
sample.workstation.one
```

You could mask this value in the following manner:

```
                    sample.work*.%%%
```

Note: See "Pattern Matching: Creating Rule Operand Masks" on page 27 for information on creating masks.

Netid

The **Netid** operand identifies the eight-character network name for the home network of the Olu/Slu. This value is derived from the Resource Identifier Control Vector (RIC). You may use pattern matching or a Value Group in this field.

Sscp

The **Sscp** operand identifies the eight-character logical unit name for the system services control point (SSCP) for the domain that controls the Olu/Slu. This value is derived from the Resource Identifier Control Vector (RIC). You may use pattern matching or a Value Group in this field.

Subarea

The **Subarea** operand identifies the numeric value of the subarea associated with the domain that controls the Olu/Slu. This value is derived from the Resource Identifier Control Vector (RIC). You may use pattern matching or a Value Group in this field.

Option

The **Option** operand establishes the type and level of messages that the Network Center will issue when the Rule is operating.

The operand may be set as one of the following values:

HEXDUMP Produces a hex dump of all the parameters passed to the SME in addition to the normal informational messages that are produced when the Rule is matched. These messages are reproduced in the Message Queue and output log. These displays are useful when debugging the action of the SME. See "Hexdump" on page 47 for an example of the output result.

NONE Produces the normal informational messages associated with the Rule. No additional trace or debugging messages are produced.

SUPPRESS Suppresses all of the messages that are issued for this Rule.

TRACE Produces a series of trace messages that provide all of the input values associated with both of the session partners, in addition to the normal informational messages that are produced when the Rule is matched. See "Trace" on page 48 for an example of the messages that will appear.

You can use these Option settings for additional flexibility in diagnosing and evaluating the Network Center's operations.

Ruleset

The **Ruleset** operand allows you to define the Rule as a Ruleset Rule.

A Ruleset Rule establishes conditions that must match the session criteria in order for the Rules that it contains to be processed. (See "Ruleset Rules" on page 22 for an extended explanation of Rulesets).

Setting Function

No Entering "no" indicates that the Rule is not a Ruleset.

Yes Entering "yes" indicates that the Rule establishes a Ruleset.

If you enter "yes" in the Ruleset field, an additional field called "Select" appears; you can mark it with any keyboard character to open the Ruleset Rule Name List. You may then enter the names of the Rules that the Ruleset will contain.

You can use pattern matching or Value Groups in these fields. If you enter a Value Group value, you can display or define the Value Group by placing the cursor on the field and using the F11=Select action. When you are done entering the Rule and or Ruleset names, use the F16=Save action to save the Ruleset Rule Name List and return to the Rule definition panel.

You can also display the Ruleset Rule Name List by using the F11=Select action. If the 'Ruleset' field has been marked "yes" the Ruleset Rule Name List will appear. If the 'Ruleset' field is marked "no", a pop up window appears asking you to confirm that you want to display the Ruleset list: Select choice 1 to display the list, or choice 2 to resume back to the Rule definition panel.

For more information on defining Rulesets, see "Defining Rules or Rulesets" in Chapter 5.

Rule type

The **Rule type** operand determines how a requesting session's criteria is compared to the Rule's content in terms of the incoming Destination Logical Unit (DLU) or Primary Logical Unit (PLU) values and the Origination Logical Unit (OLU) or Secondary Logical Unit (SLU) values. You may enter one of the following values:

Value ***Usage***

Dual compares the incoming Plu value to the Dlu (Plu) operand, and the incoming Slu value to the Olu (Slu) operand. If the conditions don't match, the incoming Plu value will be compared to the Olu (Slu) operand and the incoming Slu value will be compared to the Dlu (Plu) operand. (In other words, PLU to PLU and SLU to SLU first, then PLU to SLU and SLU to PLU).

The Dual value is useful for situations where either session partner can act as the PLU or the SLU. It allows you to create just one Rule (instead of two) to handle both possibilities.

Olu-Dlu compares the incoming values for the Origin Logical Unit (Olu) against the Olu (Slu) operand, and the incoming values for the Destination Logical Unit (Dlu) against the Dlu (Plu) operand.

Slu-Plu compares the incoming values for the SLU against the Olu (Slu) operand, and the incoming values for the PLU against the Dlu (Plu) Rule settings.

Note: The Olu and Slu are usually the same value when the Slu is a terminal. However, certain programmable devices or LU6 programs can act as both a Dlu (Plu) and an Olu (Slu). If this is the case, VTAM will indicate the condition in the control vectors that are passed to this Component. The "rule type" field is intended to give you control over which of the session elements the Dlu (Plu) and Olu (Slu) values apply to.

Session type

The **Session type** operand identifies the type of session initiation that is defined by the Rule.

Value	*Usage*
*	Any type of session initiation.
AUTOLOGON	The session is being initiated as a result of a VARY LOGON or LOGAPPL.
PLU-REQUEST	The subsystem has requested the session.
RD-SEARCH	The request was initiated as the result of a resource discovery search.
SLU-REQUEST	The terminal device has initiated the session
THIRD-PARTY	Another PLU has requested the session (for example, a LOGAPPL type subsystem)

Session type information is extracted from the Exit Routine Function Code available to this Component.

Time

The **Time** operand establishes the first and last wall clock time (HH:MM format) that the Rule will be effective. These are inclusive times of the day.

To define this operand, enter the start time for the Rule in the "first" field, and the end time for the Rule in the "last" field. For example, if you want the Rule to become effective at 8:00 a.m. and to end at 5:00 p.m., you would enter "08:00" in the first field and "17:00" in the last field.

Title

The **Title** operand allows you to establish a 1 to 28 character description of the Rule. The title will be used in several Component panels to help you identify the Rule.

Rule Operand Sources

In order to create correct Rules, you need to understand the source for each operand value. The following illustration gives a conceptual overview of these sources:

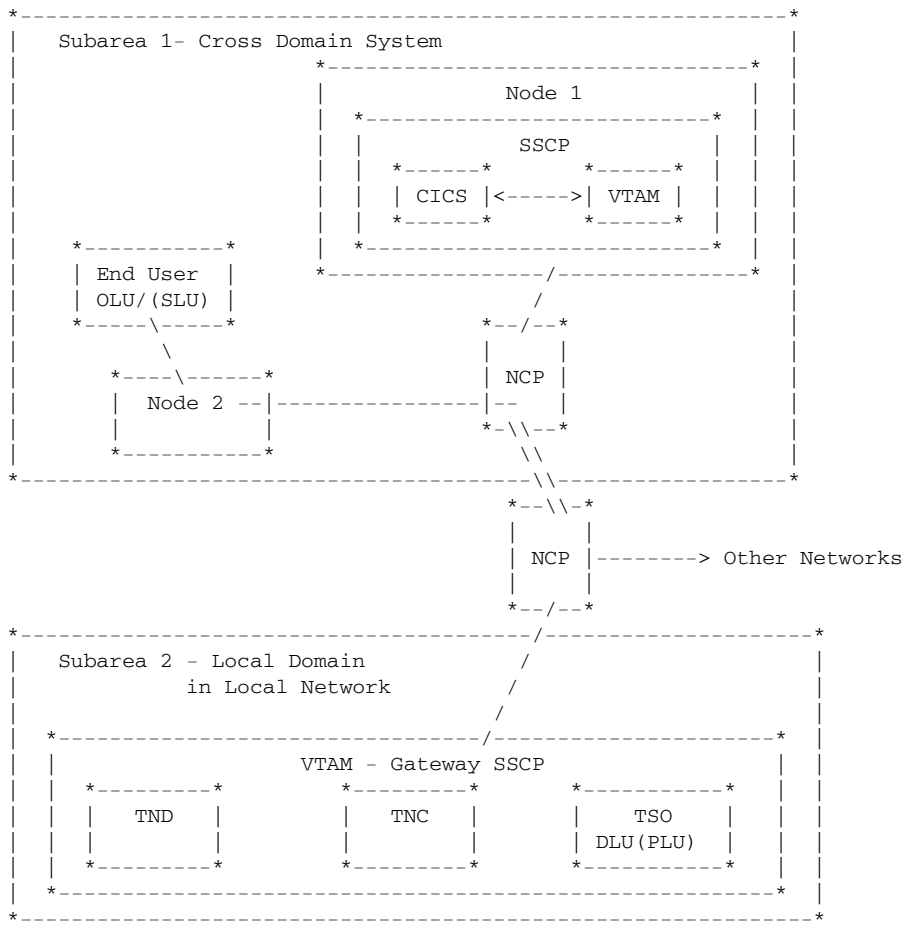

Figure 4. Rule Operand Source Locations

Ruleset Rules

A **Ruleset Rule** is a Rule that defines a set of Rules. When Access is actively processing Rules, it acts as a "gate" that allows Access to bypass the Rules it contains, unless the session criteria matches its operands. If the session criterion matches the operands in the Ruleset Rule, Access will begin to process the Rules it contains.

Ruleset Rules ensure that Access does not waste time evaluating Rules that do not apply to a requesting session. When Access is processing a session request, it scans each Rule until it finds one that matches the session's criteria. The more Rules that do not match the session, the longer it takes for Access to process.

Rulesets also allow you to organize and simplify your Rule structure. For example, you can place all of the Rules for a particular condition under one Ruleset Rule (according to their processing order). To illustrate this, assume that you defined the following Rules for a domain (these examples provide a syntactical representation of the Rule definition panel):

```
TERM1S   TNCRULE ACTION=ALLOW,SLU=TERM1*,SLUNETID=CREDIT,PLU=*
TERM2S   TNCRULE ACTION=ALLOW,SLU=TERM2*,SLUNETID=CREDIT,PLU=TSO*
TERM3S   TNCRULE ACTION=ALLOW,SLU=TERM3*,SLUNETID=CREDIT,PLU=CICS*
SYS1435  TNCRULE ACTION=ALLOW,SLU=SYS1435,SLUNETID=SYSTEMS,PLU=CICS*
SYS1422  TNCRULE ACTION=ALLOW,SLU=SYS1422,SLUNETID=SYSTEMS,PLU=*
I8204    TNCRULE ACTION=ALLOW,SLU=IB204,SLUNETID=SYSTEMS,PLU=*
SYS7045  TNCRULE ACTION=ALLOW,SLU=SYS7045,SLUNETID=SYSTEMS,PLU=*
ABTI83   TNCRULE ACTION=ALLOW,SLU=ABTI83,SLUNETID=SYSTEMS,PLU=*
OTHERS   TNCRULE ACTION=DENY,SLU=*,PLU=*,SLUNETID=*
```

These Rules allow specific SLU's (for example, SYS1435) with specific netid's (for example, SYSTEMS) to go into session with certain PLU's (for example, CICS). The last Rule denies any sessions that do not match one of the Rules conditions.

Therefore, if an SLU named TERM5500 with the netid HDQTRS made a session request, Access would evaluate the first nine Rules until finally using the OTHERS Rule to process the session (in this case, to deny the session). You could accelerate this process by using Ruleset Rules.

Consider the following changes using Ruleset Rules:

```
TERMS    TNCRULE ACTION=ALLOW,SLUNETID=CREDIT,RULESET=YES
     TERM1S   TNCRULE ACTION=ALLOW,SLU=TERM1*,PLU=*
     TERM2S   TNCRULE ACTION=ALLOW,SLU=TERM2*,PLU=TSO*
     TERM3S   TNCRULE ACTION=ALLOW,SLU=TERM3*,PLU=CICS*

SYSTEMS  TNCRULE ACTION=ALLOW,SLUNETID=SYSTEMS,RULESET=YES
      SYS1435  TNCRULE ACTION=ALLOW,SLU=SYS1435,PLU=CICS*
      SYS1422  TNCRULE ACTION=ALLOW,SLU=SYS1422,PLU=*
      I8204    TNCRULE ACTION=ALLOW,SLU=IB204,PLU=*
      SYS7045  TNCRULE ACTION=ALLOW,SLU=SYS7045,PLU=*
      ABTI83   TNCRULE ACTION=ALLOW,SLU=ABTI83,PLU=*

OTHERS   TNCRULE ACTION=DENY,SLU=*,PLU=*,SLUNETID=*
```

Figure 5. Example Rulesets

In Figure 5 on page 22, we grouped all the Rules into Rulesets according to their SLUNETID. Each of these Rulesets would only allow Access to process the Rules it contains if the requesting session matched the parameters contained in the Ruleset definition (i.e. the netid must match).

Now, if the same SLU (TERM5500) with the Netid of HDQTRS requested a session, Access would first evaluate the Rule operand values of the TERMS Ruleset. The SLUNETID would not match, and Access would skip to the Systems Rule to continue evaluation. Its SLUNETID would not match either, so Access would skip to OTHERS, where it would locate a match (the '*' indicates that any valid value matches). Notice that this Rule interpretation process evaluated only three Rules, instead of the previous nine.

To define a Ruleset, set a Rule definition panel with the Ruleset Rule's operands and press the F11=Select key to open the Ruleset Rule Name List panel. This panel provides an area for you to define the names of the Rules that the Ruleset contains. The following two figures show the definition process for the "TERMS" Ruleset. The Rule definition panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 12:47:11        User: EXAMPLE        Version: 2.0.0

Name . . . . TERMS___                   Title Ruleset_for_TERMS___________
Count  . . .
Action . . . Allow____     . . Alias  . *________
Date. .first *_____        . . Aliasnet *________
. . . . last *_____        . . Hcvname. *________
Day  . . . . *_________    . . Hcvtype. 0_
Dlu (Plu)  . *________     . . Netid  . CREDIT__
. . Adjsscp  *________     . . Sscp . . *________
. . Alias  . *________     . . Subarea. *________
. . Aliasnet *________     . . IP data. No_
. . Hcvname. *________     Option . . . None____
. . Hcvtype. 0_            Rule type  . Slu-Plu
. . Netid  . *________     Ruleset  . . Yes Select _
. . 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. TERMS Ruleset

The Ruleset Rule Name List panel would appear as follows:

```
TNCRNAM                 Ruleset Rule Name List                      ACCESS
Date: 01/15/2007       Time: 12:49:07        User: EXAMPLE        Version: 2.0.0

  1. TERM1S__        20. ________        39. ________        58. ________
  2. TERM2S__        21. ________        40. ________        59. ________
  3. TERM3S__        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 7. Ruleset Rule Name List with Example Ruleset

In the Ruleset Rule Name List, make sure to define the names of each Rule to be included in the Ruleset according to their processing order.

For more information on Ruleset definition, see "Defining Rules and Rulesets" on page 90. To learn how Access processes Rules, see "Rule Processing" on page 26. For more information on how Access processes, see "Organizing Rules into a Hierarchy" on page 43.

Rule Groups

A Rule **Group** is an organizational construct that allows you to set the processing order for any combination of Rules, Rulesets or Groups. Unlike Rulesets, a Group does not *define* a set of Rules, it contains and organizes them, allowing you to present Rules, Rulesets, and other groups to Access as one processing unit.
The following figure shows a Group Definition panel:

```
TNCGRPD                Group Definition                          ACCESS
Date: 01/15/2007       Time: 14:12:47       User: EXAMPLE      Version: 2.0.0

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

Name . . . . ________                  Title _____________________________

  1. ________        16. ________        31. ________        46. ________
  2. ________        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 8. Group Definition Panel (TNCGRPD)

To define a Group, give it a "Name" and "Title" and then place the Rules, Rulesets, and/or Groups that you wish to include in the Group in the numbered fields according to their processing order.

For example, if you placed the TERMS and SYSTEMS Rulesets and the OTHERS Rule from Figure 5 on page 22 into a Rule Group, the Group definition panel would appear as follows:

```
TNCGRPD                 Group Definition                          ACCESS
Date: 01/15/2007        Time: 12:50:47        User: EXAMPLE     Version: 2.0.0

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

Name . . . . GROUP___                    Title Group_for_TERMS_and_SYSTEMS_

  1. TERMS___        16. ________        31. ________        46. ________
  2. SYSTEMS_        17. ________        32. ________        47. ________
  3. OTHERS__        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 9. Group Definition Example

Groups allow you to activate more than one Rule, Ruleset, or Group. To do this, define all of the desired Rule, Rulesets, and/or Groups within one Group and then specify the Group in the Component options record. For more information, see "Defining a Rule Group" on page 105 and "Specifying the Active Rules" on page 115.

Rule Processing

When a session request is made to your local domain, Access collects information from the session and begins to process the active Rules, starting with the first defined Rule, Ruleset, or Group within the Component options record. If the Ruleset or Rule does not match the session information, Access skips to the next Ruleset or Rule.

If Access finds a Rule where all the operands are true, it takes the ACTION specified in the "action" operand: it either allows or denies the session. (You can think of the Rule operands as being "**and**ed" together and the Rules as being "**or**ed" together.) If no Rule exists that grants access, then Access automatically rejects the session.

If Access finds a Ruleset where all of the operands are true, it continues to search the Rules contained within the Ruleset until it finds a match. If the operands in the Ruleset are not matched, then Access skips to the next active Ruleset (or Rule) to continue its search.

See "Organizing Rules into a Hierarchy" on page 43 and "Specifying the Active Rules" on page 115 for more information.

Chapter 3. Techniques for Creating Efficient Rules Faster

This chapter describes techniques that can help you to build Rules quickly and for maximum processing efficiency. Topics include:

- "Pattern Matching: Creating Rule Operand Masks"
- "Value Groups: Creating Symbolic Rule Operand Values" on page 29
- "Organizing Rules into a Hierarchy" on page 43
- "Diagnosing Session Management Exit Information" on page 47

Note: You can also test Rules to ensure their efficiency. See "Testing Rules" on page 124.

Pattern Matching: Creating Rule Operand Masks

Pattern matching is a process that allows a single value to represent one or more values. You can use pattern matching to greatly reduce the number of Rules that you must define by creating masks for the operand values. For example, the asterisk (*) pattern character - which is the default value for many of the Rule operands - allows any applicable value to match the operand.

You can use pattern matching characters in all of the Rule operands and panel fields unless it is specifically excepted under the description of the individual operand or entity. To view a description while using Access online, place the cursor on the field and use the F1=Help action. You can also view descriptions in "Rule Operand Definitions" on page 10.

The following pattern characters are available for Access. You can use them to mask numbers and alphabetic characters:

Character	*Meaning*
*	The asterisk represents any number of characters from none to the maximum number of characters in the operand or field. You may use as many asterisks as necessary within the operand.
%	The percent sign represents a single character of any value at the position that the percent sign is placed. You may use as many percent signs as necessary within the operand.

Figure 10. Pattern Matching Characters

The following figure demonstrates the pattern characters ability to mask diverse values. The first row gives example field entries; the column gives possible pattern strings; and the coordinates indicate whether the value is matched by the pattern string (YES) or not (NO).

Pattern	AB21HD00	AB31	SYS140	SSCP1
*	YES	YES	YES	YES
*1	NO	YES	NO	YES
1	YES	YES	YES	YES
HD	YES	NO	NO	NO
AB%1	NO	YES	NO	NO
AB%1*	YES	YES	NO	NO
%%%1*	YES	YES	YES	NO
%%%%1*	NO	NO	NO	YES

Figure 11. Pattern Matching Examples

To illustrate how pattern matching simplifies Rule definition, assume that you want to allow several devices from the CREDIT network with access to your TSO systems. The devices' names all begin with "SYS" followed by four numbers. Instead of creating a Rule for each device, you could define just one Rule, where the Olu (Slu) operand is defined with the mask "SYS%%%%":

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 12:52:15        User: EXAMPLE        Version: 2.0.0

Name . . . . SYSTEMS_                   Title Rule_for_SYSTEMS___________
Count  . . .
Action . . . Allow____    . . Alias  . *_______
Date. .first *_____       . . Aliasnet *_______
. . . . last *_____       . . Hcvname. *_______
Day  . . . . *________    . . Hcvtype. 0_
Dlu (Plu)  . TSO*____     . . Netid  . CREDIT__
. . 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)  . SYS%%%%_
. . Adjsscp  *_______
--------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 12. Rule Definition Panel with Pattern Matching

If a value or set of values is too diverse for pattern matching, you can define a Value Group instead. See "Value Groups: Creating Symbolic Rule Operand Values".

Value Groups: Creating Symbolic Rule Operand Values

Value Groups simplify Rule definition by allowing you to create one symbolic value that references a group of values. Because Value Groups are all inclusive, they are useful for situations where you can't use pattern matching.

To illustrate how they work, assume that you need to authorize three devices in a specific location for access to TSO; the devices' names - T34004, AXSR, and JR9X329 - are too diverse for pattern matching. Without using a Value Group, you would have to create the following Rules. (Each Rule is a syntactical representation of a Rule created in the Rule definition panel, 'TNCRULD'):

```
TSO1    TNCRULE ACTION=ALLOW,PLU=TSO*,SLU=T34004
TSO2    TNCRULE ACTION=ALLOW,PLU=TSO*,SLU=AXSR
TSO3    TNCRULE ACTION=ALLOW,PLU=TSO*,SLU=JR9X329
```

Subsequently, you decide that the same set of devices should have access to the CICS systems, so you create these additional Rules:

```
CICS1    TNCRULE ACTION=ALLOW,PLU=CICS*,SLU=T34004
CICS2    TNCRULE ACTION=ALLOW,PLU=CICS*,SLU=AXSR
CICS3    TNCRULE ACTION=ALLOW,PLU=CICS*,SLU=JR9X329
```

So far, you have created six Rules. However, you could simplify this structure by using a Value Group instead. To create the Value Group, you would simply place the three devices' names into a Group definition panel.
You would identify that the Group is a Value Group by specifying an "&" at the beginning of the Value Group's name. We named our Value Group &SYSTEMS:

```
TNCGRPD                Group Definition                          ACCESS
Date: 01/15/2007       Time: 13:22:32       User: EXAMPLE      Version: 2.0.0

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

Name . . . . &SYSTEMS                  Title Systems_Programmers_________

  1. T34004__        16. ________       31. ________       46. ________
  2. AXSR____        17. ________       32. ________       47. ________
  3. JR9X329_        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 13. &SYSTEMS Value Group

Now, the single value &SYSTEMS specifies all of the devices' names. You now only need to define the following two Rules (notice that we placed the Value Group name in the SLU field):

```
TSO      TNCRULE ACTION=ALLOW,PLU=TSO*,SLU=&SYSTEMS
CICS     TNCRULE ACTION=ALLOW,PLU=CICS*,SLU=&SYSTEMS
```

The Rule definition panel would appear as follows (this example shows the TSO Rule):

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 13:24:21        User: EXAMPLE        Version: 2.0.0

Name . . . . TSO_____                  Title Rule_for_TSO_access_________
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 . . . . *_______     Session type *__________
Mode . . . . Active_
Olu (Slu)  . &SYSTEMS
. . Adjsscp  *_______
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 14. Rule Definition Panel with Value Group

You have reduced the number of Rules from six to two. If you needed to add a new device that would be susceptible to the TSO and CICS Rules, you would simply add it to the &SYSTEMS Value Group.

If you wanted to generalize this structure even more, you could create an additional Value Group (call it &ONLINE) that contains the interactive systems that match the pattern TSO* or CICS*:

```
TNCGRPD                Group Definition                          ACCESS
Date: 01/15/2007       Time: 13:25:41       User: EXAMPLE      Version: 2.0.0

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

Name . . . . &ONLINE_                  Title Value_Group_for_Systems_____

  1. TSO*____        16. _________       31. _________       46. _________
  2. CICS*___        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 15. &ONLINE Value Group

Notice that the &ONLINE Value Group defines the PLU values, whereas the &SYSTEMS Value Group defines the SLU values. Using these two Value Groups, you could create just one Rule instead of the previous six, as follows:

```
ONLINE  TNCRULE ACTION=ALLOW,PLU=&ONLINE,SLU=&SYSTEMS
```

The Rule definition panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 13:27:02        User: EXAMPLE        Version: 2.0.0

Name . . . . ONLINE__                   Title Rule_for_TSO_and_CICS_system
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . &ONLINE_      . . 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)  . &SYSTEMS
. . Adjsscp  *_______
-----------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 16. Rule with Two Value Groups

You can specify Value Groups in the majority of Rule operands. A Value Group can also contain a reference to an additional Value Group. You can modify Value Groups via the Display (Value) Group choice from the Access Menu. For more information, see "Defining a Rule Group" on page 105.

Using Value Groups to Specify IP Data

You can also use Value Groups to specify IP Data pattern matching values in an Access Rule.

Steps:

1. Open an Access Rule definition panel (see "Defining Rules and Rulesets" on page 90), defining the 'Name' and 'Title' fields first. See the following figure for an example:

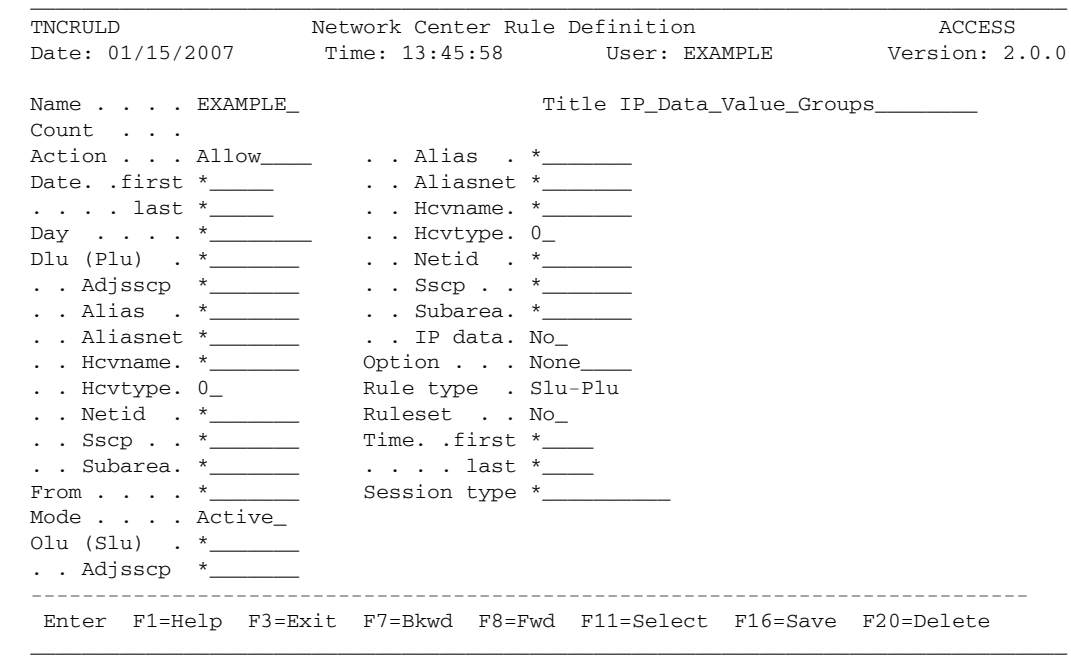

Figure 17. Rule Definition Panel, IP Data

2. Enter "Yes" in the IP data field; the cursor will jump to the next field.

3. Locate the cursor back onto the IP data field and press F11 (Select); the 'IP Data Display/Update' window appears:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 13:49:07        User: EXAMPLE        Version: 2.0.0

Name . . . . EXAMPLE_                   Title IP_Data_Value_Group_________
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  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 18. IP Data Display/Update Window

4. Enter the desired values in the fields. You can create a Value Group for the IP address, Port Number, or DNS Name. The following figure shows an example:

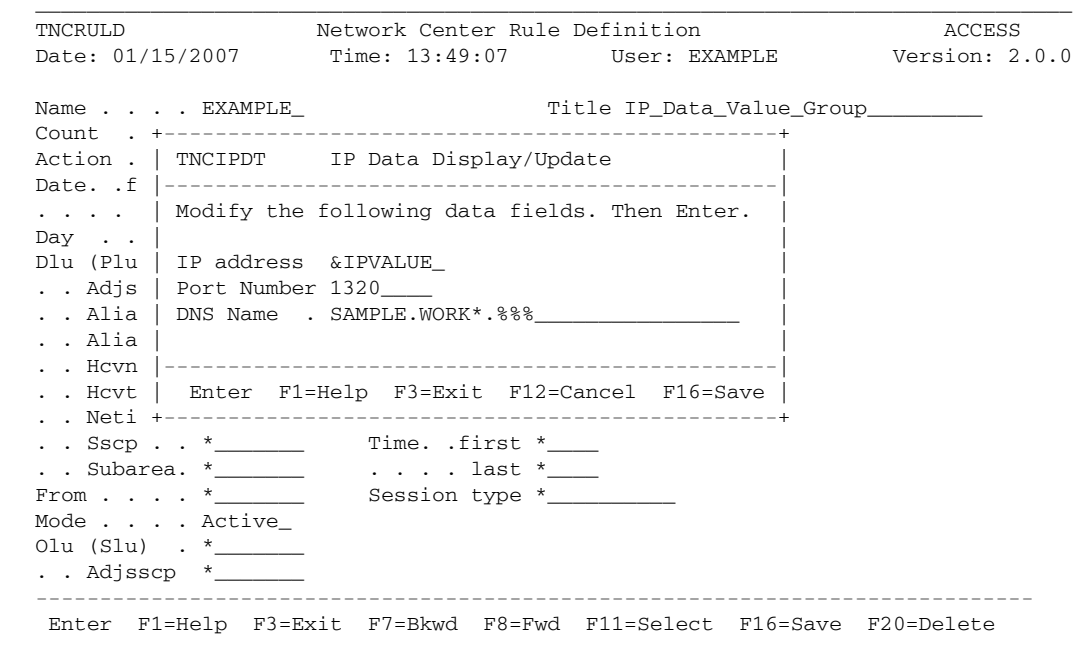

Figure 19. IP Data Display/Update Window with Value Group

5. After entering the desired value for a Value Group name in a field, place the cursor on the field value and press F11 (Select); the Group Definition panel for the Value Group appears:

```
TNCGRPD                 Group Definition                          ACCESS
Date: 01/15/2007        Time: 14:23:33        User: EXAMPLE     Version: 2.0.0

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

Name . . . . &IPVALUE                  Title _____________________________

  1. _________________     16. _________________     31. _________________
  2. _________________     17. _________________     32. _________________
  3. _________________     18. _________________     33. _________________
  4. _________________     19. _________________     34. _________________
  5. _________________     20. _________________     35. _________________
  6. _________________     21. _________________     36. _________________
  7. _________________     22. _________________     37. _________________
  8. _________________     23. _________________     38. _________________
  9. _________________     24. _________________     39. _________________
 10. _________________     25. _________________     40. _________________
 11. _________________     26. _________________     41. _________________
 12. _________________     27. _________________     42. _________________
 13. _________________     28. _________________     43. _________________
 14. _________________     29. _________________     44. _________________
 15. _________________     30. _________________     45. _________________
------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 20. Group Definition Panel, IP Data Value Group

6. Designate the type of Value Group you are defining by pressing F11 (Select); the Group/List function window appears:

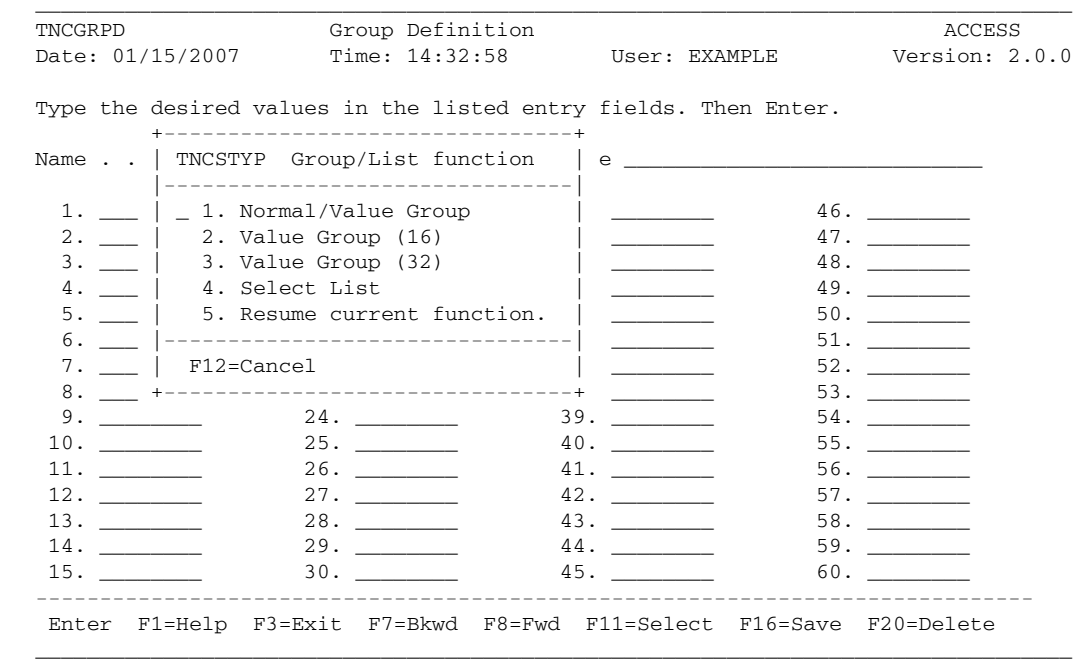

Figure 21. Group/List Function Window

To define a Value Group for IP address values, select choice 2, 'Value Group (16)'; this produces a Value Group with fields long enough to accommodate IP address value specifications:

```
TNCGRPD                 Group Definition                          ACCESS
Date: 01/15/2007        Time: 14:32:58        User: EXAMPLE     Version: 2.0.0

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

Name . . . . &IPVALUE                  Title _____________________________

  1. _________________     16. _________________     31. _________________
  2. _________________     17. _________________     32. _________________
  3. _________________     18. _________________     33. _________________
  4. _________________     19. _________________     34. _________________
  5. _________________     20. _________________     35. _________________
  6. _________________     21. _________________     36. _________________
  7. _________________     22. _________________     37. _________________
  8. _________________     23. _________________     38. _________________
  9. _________________     24. _________________     39. _________________
 10. _________________     25. _________________     40. _________________
 11. _________________     26. _________________     41. _________________
 12. _________________     27. _________________     42. _________________
 13. _________________     28. _________________     43. _________________
 14. _________________     29. _________________     44. _________________
 15. _________________     30. _________________     45. _________________
-------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 22. Value Group (16), IP Data

To define a Value Group for DNS Name values, select choice 3, 'Value Group (32)'; this produces a Value Group with fields long enough to accommodate a DNS name value (i.e. the URL) of up to thirty-two characters:

```
TNCGRPD                 Group Definition                          ACCESS
Date: 01/15/2007        Time: 14:37:45        User: EXAMPLE     Version: 2.0.0

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

Name . . . . &IPVALUE                    Title ________________________________

  1. ____________________________________    16. ____________________________________
  2. ____________________________________    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. ____________________________________
------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 23. Value Group (32), IP Data

7. In the numbered blanks, enter the values you wish to include in the Value Group. The following figure shows an example of IP address values:

```
TNCGRPD                 Group Definition                              ACCESS
Date: 01/15/2007        Time: 14:23:33        User: EXAMPLE        Version: 2.0.0

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

Name . . . . &IPVALUE                  Title IP_Address_Values___________

  1. 4.33.18.133_____      16. _________________      31. _________________
  2. 4.33.18.393_____      17. _________________      32. _________________
  3. 4.33.44.681_____      18. _________________      33. _________________
  4. 4.44.67.450_____      19. _________________      34. _________________
  5. 4.59.53.267_____      20. _________________      35. _________________
  6. 4.44.46.295_____      21. _________________      36. _________________
  7. 4.44.46.296_____      22. _________________      37. _________________
  8. 4.44.46.297_____      23. _________________      38. _________________
  9. 4.44.46.298_____      24. _________________      39. _________________
 10. 4.44.46.298_____      25. _________________      40. _________________
 11. 4.44.46.299_____      26. _________________      41. _________________
 12. 4.44.47.001_____      27. _________________      42. _________________
 13. 4.44.47.002_____      28. _________________      43. _________________
 14. 4.44.47.003_____      29. _________________      44. _________________
 15. 4.44.47.004_____      30. _________________      45. _________________
--------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 24. Example IP Value Group

8. After defining the values in the Value Group, press F3 (Exit); the 'Exit Function' window appears:

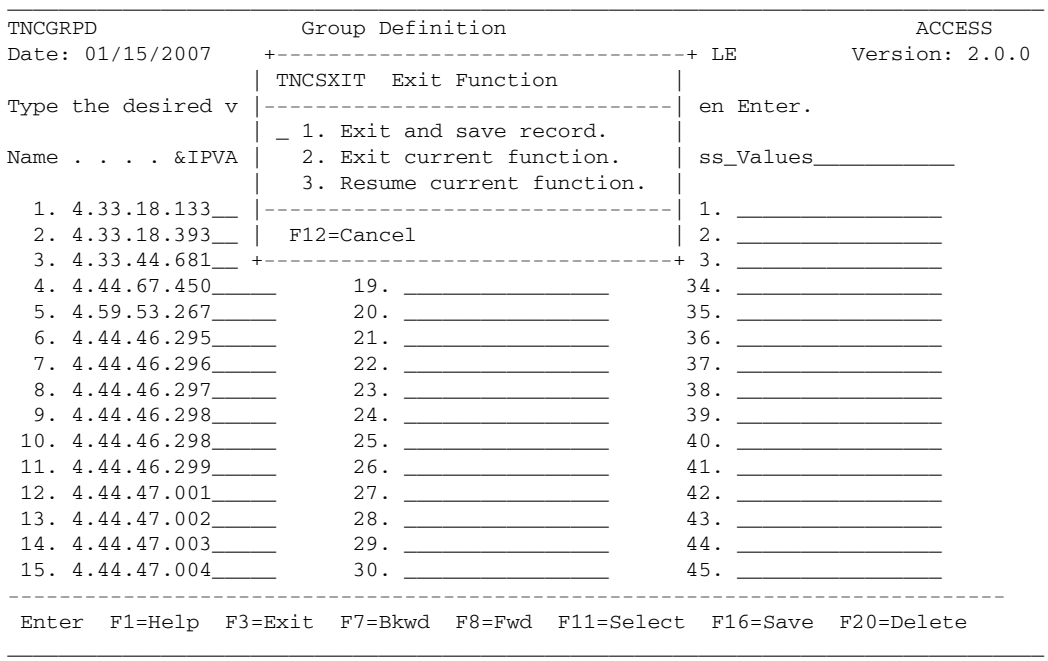

Figure 25. Exit Function Window

9. Select choice 1, 'Exit and save record'; a message appears stating that the record updated successfully:

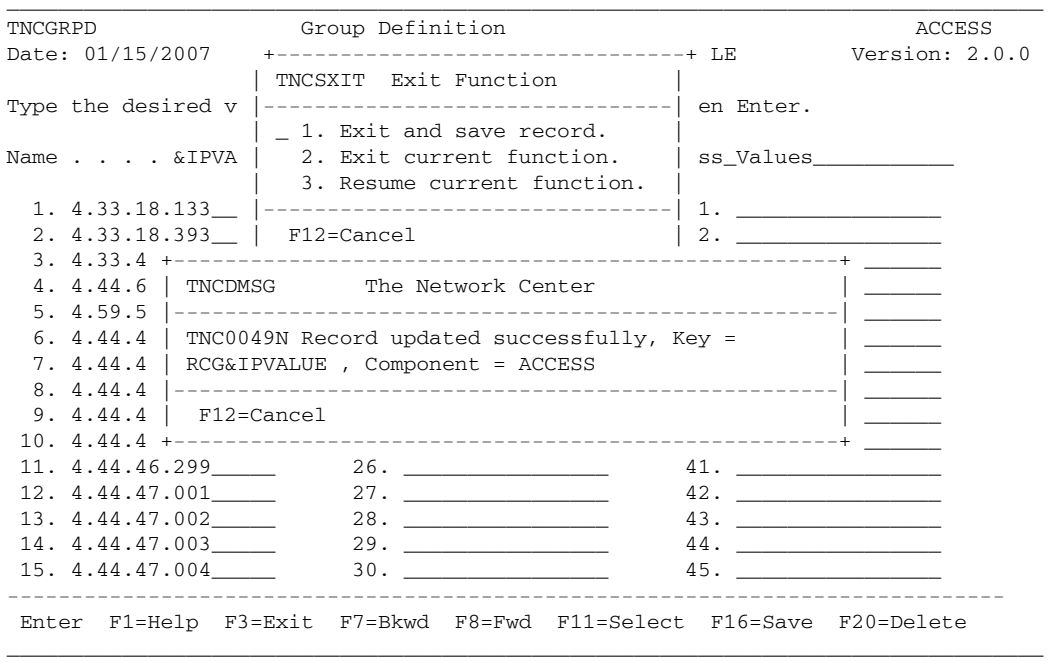

Figure 26. Value Group Update Message

10. Press F12 (Cancel) to cancel the message and return to the 'IP Data Display/Update' Window.

11. Press F16 (Save) to save the IP Data Display/Update information; a message appears stating that the record updated successfully.

12. Press F12 (Cancel) to cancel the message and return to the Network Center Rule Definition' panel.

13. Finish defining the Rule, following the procedures in "Defining Rules and Rulesets" on page 90. (Press F16=Save to save the Rule.)

Organizing Rules into a Hierarchy

An efficient Rule hierarchy provides for quick and efficient Rule processing: the less time it takes Access to process the Rules, the less CPU time it uses. An efficient Rule hierarchy can also help you to more easily organize and maintain various Rule, Ruleset, and Group definitions.

To review, Access Rules can be standalone, collected into Rulesets and/or collected into Groups. A Ruleset can contain Rules and Rulesets. A Group can contain Rules, Rulesets, and other Groups. (See "Chapter 2. Using Rules to Control Session Establishment" on page 9 for more information.)

The following examples of a simple and complex Rule structure are demonstrate how you can use Rulesets and Groups to keep your Rules manageable.

Simple Rule Structure

Assume that you are interested in creating Rules for the following situations:

- To restrict access to TSO and CICS to specific devices
- To allow access to any other subsystem from devices in your domain
- To reject access to a subsystem in your domain from any other devices

You would first create the following four Rules:

Rule	*Contents*
TSO	Set the PLU value to "TSO", the SLU value to the pattern of approved device names, and ACTION to "Allow"
CICS	Set the PLU value to "CICS", the SLU value to the pattern of approved device names, and ACTION to "Allow"
LOCALS	Set the Netid to your own netid, Subarea to your subarea value, and ACTION to "Allow"
OUTSIDE	Set ACTION to "Deny"

You would then group the Rules for reference purposes by creating a Group called "DAILY" that includes TSO, CICS, LOCALS, and OUTSIDE Rules, in that sequence. The following figure illustrates this Rule hierarchy:

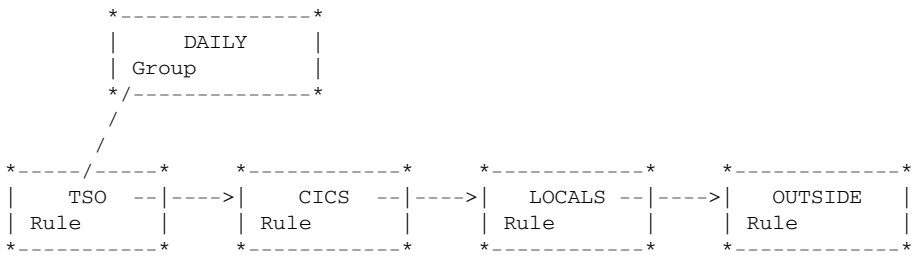

Figure 27. Simple Rule Hierarchy

When the "DAILY" Group is activated (see "Component Options" on page 153), the Rules are loaded and interpreted as indicated by the arrows.

Complex Rule Structure

Now, assume that you need to add access for the following devices and subsystems:

- TSO for devices with a pattern of T1*
- TSO when a LOGAPPL subsystem forwards the device
- TSO from another network
- CICS for devices with a pattern of UR%44*
- CICS when a LOGAPPL subsystem forwards the device
- CICS when CICS has requested the session
- any other subsystem whose name matches the pattern A*
- any subsystem if the device's name is T77R992

You would first create the following nine Rules:

Rule	*Contents*
TSOT1	Set the PLU value to "TSO", the SLU value to "T1*", and ACTION to "Allow"
TSOLOG	Set the PLU value to "TSO", the TYPE value to "THIRD-PARTY", and ACTION to "Allow"
TSONET	Set the PLU value to "TSO", the NETID value to the other network's Netid, and ACTION to "Allow"
CICSUR	Set the PLU value to "CICS", the SLU value to "UR%44*" and ACTION to "Allow"
CICSLOG	Set the PLU value to "CICS", the TYPE value to "THIRD-PARTY" and ACTION to "Allow"
CICSREQ	Set the PLU value to "CICS", the TYPE value to "PLU-REQ" and ACTION to "Allow"
LOCALS	Set the Netid value to your own netid, the Subarea value to your subarea value, and the SLU value to the pattern "A*", and ACTION to "Allow"
T77R992	Set the SLU value to "T77R992" and ACTION to "Allow"
OUTSIDE	Set ACTION to "Deny"

You would then create a Group called "COMPLEX" that references each Rule in the desired sequence. If you needed to reference the TSO based Rules in more than one grouping, you could collect the TSO oriented Rules them into Rulesets. (Breaking Rule definitions into Rulesets can be quite useful if you expect to create different combinations of Rules to respond to different processing requirements.)

The following figure demonstrates the collection the collection of the TSO, CICS, and local system oriented Rules into Rulesets:

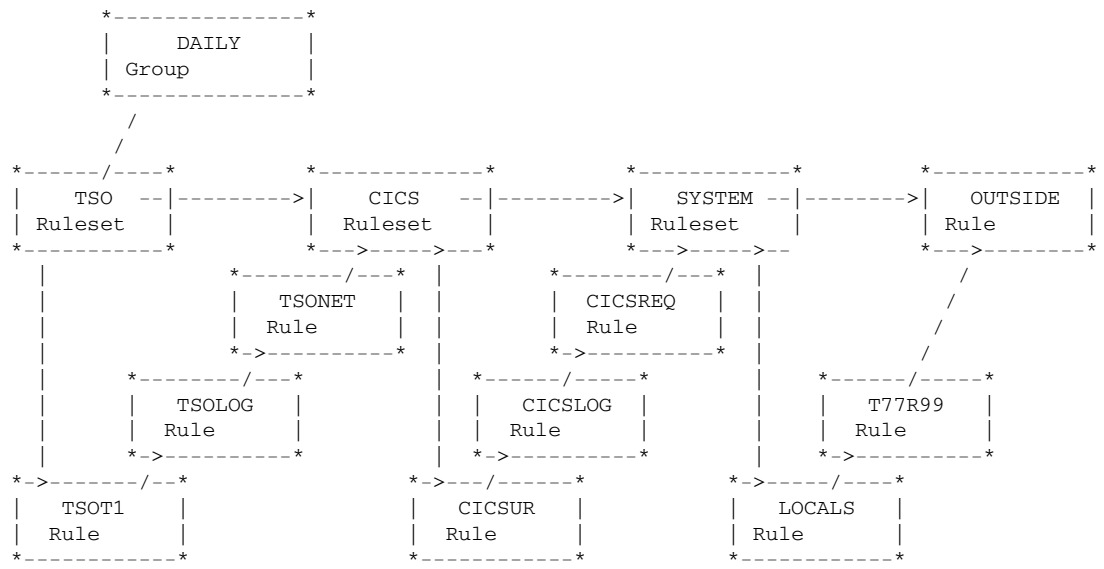

Figure 28. Complex Rule Hierarchy

The flexibility of Rulesets and Groups allows you to structure the defined Rules into an unlimited set of groupings that match the requirements at your installation.

Diagnosing Session Management Exit Information

When creating Access Rules, you may need to isolate the information that is available to the Access Session Management Exit (SME). You can produce this diagnostic information in the Message queue by activating a Rule with a the Option operand set to "Hexdump" or "Trace".

Note: The Message queue is available from the Administration menu; see the *Installation and Operations* (TNC-0003) manual for more information.

Hexdump

The **Hexdump** setting of the Option operand allows you to evaluate the parameter list that is passed to the SME from VTAM. When the Network Center uses a Rule with Hexdump in effect, it produces a series of TNC0245 messages in the following general format:

```
TNC0245N 01.00 0000  003C0A06 D5D9E240 40404040 0A07E2E2  * ....NRS     ..SS *
TNC0245N 01.00 0010  C3D7F140 40400A08 E5E3C1D4 F1404040  * CP1   ..VTAM1    *
TNC0245N 01.00 0020  08090000 00010000 0A0AD5D9 E2404040  * ..........NRS    *
TNC0245N 01.00 0030  40400A0B D5D9E240 40404040           *   ..NRS          *
TNC0245N 01.04 0000  01300000                             * ....             *
TNC0245N 01.08 0000  0026F770                             * ..7.             *
TNC0245N 01.12 0000  193D0AC0 08E2E2C3 D7F14040 4008D5D9  * ...{.SSCP1   .NR *
TNC0245N 01.12 0010  E2404040 404008C1 F0F1E5D4 40404008  * S     .A01VM   . *
TNC0245N 01.12 0020  D5D9E240 40404040 08C1F0F1 E5D44040  * NRS     .A01VM   *
TNC0245N 01.12 0030  401A0800 00000100 0700001A 001A00FF  *  ................ *
TNC0245N 01.16 0000  193D0A80 08E2E2C3 D7F14040 4008D5D9  * .....SSCP1   .NR *
TNC0245N 01.16 0010  E2404040 404008E3 F0F1F0F0 F6404008  * S     .T01006  . *
TNC0245N 01.16 0020  D5D9E240 40404040 08E3F0F1 F0F0F640  * NRS     .T01006  *
TNC0245N 01.16 0030  401A0800 00000100 5A00001A 001A00FF  *  .......!.......  *
TNC0245N 01.20 0000  EC77BE92 3AD870EA D5D9E24B E2E2C3D7  * ...k.Q..NRS.SSCP *
TNC0245N 01.20 0010  F1404040 40404040 40000000           * 1        ...     *
TNC0245N 01.56 0000  191F0000 08E2E2C3 D7F14040 4008D5D9  * .....SSCP1   .NR *
TNC0245N 01.56 0010  E2404040 404008C1 F0F1D7D9 D6C44000  * S     .A01PROD .  *
TNC0245N 01.56 0020  00000000                             * ....             *
TNA1002N Session approved between Slu T01006 and Plu A01PROD by rule LOGAPPL
TNA0245N CC.04 0000  CC000000
TNA0245N CC.08 0000  00000000
```

Each word in the parameter list points at a portion of storage, which is formatted in hexadecimal for placement into the Message Queue. This allows you to evaluate precisely what has been passed to Access. You can interpret these parameter list entries by referring to the VTAM *Customization* manual for your version of VTAM.

Trace

The **Trace** setting of the Option operand lets you evaluate the individual operand values associated with the session. When the Network Center uses a Rule with Trace in effect, it produces a series of messages in the following general format:

```
TNC0192W Rule: INPUT , Action: None , Start-date: 060508, End-date: , Day: Monday
TNC0193W ..PLU Name: A01VM , Adjsscp: , Alias: A01VM , Alias-net: NRS
TNC0194W ..PLU Netid: NRS , Sscpname: SSCP1 , Subarea: 00000001
TNC0195W ..PLU Hcvtype: 16, Hcvname: A01VM
TNC0195W ..PLU Hcvtype: 2, Hcvname: A01NRS
TNC0193W ..SLU Name: T01006 , Adjsscp: , Alias: T01006 , Alias-net: NRS
TNC0194W ..SLU Netid: NRS , Sscpname: SSCP1 , Subarea: 00000001
TNC0195W ..SLU Hcvtype: 22, Hcvname: T01006
TNC0195W ..SLU Hcvtype: 3, Hcvname: T01L
TNC0196W ..From:A01PROD, Mode:None, Start-time:09:42, End-time:, Type:Third-party
```

The information is similar to that in Hexdump, but is presented in a more readable format (Trace does not require that you parse the hexadecimal information displayed by Hexdump).

Chapter 4. Planning for Access Implementation

The Access Component's flexible design provides for maximum control over session establishment within the local domain. However, due to this flexibility, we recommend planning and testing your Rules prior to active implementation. Planning and testing can help you to avoid denying sessions that should be allowed and to avoid allowing sessions that should be denied.

This chapter covers planning tasks including identifying which applications need access to particular resources and whether particular applications should be denied access to particular resources. It also helps you to organize your findings into Rules and/or Rulesets and to set the Rules into a Rule processing order. You can use much of the information to help build a Rule plan that is easily implemented online.

Topics include:

- "Establishing Rule Criteria and Requirements".
- "Example Rule Arrangements" on page 50.
  "Example Network Rules" on page 69.
- "Rule Definition Worksheet" on page 81.
- "Group Definition Worksheet" on page 83.

Note: Testing your Rules is also an important resource in planning for implementation. See "Testing Rules" on page 124 for more information.

Establishing Rule Criteria and Requirements

Before creating Rules, you should evaluate the access requirements for your domain and decide which sessions should be allowed or denied establishment. We recommend doing the following:

- Evaluate your network for sessions that need to be allowed, remembering that if you do not create a Rule that allows establishment, the session will automatically be denied establishment.
- Consider the types of conditions under which you would like to control session establishment. You can use a combination of Rule conditions, based on Rule operands. Some of these conditions are explained in "Example Rule Arrangements" on page 50.
- Create a Rule that denies all of the sessions that you do not want to allow. Although it is not necessary (Access automatically denies session establishment for sessions that do not match any of the active Rules), it will cause Access to log the information so that you can view these sessions as well.

- Before activating any Rules, follow the guidelines in "First Time Implementation" on page 85.

Example Rule Arrangements

The following simple examples show how you can use Rules to express your installation's requirements. Examples of requirements include conditions like time, day, and date restrictions or application access requirements. (Assume that each of the following example Rule arrangements contains the complete active Rule list for an executable domain with Access in MODE=ACTIVE; see "Activating Rules" on page 115 for more information.)

Device Controls

You can base session authorization around a device's name (LUNAME). For example, the following Rule allows any terminal device with an "A" in the second byte of its name to go into session with any subsystem. Any device without this pattern in the luname is denied session access:

```
LOCALS TNCRULE SLU=%A*,ACTION=ALLOW
```

Now, assume that a specific control unit in the Accounts Payable department needs to access your production CICS system. You would simply add a Rule that allows access for the control unit's devices:

```
LOCALS  TNCRULE SLU=%A*,ACTION=ALLOW
PAYABLE TNCRULE SLU=PY*,ACTION=ALLOW,PLU=DBDCCICS
```

Now, devices that start with "PY" are allowed to go into session with DBDCCICS.

The LOCALS Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:29:23        User: EXAMPLE        Version: 2.0.0

Name . . . . LOCALS__                   Title CICS_access_for_Accounts_pay
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)  . %A*_____
. . Adjsscp  *_______
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 29. LOCALS Rule Panel

The PAYABLE Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:30:38        User: EXAMPLE        Version: 2.0.0

Name . . . . PAYABLE_                  Title Access_for_Accounts_Payable_
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . DBDCCICS      . . 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)  . PY*_____
. . Adjsscp  *_______
--------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 30. PAYABLE Rule Panel

Controlling Applications

Many installations use a VTAM front end processor (a Network Management System such as The Network Director) to control which subsystems an individual device can access. The following Rules support Network Management Systems:

```
LOGAPPL TNCRULE PLU=TND,TYPE=AUTOLOGON,ACTION=ALLOW
```

This Rule allows devices to enter a session only with a subsystem identified to VTAM as "TND". The SLU operand has been left at the default asterisk (*), signifying that the Rule is based on session "TYPE" rather than the device name. TYPE=AUTOLOGON indicates that sessions will be approved if they were initiated as a result of VTAM's LOGAPPL specification or a VARY NET,LOGON= operator command.

If we presume that "TND" is a controlling application that will, in turn, control which sessions may be established, we simply create an additional Rule, called TND, that allows TND to establish these sessions:

```
LOGAPPL TNCRULE PLU=TND,TYPE=AUTOLOGON,ACTION=ALLOW
TND     TNCRULE PLU=T*,TYPE=THIRD-PARTY,FROM=TND
```

The TND Rule indicates that Access should allow sessions to be established to any subsystem that starts with a "T" **only if** they were immediately preceded by a session with the subsystem "TND". Typically, the subsystem known as TND will be issuing a VTAM CLSDST PASS type operation to start the session.

The LOGAPPL Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:31:47        User: EXAMPLE        Version: 2.0.0

Name . . . . LOGAPPL_                   Title Access_to_TND_______________
Count  . . .
Action . . . Allow____    . . Alias  . *_______
Date. .first *_____       . . Aliasnet *_______
. . . . last *_____       . . Hcvname. *_______
Day  . . . . *________    . . Hcvtype. 0_
Dlu (Plu)  . TND_____     . . 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 31. LOGAPPL Rule Panel

The TND Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:33:24        User: EXAMPLE        Version: 2.0.0

Name . . . . TND_____                  Title Access_for_T*_subsystems____
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . T*______      . . 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 . . . . TND_____      Session type Third-party
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 32. TND Rule Panel

Defining TSO

z/OS installations using the Time Sharing Option (TSO) operate an address space known as **TCAS**. TCAS typically operates as a VTAM subsystem with the APPLID of TSO. To start a TSO session, TCAS creates an address space and then passes control to TSO.

The following Rules allow this procedure to occur in an environment that is tightly controlled by a Network Management system:

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

The TCAS Rule allows the subsystem known as TND to pass ownership of a device to TCAS. The TSO Rule allows TCAS to pass ownership of the device to the TSO address space created for the user (this, of course, presumes the address spaces created by TCAS will all start with "TSO0").

The LOGAPPL panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:31:47        User: EXAMPLE         Version: 2.0.0

Name . . . . LOGAPPL_                   Title Access_to_TND_______________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . TND_____      . . 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 33. LOGAPPL Rule Panel

The TCAS Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 13:35:00        User: EXAMPLE        Version: 2.0.0

Name . . . . TCAS____                  Title Access_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 . . . . TND_____     Session type Third-party
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
-------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 34. TCAS Rule Panel

The TSO Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:36:31        User: EXAMPLE        Version: 2.0.0

Name . . . . TSO_____                   Title Access_to_TSO_______________
Count  . . .
Action . . . Allow____    . . Alias  . *_______
Date. .first *_____       . . Aliasnet *_______
. . . . last *_____       . . Hcvname. *_______
Day  . . . . *________    . . Hcvtype. 0_
Dlu (Plu)  . TSO0*___     . . 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 35. TSO Rule Panel

Defining VSCS

For z/VM installations using VSCS to create virtual consoles, a VTAM subsystem known as VSCS operates in the GCS virtual machine with VTAM.

The following Rules allow this procedure to occur in an environment tightly controlled by a Network Management system:

```
LOGAPPL TNCRULE PLU=TND,TYPE=AUTOLOGON,ACTION=ALLOW
TND     TNCRULE TYPE=THIRD-PARTY,FROM=TND
*  VSCS    TNCRULE PLU=VM
```

The TND Rule allows the subsystem known as TND to pass ownership of any device to any other defined VTAM subsystem (including VSCS). The commented VSCS Rule would permit any device to enter session with VSCS, if it was activated.

The LOGAPPL panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:31:47        User: EXAMPLE        Version: 2.0.0

Name . . . . LOGAPPL_                   Title Access_to_TND_______________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . TND_____      . . 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 36. LOGAPPL Rule Panel

The TND Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 13:37:51        User: EXAMPLE        Version: 2.0.0

Name . . . . TND_____                  Title Access_from_TND_____________
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 . . . . TND_____     Session type Third-party
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 37. TND Rule Panel

The VSCS Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 13:39:22        User: EXAMPLE        Version: 2.0.0

Name . . . . VSCS____                  Title Access_to_VSCS_____________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . VM______      . . 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 38. VSCS Rule Panel

Controlling Via Time or Day Intervals

Besides "Device Controls" (see "Device Controls" on page 50) and "Controlling Applications" (see "Controlling Applications" on page 52), you can use any Rule condition or combination of conditions to control access authority. The following Rules control access authority based on time and day intervals:

```
SLUPAY   TNCRULE PLU=PAYCICS,TYPE=SLU-REQUEST,ACTION=DENY
MONDAYS  TNCRULE PLU=PAYCICS,DAY=MONDAY,ACTION=ALLOW
PAYROLL  TNCRULE PLU=PAYCICS,TIME=(07:30,17:59),DAY=WEEKDAYS
```

Access would evaluate these Rules from the first defined Rule to the last defined Rule (in other words, from the top to the bottom). (In order for specific Rule to apply to a session, all of the session's characteristics must match the Rule's operands. If a Rule does not apply, Access evaluates the next Rule.)

This process would cause the SLUPAY Rule to reject any sessions requested from a device for the PAYCICS system (in other words, the device may not issue a LOGON APPLID(PAYCICS) request). If the session request was not initiated by a device, Access would move to the "MONDAYS" Rule.

If it were a Monday, Access would allow the session to proceed. If it were not a Monday, Access would move to the PAYROLL Rule. The PAYROLL Rule would allow access if the session were requested on a normal workday (MONDAY through FRIDAY) between 7:30 am and 5:59 pm. If none of the Rules match the session conditions, Access would reject the session request.

The SLUPAY Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 13:40:31        User: EXAMPLE        Version: 2.0.0

Name . . . . SLUPAY__                   Title Deny_SLU_Request_for_SLUPAY_
Count  . . .
Action . . . Deny_____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . PAYCICS_      . . 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 SLU-request
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
-----------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 39. SLUPAY Rule Panel

The MONDAYS Rule panel would appear as follows:

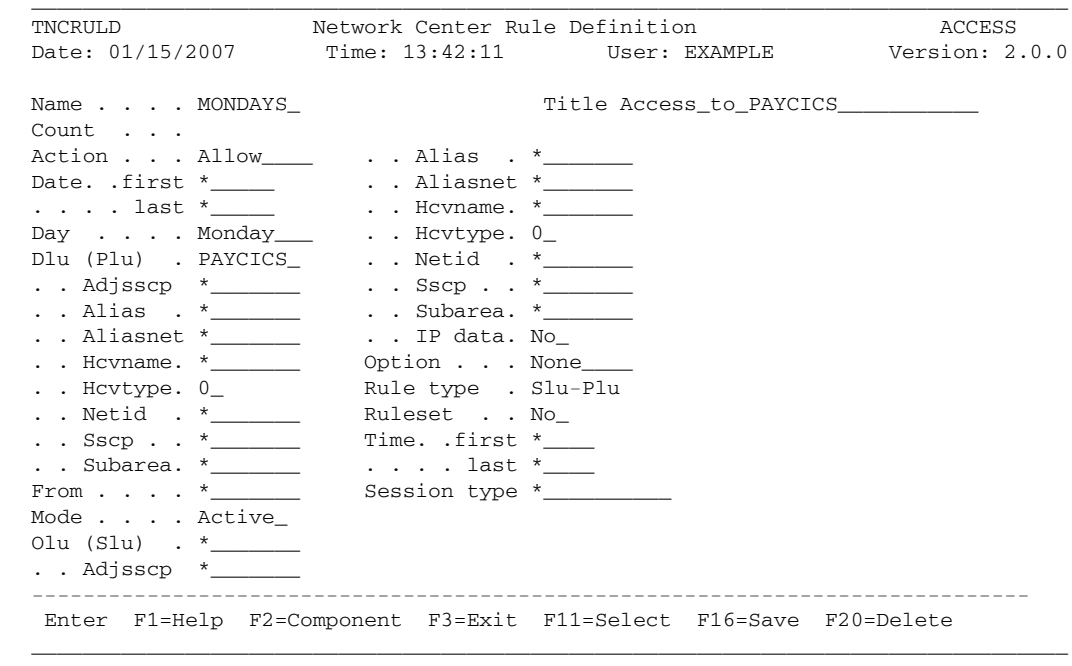

Figure 40. MONDAYS Rule Panel

The PAYROLL panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 16:58:48        User: EXAMPLE        Version: 2.0.0

Name . . . . PAYROLL_                  Title Weekday_access_to_PAYCICS___
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . Weekdays_     . . Hcvtype. 0_
Dlu (Plu)  . PAYCICS_      . . Netid  . *_______
. . Adjsscp  *_______      . . Sscp . . *_______
. . Alias  . *_______      . . Subarea. *_______
. . Aliasnet *_______      . . IP data. No_
. . Hcvname. *_______      Option . . . None____
. . Hcvtype. 0_            Rule type  . Slu-Plu
. . Netid  . *_______      Ruleset  . . No_
. . Sscp . . *_______      Time. .first 07:30
. . Subarea. *_______      . . . . last 17:59
From . . . . *_______      Session type *__________
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
--------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 41. PAYROLL Rule Panel

Controlling Network Origins

Many installations are cross-domain or cross-network to other host processors. You can create Access Rules that control these portions of the network with the network identifier (NETID) or with the subarea identifier (SUBAREA). Consider the following Rules:

```
INFOTSO  TNCRULE SLUNETID=INFO,PLU=TSO*,ACTION=ALLOW
INFONET  TNCRULE SLUNETID=INFO,ACTION=DENY
HDQTRS   TNCRULE SLUSUBA=1,SLUNETID=NRS,TYPE=AUTOLOGON,PLU=TND
TND      TNCRULE TYPE=THIRD-PARTY,FROM=TND
MYSITE   TNCRULE SLUSUBA=3,SLUNETID=NRS,PLU=*,ACTION=ALLOW
```

The INFOTSO Rule provides devices that originate from the "INFO" network with access to any subsystem that starts with "TSO". The INFONET Rule will deny any other request from a device in that network.

The HDQTRS Rule provides access to a controlling subsystem identified as "TND", provided that the session is a result of LOGAPPL and that the SLUSUBA and SLUNETID match. The TND Rule allows the controlling subsystem to forward the device anywhere it chooses.

Finally, the MYSITE Rule allows any device within my network (SLUSUBA 3, SLUNETID NRS) to enter into a session with any subsystem it chooses.

The INFOTSO Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:04:36        User: EXAMPLE        Version: 2.0.0

Name . . . . INFOTSO_                   Title Access_for_INFO_to_TSO______
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . TSO*____      . . Netid  . INFO____
. . 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 42. INFOTSO Rule Panel

The INFONET Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:05:51        User: EXAMPLE        Version: 2.0.0

Name . . . . INFONET_                   Title Deny_all_other_INFO_requests
Count  . . .
Action . . . Deny_____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . *_______      . . Netid  . INFO____
. . 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 43. INFONET Rule Panel

The HDQTRS Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:07:25        User: EXAMPLE        Version: 2.0.0

Name . . . . HDQTRS__                   Title Access_to_TND_______________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . TND_____      . . Netid  . NRS_____
. . Adjsscp  *_______      . . Sscp . . *_______
. . Alias  . *_______      . . Subarea. 00000001
. . 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 44. HDQTRS Rule Panel

The TND Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 17:08:26        User: EXAMPLE        Version: 2.0.0

Name . . . . TND_____                   Title Access_from_TND_____________
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 . . . . TND_____     Session type Third-party
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 45. TND Rule Panel

The MYSITE Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:10:24        User: EXAMPLE        Version: 2.0.0

Name . . . . MYSITE__                   Title Access_for_MYSITE___________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . *_______      . . Netid  . NRS_____
. . 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 46. MYSITE Rule Panel

Example Network Rules

The following example network demonstrates how to evaluate and plan Access Rules. It consists of primarily two domains, called Subarea 12 and Subarea 13, within the single network NRS; of a second network called FIRMB; and of additional unidentified subareas, domains, and networks. The following figure illustrates the example network:

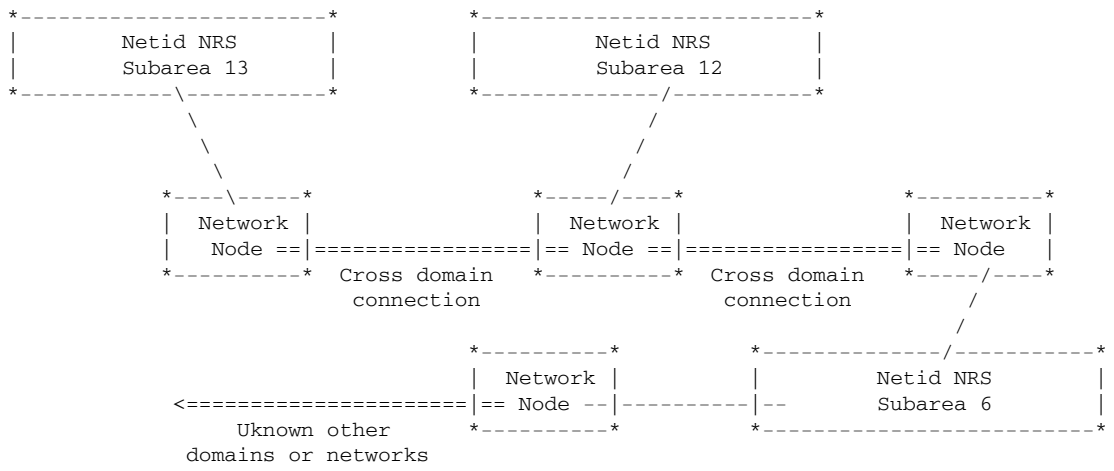

Figure 47. Example Network

For these examples, assume that you are installing Access into Subarea 12 (a simulated mainframe), which has defined the systems programmer's devices starting with the letter "S" and printer type devices (3286s, etc.) with the letter "P".

You should also assume that while evaluating sessions in the example network, you recognized that devices defined and owned by the local domain are forced to logon to the domain via a VTAM "front end" subsystem (the Network Director) prior to gaining access to the domain. The front end is a CLDST PASS type network manager and is the primary logical control point for userid and password validation.

You also know that the host domain is operating several VTAM subsystems, but specific situations require that special handling occur for TSO and CICS. Additionally, you wish to grant off hour and weekend access privileges to your systems programming staff.

The following table expresses the requirements for the example network:

Administrative			Session Criteria					
Rule name	**Title**	**Action**	**PLU**	**SLU**	**Netid**	**Subarea**	**From**	**Session Type**
Logappl	The Network Director	Allow	Director					
Director	Director Validated	Allow					Director	Third Party
TSO	Time Sharing Option	Allow	TSO		NRS	12		
TCAS	TSO Controller	Allow	TSO*				TSO	Third Party
Hdqtrs	TSO for Company B	Allow	TSO		FIRMB			
CICS	Inventory Subsystem	Allow	CICS*		NRS			
IPdevices	IP devices	Allow	CICS*		FIRMB			
Printers	Remote printers	Allow		P*				Plu-req
Systems	System Programming	Allow		S*	NRS	12		
Outside	All other combinations	Deny						

Note: Empty or unspecified fields indicate that the default value for the field is acceptable. For "Session Criteria" fields, the default is the asterisk (*) pattern matching character, which allows any value to match.

The remainder of this section discusses each example Rule in detail.

Logappl

The **Logappl** Rule defines the VTAM front end processing subsystem (in this case, "The Network Director"). All of the devices in the domain are LOGAPPLed to this subsystem and outside devices (originating from other VTAM domains) may request the services of this subsystem.

As a result, the **Logappl** Rule generally allows any type of session to proceed that includes a PLU of "Director". There are no additional restrictions and any device from anywhere in the network can successfully establish a session.

The Logappl Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:11:50        User: EXAMPLE        Version: 2.0.0

Name . . . . LOGAPPL                    Title The_Network_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 *__________
Mode . . . . Active_
Olu (Slu)  . *________
. . Adjsscp  *________
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 48. Logappl Example Network Rule

Director

Once connected to the Director subsystem, the device operator will be required to sign on to the system via the security system (ACF2, RACF, TOPSECRET, etc.). The front end subsystem will then present a menu of subsystems that are authorized for the terminal user. (Assuming that the front end program has been configured to provide these services. Access does not verify that the front end has actually done this processing, but is simply enforcing the Rules.)

The **Director** Rule allows this because the "Director" APPL name is coded in the From field and Third-Party is present in session Type.

The DIRECTOR Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:11:50        User: EXAMPLE        Version: 2.0.0

Name . . . . DIRECTOR                   Title Director_Validated__________
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 49. DIRECTOR Example Network Rule

TSO

Even though the Logappl Rule will allow the Director subsystem to forward ownership, there are devices in the network that should be allowed to go into session with TSO even if the front end subsystem is not operational. The **TSO** Rule indicates that any device in your network (NRS) and subarea (12) can request the subsystem named TSO.

The TSO Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 17:12:34        User: EXAMPLE        Version: 2.0.0

Name . . . . TSO_____                  Title Time_Sharing_Option_________
Count  . . .
Action . . . Allow____    . . Alias  . *_______
Date. .first *_____       . . Aliasnet *_______
. . . . last *_____       . . Hcvname. *_______
Day  . . . . *________    . . Hcvtype. 0_
Dlu (Plu)  . TSO_____     . . Netid  . NRS_____
. . Adjsscp  *_______     . . Sscp . . *_______
. . Alias  . *_______     . . Subarea. 00000012
. . 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 50. TSO Example Network Rule

TCAS

Technically, the subsystem identified as TSO to VTAM is actually a subsystem called TCAS. TCAS creates the actual TSO address space that will be used to support the TSO user. After TCAS goes through address space creation, it will CLSDST PASS ownership of the device to the newly created address space.

To enable this process to occur, you must authorize TCAS to perform this operation. The **TCAS** Rule authorizes this activity. This Rule will be applied by Access whether the initial session with TCAS was established as a result of the TSO or Logappl Rule.

The TCAS Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:15:39        User: EXAMPLE        Version: 2.0.0

Name . . . . TCAS____                   Title TSO_Controller_______________
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 51. TCAS Example Network Rule

Hdqtrs

The TSO Rule provides access to your TSO system for devices in your own network, but will not honor attempts to use TSO from other systems that may be interconnected with yours. The **Hdqtrs** Rule specifically authorizes devices that originate from the Network known as FIRMB to have access to your TSO subsystem.

This allows FIRMB based devices to directly connect to TSO by issuing an Unformatted System Services or equivalent request (E.G. "LOGON APPLID(TSO)").

The HDQTRS Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:17:11        User: EXAMPLE         Version: 2.0.0

Name . . . . HDQTRS__                   Title TSO_for_Company_B___________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . TSO_____      . . Netid  . FIRMB___
. . 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 52. HDQTRS Example Network Rule

CICS

The **CICS** Rule provides a facility similar to the TSO Rule, in that a specific set of devices can use a particular subsystem. In this case, devices from your network can directly use the services of any subsystem on your host whose APPL name begins with "CICS".

The CICS Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:18:21        User: EXAMPLE        Version: 2.0.0

Name . . . . CICS____                   Title Inventory_Subsystem_________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . CICS*___      . . 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)  . *_______
. . Adjsscp  *_______
-------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 53. CICS Example Network Rule

IPdevice

The CICS Rule allows local users to access the CICS subsystem. The **IPdevice** Rule allows specific IP devices from the FIRMB network to access the local CICS subsystem between 8:00am to 5:00pm. Upon activation, the IPdevice Rule would provide data in the Message Queue on the specific devices allowed access to CICS.

The IPdevice Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:26:11        User: EXAMPLE         Version: 2.0.0

Name . . . . IPDEVICE                  Title IP_Devices____________________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . CICS*___      . . Netid  . FIRMB___
. . Adjsscp  *_______      . . Sscp . . *_______
. . Alias  . *_______      . . Subarea. *_______
. . Aliasnet *_______      . . IP data. Yes
. . Hcvname. *_______      Option . . . None____
. . Hcvtype. 0_            Rule type  . Slu-Plu
. . Netid  . *_______      Ruleset  . . No_
. . Sscp . . *_______      Time. .first 08:00
. . Subarea. *_______      . . . . last 17:00
From . . . . *_______      Session type *__________
Mode . . . . Active_
Olu (Slu)  . *_______
. . Adjsscp  *_______
-----------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 54. IPdevice Example Network Rule

The IP Data Display/Update window would appear as follows:

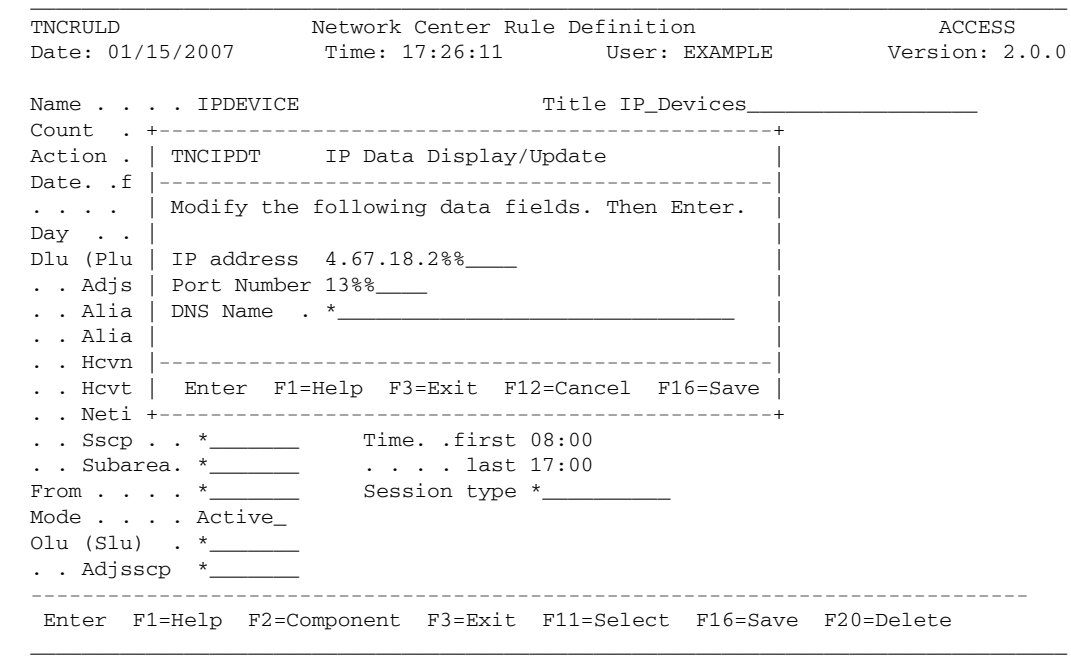

Figure 55. IPdevice Example Network IP Data Update Window

Printers

During execution, many of the subsystems in the hypothetical domain use the services of 328x type printers connected throughout the network. You can identify them by their LU name (they all begin with a "P").

The **Printers** Rule allows any subsystem on your host to obtain a session with a printer. Please note that this Rule is not restricted by Netid or Subarea, which implies that any subsystem can actually request a session with any device anywhere in the network that begins with a "P". As a result, you should carefully determine whether this will constitute a security breach or if the result is as desired.

If the naming convention for your "printers" is not easily pattern matched, consider using a Value Group (E.G. &PRINTER). See "Value Groups: Creating Symbolic Rule Operand Values" on page 29 for more information.

The PRINTERS Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:30:08        User: EXAMPLE        Version: 2.0.0

Name . . . . PRINTERS                  Title Remote_Printers_____________
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 PLU-request
Mode . . . . Active_
Olu (Slu)  . P*______
. . Adjsscp  *_______
--------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 56. PRINTERS Example Network Rule

Systems

This Rule allows devices in our subarea and network that start with the letter "S" to go into session with anything they like. It is an example of the type of authorization that may be required by the network maintenance personnel themselves.

The SYSTEMS Rule panel would appear as follows:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:31:22        User: EXAMPLE        Version: 2.0.0

Name . . . . SYSTEMS_                   Title System_Programming__________
Count  . . .
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . *_______      . . Netid  . NRS_____
. . Adjsscp  *_______      . . Sscp . . *_______
. . Alias  . *_______      . . Subarea. 00000012
. . 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)  . S*______
. . Adjsscp  *_______
------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 57. SYSTEMS Example Network Rule

Outside

The "Outside" Rule causes any session that does not match the previous Rules to be rejected. You could simply leave this Rule out and Access would automatically reject the session because no other Rule permits it. However, by naming this specific Rule, the Message queue and output log will more clearly let you know what has occurred.

The OUTSIDE Rule panel would appear as follows:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 17:32:35        User: EXAMPLE        Version: 2.0.0

Name . . . . OUTSIDE_                   Title All_other_combinations______
Count  . . .
Action . . . Deny_____     . . 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 58. OUTSIDE Example Network Rule

Rule Definition Worksheet

After establishing which sessions will or will not receive access to your network resources, you are ready to create the Rules. The Rule Worksheet emulates the Rule definition panel: it contains all of the same operands, but organizes them into three sections, allowing you to "see" your Rule before you define it online:

- The first section, "Administrative", contains the operands that name the Rule and control when and how it is processed.
- The second section, "Session Criteria" establishes the exact session criteria that must be present in order for the Rule to be used (all the operands must match).
- The third section, "Rule list", provides an area to write down the names of the Rules that the Rule defines if it is a Ruleset Rule.

The asterisk pattern-matching character (*) is the default for each operand, with the exception of Name, Title, Action, Hcvtype, Mode, Option, Rule type, and Ruleset. It indicates that all values for the field match. See "Rule Operand Definitions" on page 10 for more information.

Administrative			
Name:	Ruleset (select one): Yes No	Action (select one): Allow Deny	From:
Title:		Day:	
Mode (select one): Active Dormant Warn Test	Option (select one): Hex None Suppress Trace	Time first:	Time last:
Session type (select one): * Autologon Plu-request Slu-request Third-party Rd-search		Date first:	Date last:
Session Criteria			
OLU (SLU):		**DLU (PLU):**	
Adjsscp:	Hcvtype:	Adjsscp:	Hcvtype:
Alias:	Netid:	Alias:	Netid:
Aliasnet:	Sscp:	Aliasnet	Sscp.
Hcvname	Subarea	Hcvname	Subarea
IP data (select one): Yes No			
IP Data (If you are entering IP data, define the following data fields. You may use pattern-matching characters):			
IP address:			
Port Number:			
DNS Name:			
Rule list (If this is a Ruleset, write the names of the Rules it defines in the blanks below according to their processing order. The actual Rule list panel provides additional space):			
1.	2.	3.	4.	5.	6.
7.	8.	9.	10.	11.	12.

Group Definition Worksheet

If you define more than one Rule or Ruleset, you should place them into a Rule Group to set their processing order (see "Specifying the Active Rules" on page 115). The Rule Group worksheet allows you to plan how to set the Rules, Rulesets, and/or Groups into order.

Note: See "Rule Groups" on page 25 for a description and examples of Groups.

Note: See "Defining a Rule Group" on page 105 for online Group definition procedures.

Group name	**Group title**		
Rule, Ruleset, or Group name			
1.	14.	27.	40.
2.	15.	28.	41.
3.	16.	29.	42.
4.	17.	30.	43.
5.	18.	31.	44.
6.	19	32.	45.
7.	20.	33.	46.
8.	21.	34.	47.
9.	22.	35.	48.
10.	23.	36.	49.
11.	24.	37.	50.
12.	25.	38.	51.
13.	26.	39.	52.

Figure 59. Group Worksheet

Chapter 5. Implementing Access

This chapter guides you in implementing Access using the Network Center Interface. It demonstrates how to define and modify Rules, how to set the Rule processing order, and how to activate the Rules. It also discusses Rule-testing methods.

You can use the sections in this chapter as individual procedures, but they are organized for you to use step-by-step as you define and activate one or more Rules. Topics include:

Note: See the *User's Guide* (TNC-0002) for selection techniques, field entry methods, function key and common dialog actions, menu shortcut commands, and navigational techniques.

First Time Implementation

You should proceed cautiously when first implementing Access. Likely, you will discover sessions occurring between network elements that you didn't realize were occurring before. You may also discover that the Access Session Management Exit receives control during session establishment in some relatively surprising situations.

We recommend taking the following precautions:

- Review "Chapter 4. Planning for Access Implementation" on page 49
- Set an "OUTSIDE" Rule such as in "Example Network Rules" on page 69 with the Option operand set to TRACE. When a rule in TRACE mode matches a particular session, Access will automatically include detailed messages in the Message Queue that show the exact criteria that was in effect for the session (see the *Installation and Operations* manual (TNC-0002) for information on the Message Queue). This enables you to evaluate the

conditions that exist when a session is rejected and to determine the type of Rule that should be written to handle the situation. You can use this information to refine your Rule structure.

- Set the MODE=WARN in the Component Options record (see "Specifying the Active Rules" on page 115). This ensures that sessions are not erroneously rejected if you did not establish a Rule to handle them. When you have established that the Rule structure is operating as planned, you can set the MODE=ACTIVE.
- Check the Message queue for trace level messages (internal messages TNC0192 through TNC0196); they contain the information used by the Access Rule processor to determine if the session should be allowed or denied.
- Test your Rules and Rule hierarchy before full activation (see "Testing Rules" on page 124). Testing allows you to ascertain how the Rules function in your system and whether or not they are effective.

Rule Definition Summary

This section briefly summarizes the basic steps for defining and activating an Access Rule:

1. Define the desired Rules, including any Rulesets, using the 'Rule definition' choice (see "Defining Rules and Rulesets" on page 90).
2. If you have defined more than one Rule or Ruleset, place them into the order that they should be processed by creating a Rule Group. This function is available from the 'Group definition' choice (see "Defining a Rule Group" on page 105).
3. Test the Rules using the 'Rule test' choice (see "Testing Rules" on page 124).
4. Define the Rule, Ruleset, or Group that you wish to be the active entity in the 'Component options' function (see "Specifying the Active Rules" on page 115).
5. Activate this Rule, Ruleset, or Group using the 'Rule reload' function (see "Reloading Rules" on page 118).

Opening the Access Menu

The "Access Component Administration" menu panel provides a base for all Rule definition and maintenance procedures.

To open the menu:

1. Logon to TSO or CMS.
2. Start a session with Access by entering one of the following commands:
   - For TSO, enter "TNCENTER" (TSO CLIST)
   - For CMS, enter "TNCENTER" (CMS Command)

The Network Center LOGO panel appears:

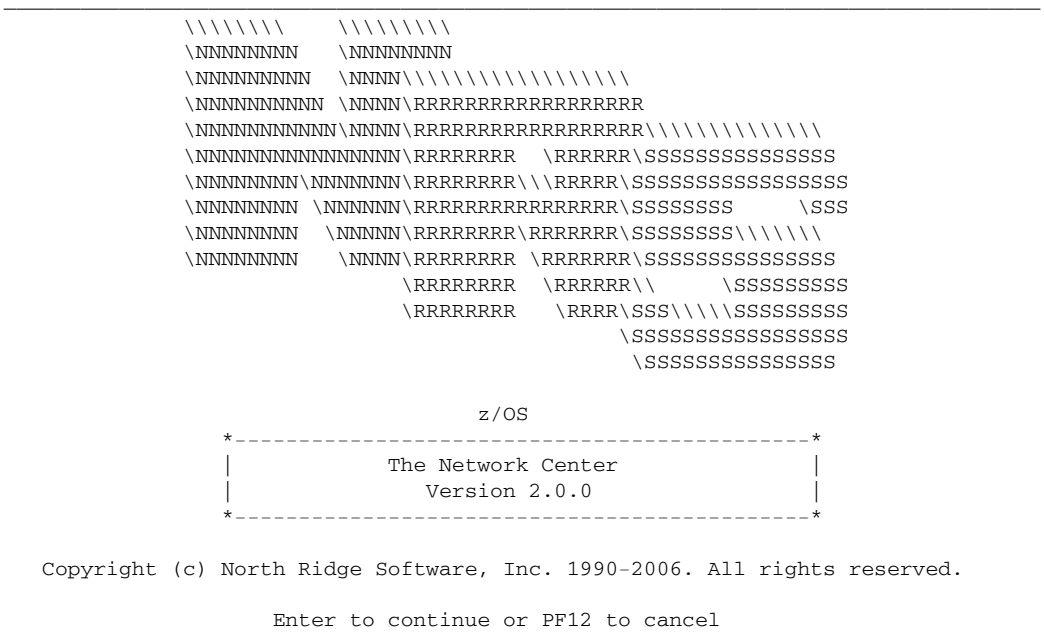

Figure 60. Network Center LOGO Panel

3. Press Enter to clear the logo panel and open the main Network Center menu (TNCMENU):

```
  Options  Exit  Help
--------------------------------------------------------------------------------
TNCMENU                        The Network 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.  Administration
     2.  Access
     3.  Alias
     4.  Query
     5.  Ruletest
     6.  Select
     7.  Timeout









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

Figure 61. The Network Center Menu Panel (TNCMENU)

4. Open the Access Administration menu panel by placing the cursor on the 'Access' choice and pressing Enter:

```
  Options  Exit  Help  Component
-------------------------------------------------------------------------------
TNCADMC              Access Component Administration                 ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 62. Access Component Administration Panel (TNCADMC)

If the 'Access' choice appears blue or low intensity, you are not authorized to administer Access. Contact the Network Administrator.

Note: See the *User's Guide* (TNC-0002) for information on using the Network Center Interface.

Defining Rules and Rulesets

After opening the Access Component Administration menu, you can start defining Rules and/or Rulesets using the 'Rule definition' function.

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

    1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 63. Access Component Administration Menu (TNCADMC)

2. Select choice 6, 'Rule definition' to open the Network Center Rule Definition panel:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                 ACCESS
Date: 01/15/2007       Time: 16:58:48        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 64. Network Center Rule Definition panel (TNCRULD)

3. Define the operand fields, starting with the 'Name' and 'Title'. The following example shows a defined Rule panel:

```
_____________________________________________________________________________
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 14:40:16        User: EXAMPLE        Version: 2.0.0

Name . . . . DIRECTOR                   Title The_Network_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 *__________
Mode . . . . Active_
Olu (Slu)  . *________
. . Adjsscp  *________
-------------------------------------------------------------------------------
Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
_____________________________________________________________________________
```

Figure 65. Sample Network Center Rule Definition

Note: We recommend setting the 'Mode' field to "warn" until you have determined the Rule's effect on your system. See "Rule Operand Definitions" on page 10 for more information.

To define IP data:

If you wish to include IP devices in the Rule, type "yes" in the IP data field. Then, keeping the cursor pointed at the IP data field, press F11 (Select) to open the IP Data Display window:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 15:07:11        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  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 66. IP Data Display Window

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 or Value groups (see "Using Value Groups to Specify IP Data" on page 34).

After entering the data, press F16 (Save) to save the changes and return to the Rule definition panel. See "Rule Operand Definitions" on page 10 for more information on the IP Data Display fields.

To define a Ruleset:

If you are defining a Ruleset, press the F11 (Select) key; the Ruleset function prompt appears:

```
TNCRULD                Network Center Rule Definition                    ACCESS
Date: 01/15/2007        Time: 15:15:25        User: EXAMPLE         Version: 2.0.0
                       +---------------------------------+
Name . . . . DIRECTOR | TNCDELT  Ruleset function       | rk_Director__
Count  . . .          |---------------------------------|
Action . . . Allow___ | _ 1. Display ruleset list       |
Date. .first *_____   |   2. Resume current function.   |
. . . . last *_____   |---------------------------------|
Day  . . . . *_______ |  F12=Cancel                     |
Dlu (Plu)  . DIRECTOR +---------------------------------+
. . 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  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 67. Ruleset Prompt

Select choice 1, 'Display Ruleset List'; the Ruleset Rule Name List panel appears:

```
TNCRNAM                 Ruleset Rule Name List                      ACCESS
Date: 01/15/2007       Time: 15:18:35        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 68. Ruleset Rule Name List Panel (TNCRNAM)

Note: You can also open the Ruleset Rule Name List by entering 'yes' in the "Ruleset" field. An additional field, called "Select" will appear next to the Ruleset field. Enter any keyboard character into the Select field; the Ruleset Rule Name List will then appear.

In the numbered fields, enter the names of the Rules that the Ruleset will contain according to their processing order. The following figure shows an example:

```
TNCRNAM                  Ruleset Rule Name List                      ACCESS
Date: 01/15/2007       Time: 15:18:35        User: EXAMPLE        Version: 2.0.0

  1. DIRECT01        20. ________        39. ________        58. ________
  2. DIRECT02        21. ________        40. ________        59. ________
  3. DIRECT03        22. ________        41. ________        60. ________
  4. DIRECT04        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 69. Ruleset Rule Name List Example

After entering the Rule and/or Ruleset names, press F3 (Exit) to save the Ruleset Rule Name List and exit the panel; a window prompt appears:

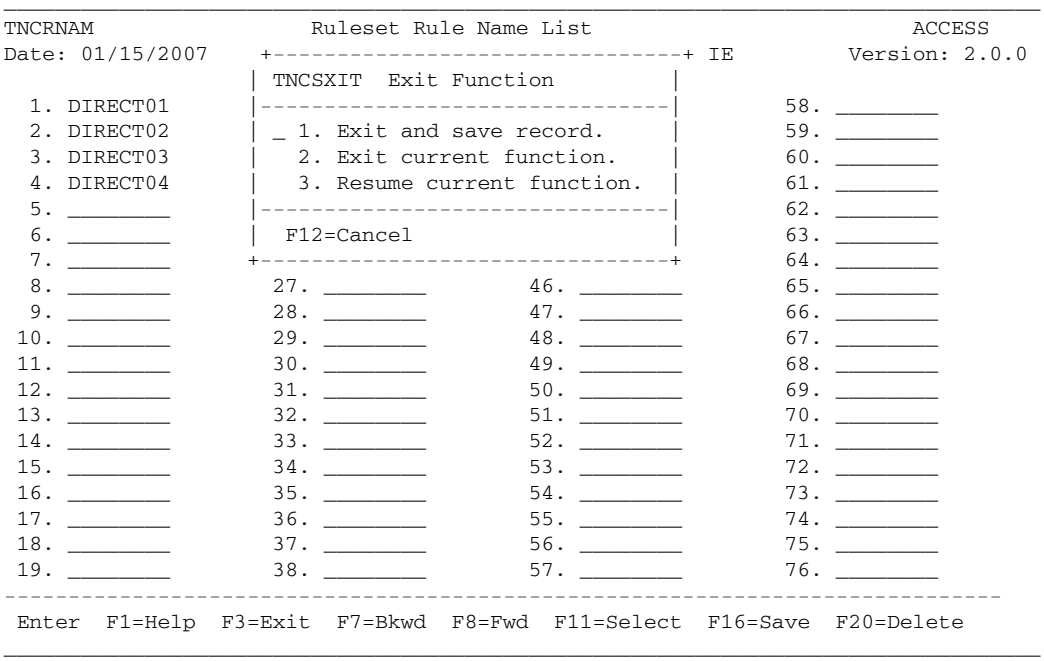

Figure 70. Ruleset Rule Name List Prompt

Select choice 1, 'Exit and save record'; a confirmation message appears:

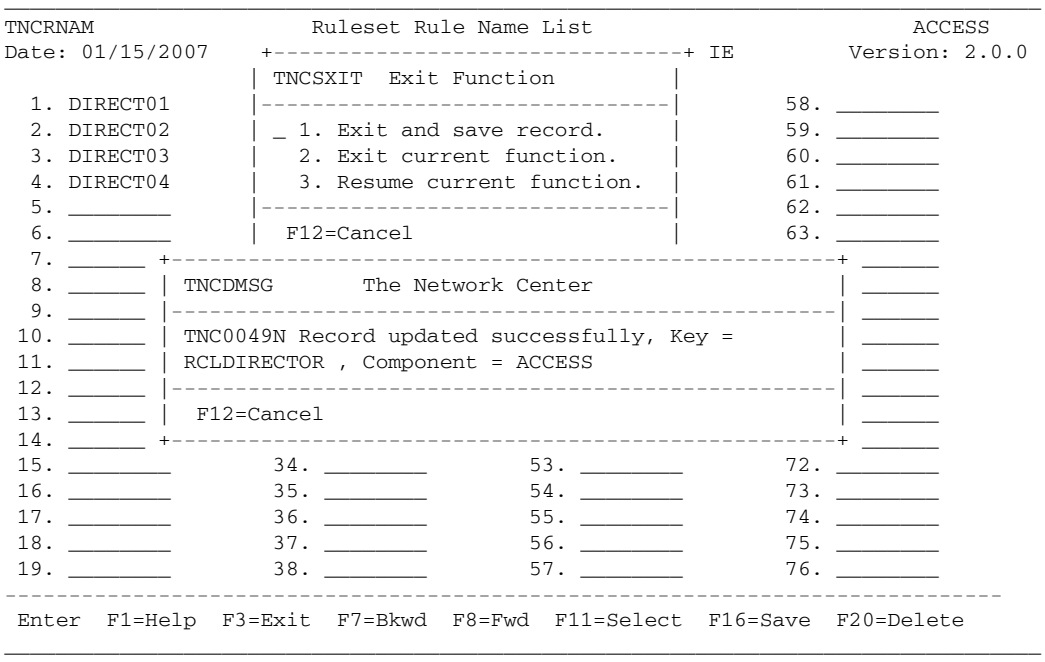

Figure 71. Ruleset Rule Name List Confirmation

Press F12 (Cancel) to cancel the message and resume Rule definition.

4. After defining the Rule operands, press Enter to refresh and edit the panel.
5. If the operands are correct, press F16 (Save) to save the Rule or Ruleset; a confirmation message appears, as in the following figure:

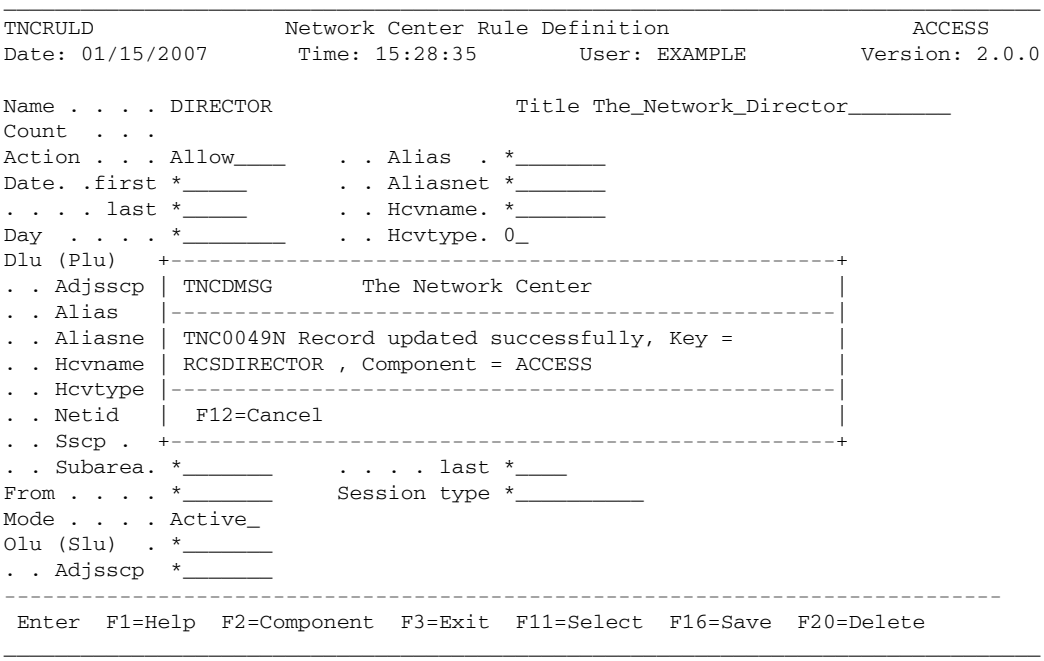

Figure 72. Rule Confirmation Message

Press F12 (Cancel) to cancel the message if it appears in a pop up window.

6. The panel will appear with the default values reinstated; you may proceed with defining the next Rule, if desired.

Note: You can display a Ruleset, Value Group, or IP data information anytime the Rule is open by placing the cursor on the related field and pressing F11=Select.

Modifying or Deleting Rules and Rulesets

If you have defined one or more Rules or Rulesets, you can use the 'Rule display' function to ensure that they are defined and saved correctly. You can also use this function to open a Rule or Ruleset panel for modification or to delete the record.

Steps:

1. Go the the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 73. Access Component Administration Menu (TNCADMC)

2. Select choice 7, 'Rule display'; the Network Center displays an alphabetized list of all the defined Rules, as in the following example:

```
TNCRULS                      Network Center Rules                      ACCESS

Select a rule by typing the number, or positioning the cursor at your choice.
Then Enter. The selected rule will be displayed.

__    1. CICS      Rule        Inventory Subsystem
      2. DIRECTOR  Rule        The Network Director
      3. HDQTRS    Rule        TSO for Company B
      4. LOGAPPL   Rule        Director Validated
      5. OUTSIDE   Rule        All other combinations
      6. PRINTERS  Rule        Remote Printers
      7. SYSTEMS   Rule        System Programming
      8. TCAS      Rule        TSO Controller
      9. TSO       Rule        Time Sharing Option

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

Figure 74. Network Center Rules Panel (TNCRULS)

To scroll through a list that exceeds the screen, use the F7 (Backward) and F8 (Forward) actions. To locate a specific Rule, use the F11 (Find) action.

3. Place the cursor on the Rule you want to view or modify and press Enter; the Rule's Rule definition panel appears, as in the following example:

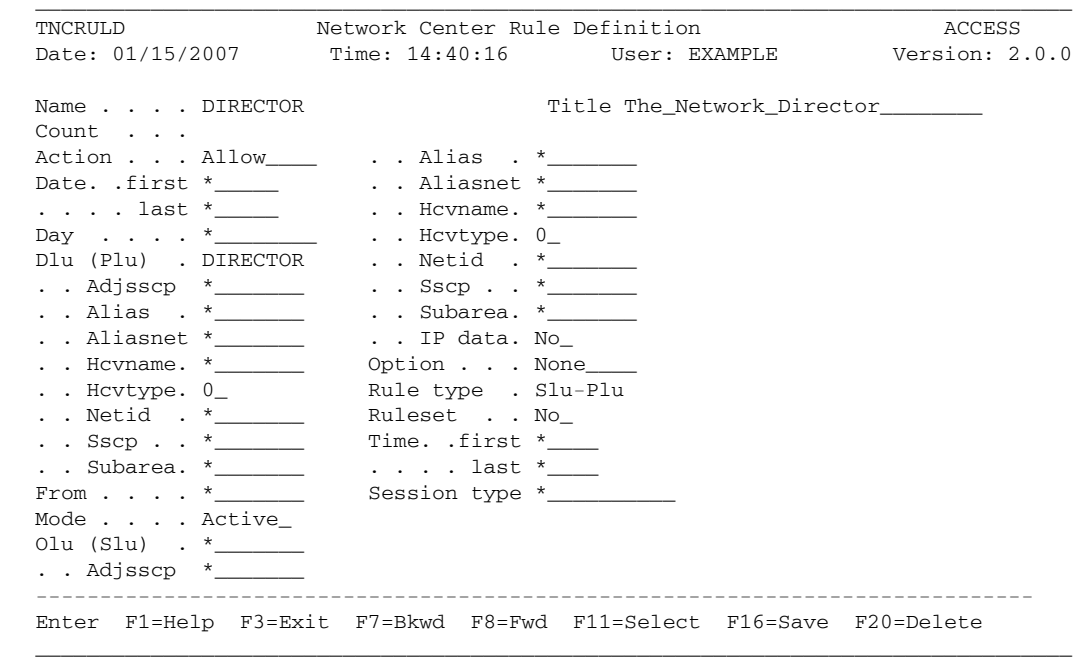

Figure 75. Example Rule Definition Panel

You may now make any desired modifications:

- **To display a Ruleset, Value Group, or IP data information**, place the cursor on the related field and press F11=Select.
- **To delete an operand entry**, type over it with blanks or use the Delete key. Press F16 (Save) to save the changes.

- **To modify an entry**, type over it with the new value. Press F16 (Save) to save the changes.
- **To delete the Rule**, press F20 (Delete); The "Delete function" window appears:

```
TNCRULD                Network Center Rule Definition                   ACCESS
Date: 01/15/2007        Time: 15:29:13        User: EXAMPLE         Version: 2.0.0
                       +---------------------------------+
Name . . . . DIRECTOR | TNCDELT  Delete function        | _Director________
Count  . . .          |---------------------------------|
Action . . . Allow___ | _ 1. Delete the record.         |
Date. .first *_____   |   2. Resume current function.   |
. . . . last *_____   |---------------------------------|
Day  . . . . *_______ |  F12=Cancel                     |
Dlu (Plu)  . *_______ +---------------------------------+
. . Adjsscp  *_______     . . Sscp . . *_______
. . Alias  . *_______     . . Subarea. *_______
. . Aliasnet *_______     . . IP data. No_
. . Hcvname. *_______     Option . . . None____
. . Hcvtype. 0_           Rule type  . Slu-Plu
. . Netid  . *_______     Ruleset  . . Yes Select _
. . 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 76. Delete Function Window

Select choice 1, 'Delete the record'; a message appears stating that the record deleted successfully:

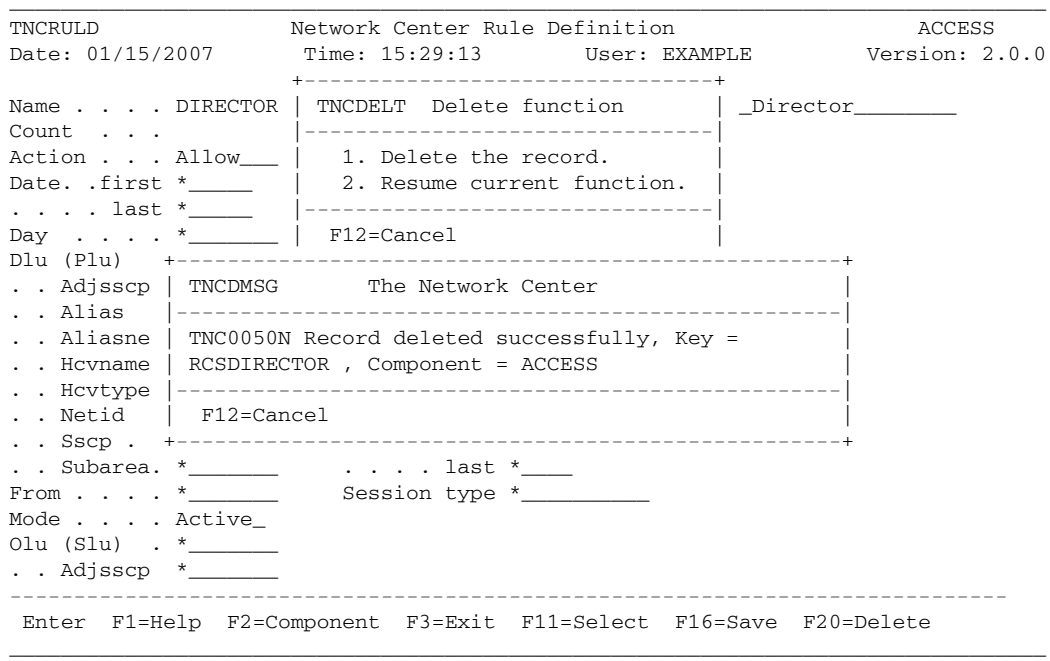

Figure 77. Rule deletion confirmation

4. After viewing, modifying, or deleting the Rule, you can return to the selection list by pressing F12 (Cancel). Do a Rule reload to make the changes active (see "Reloading Rules" on page 118).

Defining a Rule Group

Rule Groups tell the Network Center the order in which to process the Rules, Rulesets, and/or Groups it contains. If you define more than one Rule, Ruleset, or Group, you must specify them in a Rule Group using a Group Definition panel. You can also use the Group Definition panel to define a Value Group (see "Value Groups: Creating Symbolic Rule Operand Values" on page 29).

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 78. Access Component Administration Menu (TNCADMC)

2. Select choice 3, 'Define (value) Group'; the Group Definition panel appears:

```
TNCGRPD                 Group Definition                          ACCESS
Date: 01/15/2007        Time: 16:03:16        User: EXAMPLE     Version: 2.0.0

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

Name . . . . ________                    Title ________________________________

  1. ________        16. ________        31. ________        46. ________
  2. ________        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 79. Group Definition panel (TNCGRPD)

3. You can use the "Group Definition" panel to set the processing order of any Rule, Ruleset, or Group. Enter the Group's 'Name' and 'Title' first. Then, enter the names of the Rules, Rulesets, and/or Groups to be included in the Group into the numbered input fields according to their processing order. The following figure shows a defined Rule Group panel:

```
TNCGRPD                Group Definition                          ACCESS
Date: 01/15/2007       Time: 15:33:08       User: EXAMPLE      Version: 2.0.0

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

Name . . . . ACCESS__                  Title Access_for_Example_Network__

  1. DIRECTOR        16. ________        31. ________        46. ________
  2. LOGAPPL_        17. ________        32. ________        47. ________
  3. TSO_____        18. ________        33. ________        48. ________
  4. TCAS____        19. ________        34. ________        49. ________
  5. HDQTRS__        20. ________        35. ________        50. ________
  6. CICS____        21. ________        36. ________        51. ________
  7. PRINTERS        22. ________        37. ________        52. ________
  8. SYSTEMS_        23. ________        38. ________        53. ________
  9. OUTSIDE_        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 80. Example Group Definition Panel

To insert additional fields in the Group definition list, enter "**.I**" in the field following the insertion point. (If the field already contains an entry, simply type "**.I**" over the beginning of the field; the field's full name will be reinstated). Five input fields will appear, as in the following example:

```
TNCGRPD                Group Definition                              ACCESS
Date: 01/15/2007       Time: 15:33:08       User: EXAMPLE       Version: 2.0.0

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

Name . . . . ACCESS__                  Title Access_for_Example_Network__

  1. DIRECTOR        16. ________        31. ________        46. ________
  2. LOGAPPL_        17. ________        32. ________        47. ________
  3. TSO_____        18. ________        33. ________        48. ________
  4. TCAS____        19. ________        34. ________        49. ________
  5. HDQTRS__        20. ________        35. ________        50. ________
  6. .________       21. ________        36. ________        51. ________
  7. .________       22. ________        37. ________        52. ________
  8. .________       23. ________        38. ________        53. ________
  9. .________       24. ________        39. ________        54. ________
 10. .________       25. ________        40. ________        55. ________
 11. CICS____        26. ________        41. ________        56. ________
 12. PRINTERS        27. ________        42. ________        57. ________
 13. SYSTEMS_        28. ________        43. ________        58. ________
 14. OUTSIDE_        29. ________        44. ________        59. ________
 15. ________        30. ________        45. ________        60. ________
-------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F7=Bkwd  F8=Fwd  F11=Select  F16=Save  F20=Delete
```

Figure 81. Inserting Additional Fields

After defining the desired fields, press Enter and the unmodified inserted fields will disappear.

Note: To display a Group, Ruleset, or Rule defined within the Group, place the cursor on its name and press F11 (Select).

4. After entering the names of the Rules, Rulesets, and/or Groups, press Enter to refresh and edit the panel.

5. If the fields are correct, press F16 (Save) to save the Group; a confirmation message appears stating that the record updated successfully:

```
TNCGRPD                Group Definition                              ACCESS
Date: 01/15/2007       Time: 15:44:55        User: EXAMPLE        Version: 2.0.0

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

Name . . . . ACCESS__                  Title Access_for_Example_Network__

  1. DIRECTOR        16. _________       31. _________       46. _________
  2. LOGAPPL_        17. _________       32. _________       47. _________
  3. TSO___ +-------------------------------------------------+ _______
  4. TCAS__ | TNCDMSG       The Network Center                | _______
  5. HDQTRS |-------------------------------------------------| _______
  6. CICS__ | TNC0049N Record updated successfully, Key =     | _______
  7. PRINTE | RCGACCESS , Component = ACCESS                  | _______
  8. SYSTEM |-------------------------------------------------| _______
  9. OUTSID |  F12=Cancel                                     | _______
 10. _______ +-------------------------------------------------+ _______
 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 82. Group Definition Confirmation Message

Note: To cancel a pop up window, press F12 (Cancel).

Modifying or Deleting Groups and Value Groups

After you have defined a Group or Value Group, you can use the 'Display (value) Group' function to ensure that it is defined and saved correctly. You can also use this function to open a Group Definition panel for modification or to delete the record.

Steps:

1. Go to the Access Component Administration panel (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 83. Access Component Administration Menu (TNCADMC)

2. Select choice 4, 'Display (value) Group'; a panel appears displaying an alphabetized list of all the defined Groups for Access as in the following example:

```
TNCGRPS                Network Center Groups                        ACCESS

Select a group by typing the number, or positioning the cursor at your choice.
Then Enter. The selected group will be displayed.

__   1. ACCESS    Access for Example Network




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

Figure 84. Network Center Groups Panel (TNCGRPS)

The first column indicates the Group and/or Value Group names. The second column indicates the Group and/or Value Group titles.

3. To view or modify a Group or Value Group, place the cursor on the choice and press Enter; the Group Definition panel appears, as in the following example:

```
_____________________________________________________________________________
TNCGRPD                Group Definition                          ACCESS
Date: 01/15/2007       Time: 15:33:08       User: EXAMPLE       Version: 2.0.0

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

Name . . . . ACCESS__                  Title Access_for_Network_Director_

  1. DIRECTOR        16. ________        31. ________        46. ________
  2. LOGAPPL_        17. ________        32. ________        47. ________
  3. TSO_____        18. ________        33. ________        48. ________
  4. TCAS____        19. ________        34. ________        49. ________
  5. HDQTRS__        20. ________        35. ________        50. ________
  6. CICS____        21. ________        36. ________        51. ________
  7. PRINTERS        22. ________        37. ________        52. ________
  8. SYSTEMS_        23. ________        38. ________        53. ________
  9. OUTSIDE_        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 85. Example Group Definition Panel

You can then proceed with modifications:

- **To delete a field entry**, overtype it with blanks or use the delete key. Press F16 (Save) to save the changes.
- **To insert a field into an existing list**, use the '.I' prefix command (see "Defining a Rule Group" on page 105).
- **To modify a field entry**, overtype it with the new value. Press F16 (Save) to save the changes.
- **To display a Group, Ruleset, or Rule** defined within the Group, place the cursor on its name and press F11 (Select); the resource's definition panel will then appear.

- **To delete the Group**, press F20 (Delete); the "Delete function" window appears:

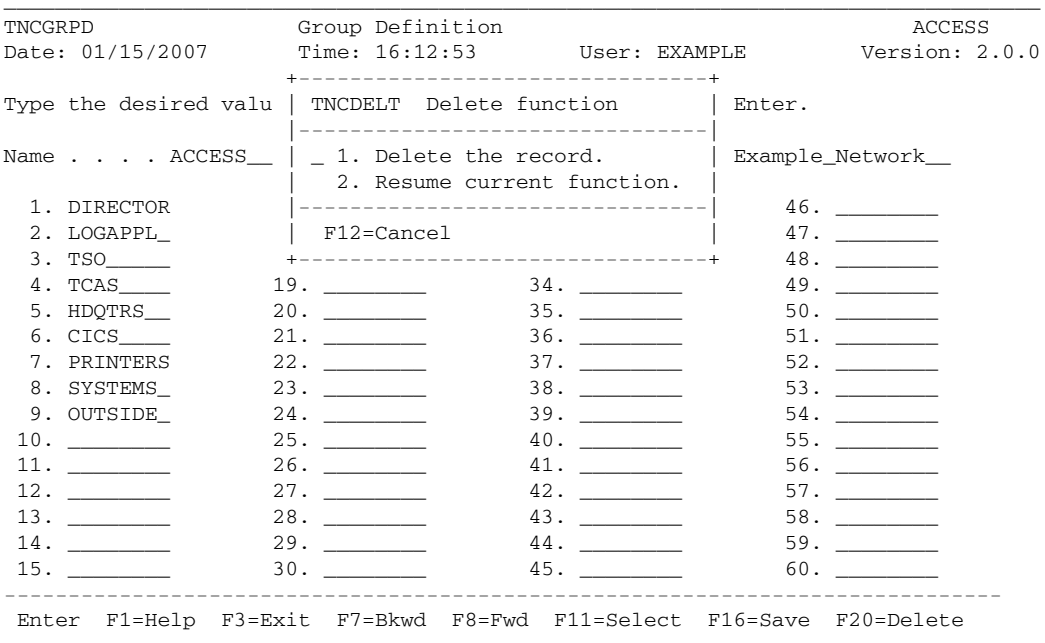

Figure 86. Delete Function Window

Select choice 1, 'Delete the record'. A message appears stating that the record deleted successfully:

```
TNCGRPD                 Group Definition                              ACCESS
Date: 01/15/2007        Time: 16:12:53        User: EXAMPLE        Version: 2.0.0
                       +--------------------------------+
Type the desired valu  | TNCDELT  Delete function       | Enter.
                       |--------------------------------|
Name . . . . ACCESS__  | 1 1. Delete the record.        | Example_Network__
                       |   2. Resume current function.  |
  1. DIRECTOR __       |--------------------------------|     46. ________
  2. LOGAPPL_ __       |  F12=Cancel                    |     47. ________
  3. TSO___ +-----------------------------------------------------+ ______
  4. TCAS__ | TNCDMSG       The Network Center                      | ______
  5. HDQTRS |-------------------------------------------------------| ______
  6. CICS__ | TNC0050N Record deleted successfully, Key =           | ______
  7. PRINTE | RCGACCESS , Component = ACCESS                        | ______
  8. SYSTEM |-------------------------------------------------------| ______
  9. OUTSID |  F12=Cancel                                           | ______
 10. ______ +-------------------------------------------------------+ ______
 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 87. Group Deletion Confirmation

Press F12 (Cancel) to cancel the message.

4. To save any modifications, press F16 (Save).

Activating Rules

After ensuring that your Rules are correctly saved (see "Modifying or Deleting Groups and Value Groups" on page 110), you can activate the Rules. There are two steps to Rule activation: specifying the Rules in the 'Component Options' record and reloading the Rules using the 'Rule reload' function. You should also verify that the active Rules are operating correctly.

Specifying the Active Rules

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
  Options  Exit  Help  Component
--------------------------------------------------------------------------------
TNCADMC               Access Component Administration                 ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 88. Access Component Administration Menu (TNCADMC)

2. Select choice 2, 'Component Options'; the "Component Options" panel appears:

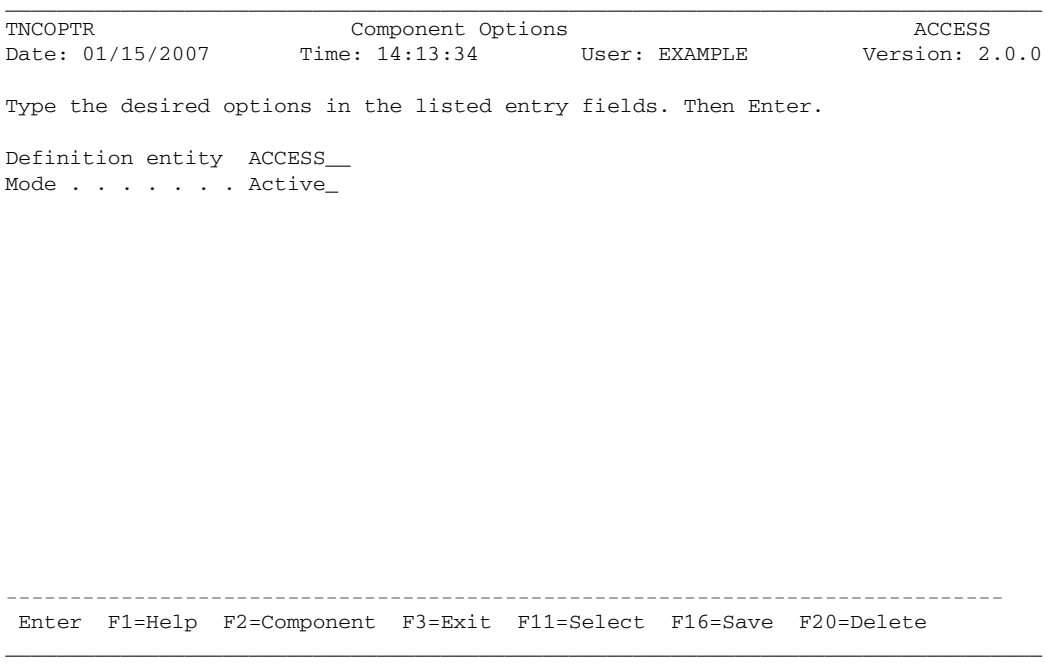

Figure 89. The Component Options Panel (TNCOPTR)

3. In the 'definition entity' field, enter the name of the Rule, Ruleset, or Group that you want to active (i.e. used during Rule processing).

4. In the "Mode" field, enter one of the following methods of operation:

   - Enter **Active** to allow your Access Rules to operate. Each Rule's individual mode setting, which you defined in the Rule definition panel, is honored.

   - Enter **Dormant** to turn off Rule processing. Access will operate without using the defined Rules.

   - The default, **Warn**, causes Access to evaluate the Rules defined in the 'definition entity' field and issue messages, but not perform any of the requested operations. This option is useful for testing a Rule structure without it affecting your installation.

   We recommend that you set the mode to "Warn" during initial implementation. Then, after determining that the Rule is satisfactory, change the mode to "Active".

5. After entering the Options 'mode', press F16 (Save) to save the record; a message appears confirming the update:

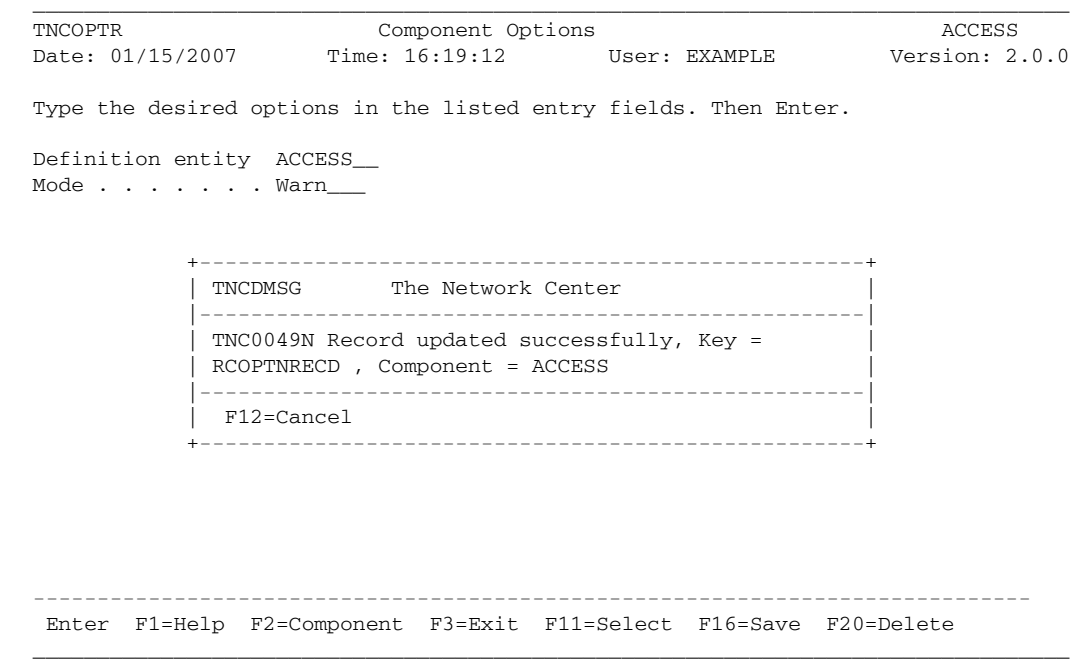

Figure 90. Component Options Confirmation Message

Note: After defining the Component Options, you can use it to view the active Rules by locating the cursor on the 'Definition entity' field and pressing F11 (Select).

Reloading Rules

After defining the active Rules using the Component Options function, you are ready to reload the Rules. You should also reload the Rules anytime you make a change to a Rule, Ruleset, or Group that you wish to make active.

The 'Rule reload' function causes Access to obtain the "entity" defined in the Component Options record, to load the Rules, and to immediately begin using them.

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 91. Access Component Administration Menu (TNCADMC)

2. Select choice 8, "Rule reload"; a pop up window appears asking you to confirm that the Rules should be reloaded:

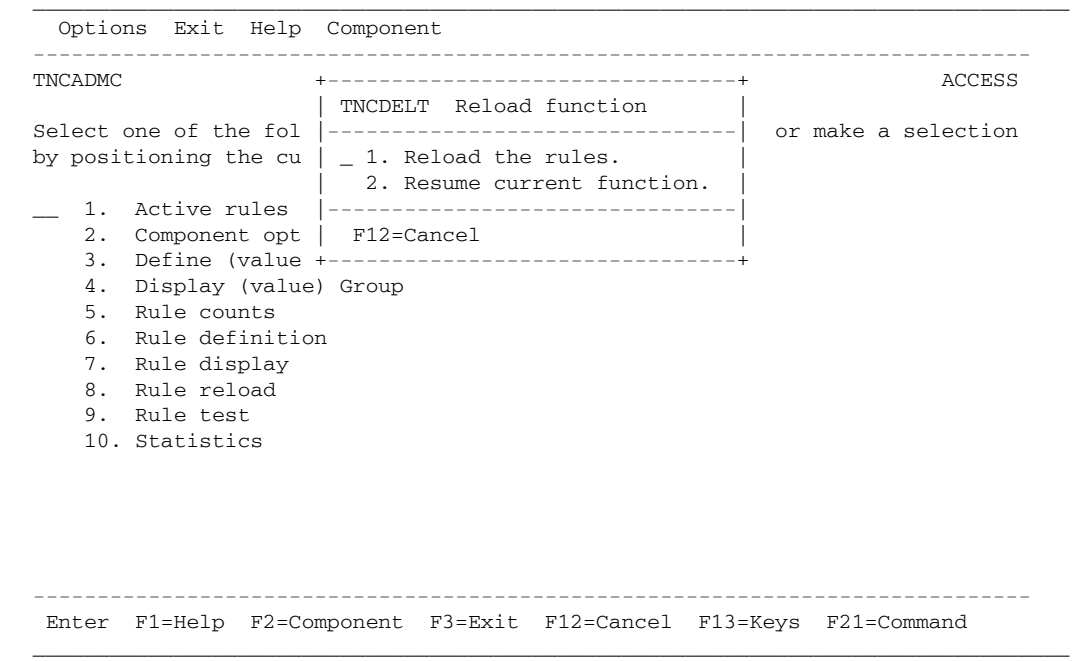

Figure 92. Rule Reload Function (TNCDELT)

3. Press Enter to confirm the Reload; a message appears stating that your Rules are being reloaded:

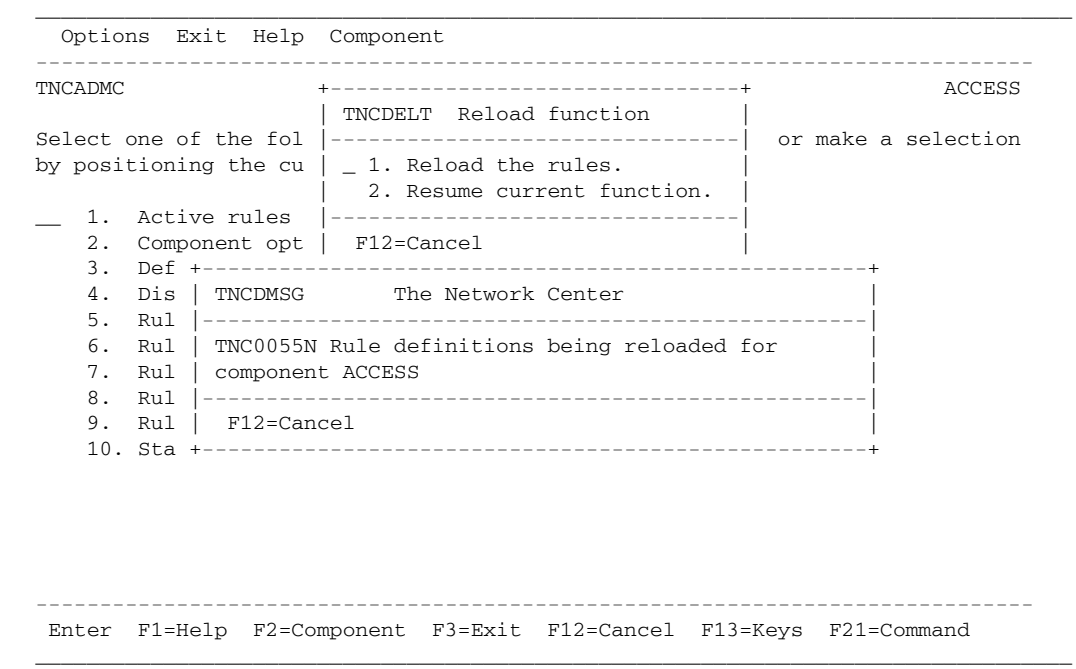

Figure 93. Rule Reload Message

Access is now actively processing your Rules (based on the 'mode' field in the Component options record; see "Specifying the Active Rules" on page 115.)

Verifying the Operation of the Active Rules

After activating one or more Rules, you can ensure that they are operating correctly by using the 'Active rules' function. This function lists the Rules, Rulesets, and Groups that have been activated for Access according to their processing order and also displays how often an active Rule has been used.

Note: You can also verify that the active Rules are operating by searching the Message Queue for messages TNA1002 and TNA1003, which indicate that sessions are being evaluated by the proper Rules. (See "Viewing Rule Messages" on page 137 for more information on using the Message Queue.)

To view the active Rules:

1. Go to the Access Component Administration menu (See "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC              Access Component Administration                 ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 94. Access Component Administration Menu (TNCADMC)

2. Select choice 1, 'Active Rules'; the Network Center Rules panel appears (the panel you receive will reflect the Rules defined at your installation):

```
TNCRULS                      Network Center Rules                      ACCESS

Select a rule by typing the number, or positioning the cursor at your choice.
Then Enter. The selected rule will be displayed.

__    1. ACCESS    Group   1   Access for Example Network      0
      2. DIRECTOR  Rule    2   The Network Director            29952
      3. LOGAPPL   Rule    2   Director Validated              2165
      4. TSO       Rule    2   Time Sharing Option             10368
      5. TCAS      Rule    2   TSO Controller                  10368
      6. HDQTRS    Rule    2   TSO for Company B               4144
      7. CICS      Rule    2   Inventory Subsystem             12352
      8. PRINTERS  Rule    2   Remote Printers                 2064
      9. SYSTEMS   Rule    2   System Programming              1056
     10. OUTSIDE   Rule    2   All other combinations          775

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

Figure 95. The Network Center Rules Panel (TNCRULS)

Note: If no Rules are currently defined, you will receive an error message.

The Network Center Rules panel displays the active Rules according to the Rule processing order. The first column displays the Rule, Ruleset or Group names; the second column displays whether it is a Rule, Ruleset, or Group; the third column displays the Rule hierarchy level; the fourth column displays the Rule, Ruleset, or Group title; and the fifth column indicates how many times the Rule or Ruleset has been used since the last Rule reload.

3. To display a Rule, Ruleset, or Group, place the cursor on the desired item and press Enter.

If you select a Rule, the Rule definition panel will display an additional field named 'count'. This field indicates how often the Rule has been matched, as in the following example:

```
TNCRULD               Network Center Rule Definition                  ACCESS
Date: 01/15/2007       Time: 15:22:19        User: ACTIVE          Version: 2.0.0

Name . . . . DIRECTOR                   Title The_Network_Director________
Count  . . . 29952
Action . . . Allow____     . . Alias  . *_______
Date. .first *_____        . . Aliasnet *_______
. . . . last *_____        . . Hcvname. *_______
Day  . . . . *________     . . Hcvtype. 0_
Dlu (Plu)  . DIRECTOR      . . Netid  . *_______
. . Adjsscp  *_______      . . Sscp . . *_______
. . Alias  . *_______      . . Subarea. *_______
. . 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_
Olu (Slu)  . SC0TCP*_
. . Adjsscp  *_______
--------------------------------------------------------------------------------
 Enter  F1=Help  F2=Component  F3=Exit  F11=Select  F16=Save  F20=Delete
```

Figure 96. Rule Definition Panel with Count Field

Testing Rules

We recommend testing all Rules prior to making them fully active (i.e. setting the Rule's mode to 'active' in the Rule definition and Component options panels). Testing allows you to determine the effectiveness of your Rules and to modify any Rules or Rule processing order that might be detrimental to your system's operation.

There are several methods for testing Rules. "Testing Session Criteria against the Active Rules" guides you in using the 'Rule test' function to create mock sessions to test against Rules. "Testing the Rule Hierarchy" on page 127 shows how to use the 'Ruletest component' function (available from the main Network Center menu), which allows you to transfer an entire Rule hierarchy or individual Rules into a test Component environment.

Testing Session Criteria against the Active Rules

You can use the 'Rule test' function to create a sample session and test it against the active Rules (see "Specifying the Active Rules" on page 115). This allows you to determine if a Rule functions correctly in allowing or denying a particular session or type of session.

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 97. Access Component Administration Menu (TNCADMC)

2. Select choice 9, 'Rule test'; the Network Center Rule Match panel appears:

```
TNCRULD               Network Center Rule Match Test                  ACCESS
Date: 01/15/2007       Time: 15:24:24        User: EXAMPLE         Version: 2.0.0

Name . . . . RULETEST                  Title Match_a_rule_________________
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  F12=Cancel  F16=Test  F21=Command
```

Figure 98. The Network Center Rule Match Test Panel (TNCRULD)

3. Enter the operands for the session that you wish to test against the active Rules. (To get help for an operand, place your cursor on the operand and press the F1=Help key.)

4. When you are done defining the session parameters, press F16 (Test); a message appears stating the first active Rule within the Rule hierarchy that matched the session. If no Rule matched the session, a message appears stating that no Rules are matched by the parameters.

5. If a Rule match was found, press F12 (Cancel) to cancel the pop up window message; a window appears that allows you to display the Rule:

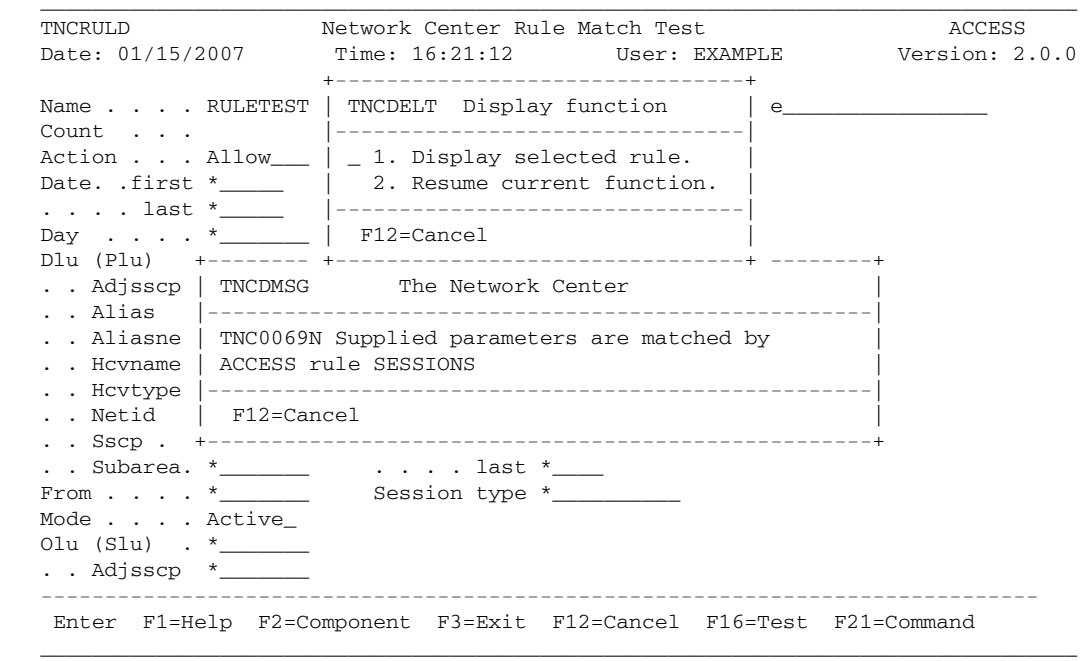

Figure 99. Display Function Window

Select choice 1, 'Display selected rule', to view the Rule's Rule definition panel. Select choice 2, 'Resume current function', to return to the Network Center Rule Match Test panel.

Note: After determining that your Rules are satisfactory, you may want to change the Rule mode to 'active'. Make sure to set the mode in the Component Options record (see "Specifying the Active Rules" on page 115) and in the Rule's Rule definition panel, (see "Defining Rules and Rulesets" on page 90) and to reload the Rules (see "Reloading Rules" on page 118).

Testing the Rule Hierarchy

The Ruletest Component is available from the main Network Center menu. It allows you to test a Component's complete active Rule hierarchy or individual Rules in a test environment and then save the changes back to the active environment. While in the test environment, you may create, modify, "activate" and test Rules.

You must first copy the Rule, Ruleset, or Group that you wish to test from its record in the Network Data File to the Ruletest Component.

Steps:

1. Go to the main Network Center menu (TNCMENU) (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help
-----------------------------------------------------------------------------
TNCMENU                       The Network 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.  Administration
     2.  Access
     3.  Alias
     4.  Query
     5.  Ruletest
     6.  Select
     7.  Timeout









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

Figure 100. The Network Center Menu (TNCMENU)

2. Select choice 1, 'Administration'; the Network Center Administration panel appears:

```
  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 101. The Network Center Administration Panel

3. Select choice 7, 'Network Data File'; the Network Data File Administration menu appears:

```
  Options  Exit  Help  Component
--------------------------------------------------------------------------------
TNCADMF                Network Data File 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.  Copy records
      2.  Data area offsets
      3.  Data area definitions
      4.  Data area identifiers
      5.  Data area tables
      6.  Data file records
      7.  Help text
      8.  Message text
      9.  Status of file
     10.  Summary report
     11.  Switch file mode




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

Figure 102. Network Data File Administration Panel (TNCADMF)

4. Select choice 1, 'Copy records'; the Copy Data File Records panel appears:

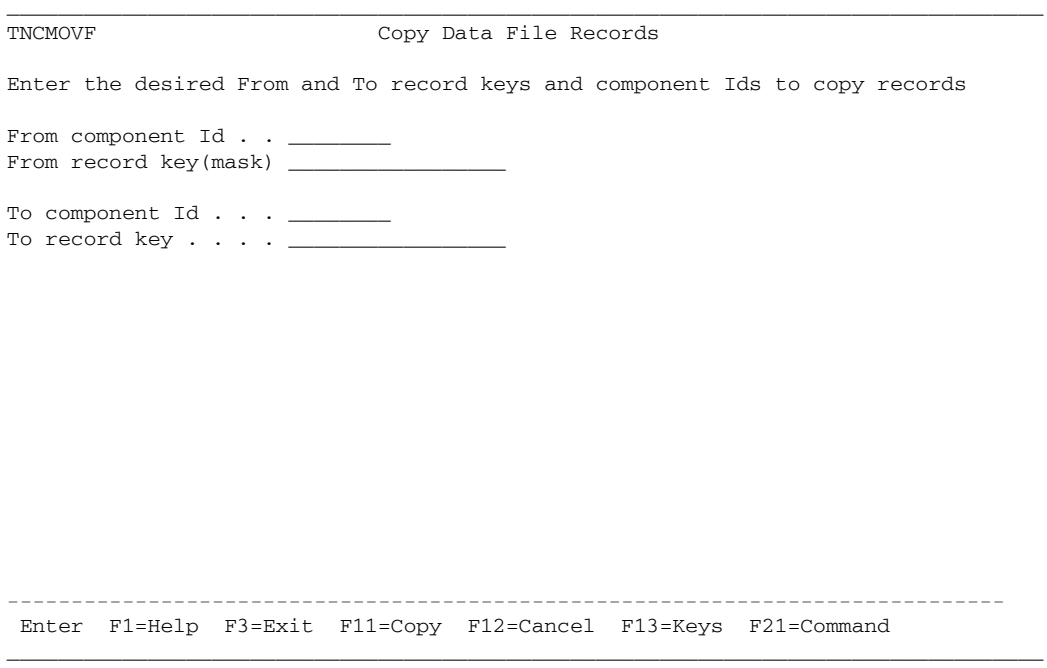

Figure 103. The Copy Data File Records Panel (TNCMOVF)

5. Define the fields as follows:

   From component Id ACCESS
   From record key(mask) R*

   To component Id RULETEST
   To record key(mask)

The panel should appear as follows:

```
TNCMOVF                        Copy Data File Records

Enter the desired From and To record keys and component Ids to copy records

From component Id . . ACCESS__
From record key(mask) R*_________________

To component Id . . . RULETEST
To record key . . . . ___________________




 Enter  F1=Help  F3=Exit  F11=Copy  F12=Cancel  F13=Keys  F21=Command
```

Figure 104. Example Copy Data File Records

6. Press F11 (Copy) to copy the record from the Network Data File to the Ruletest Component; a confirmation message appears:

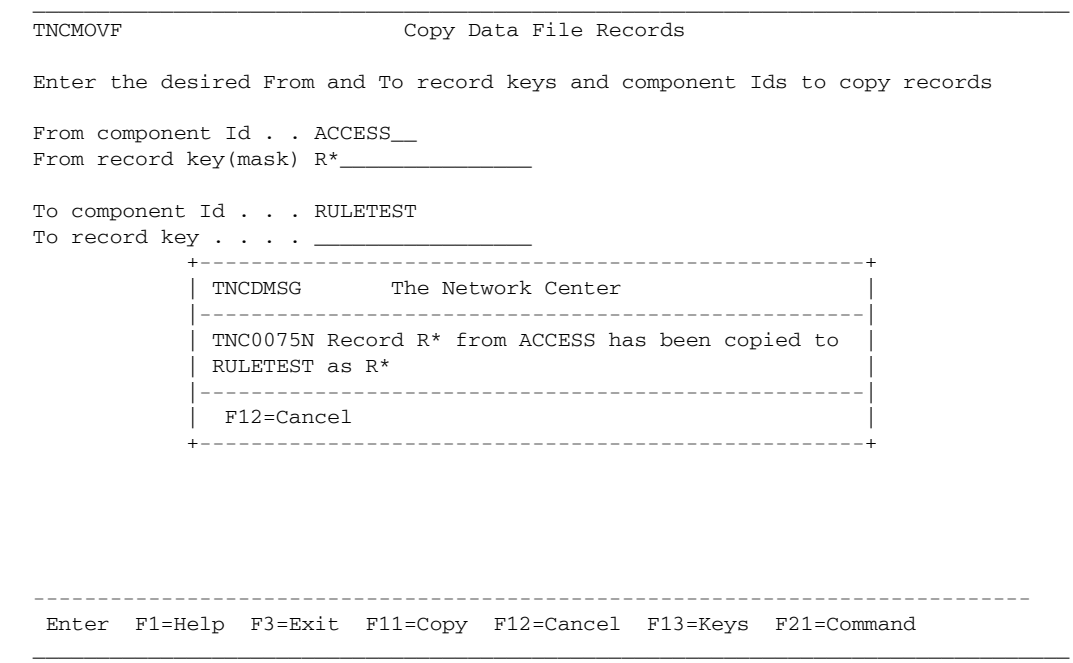

Figure 105. Copy Data File Confirmation Message

You can now actively use the Ruletest Component.

7. Open the Ruletest Component by selecting the Ruletest choice from the Network Center Menu (TNCMENU), or to jump straight to the Ruletest Component, enter "RULETEST" in the command line. The following panel appears:

```
 Options  Exit  Help  Component
------------------------------------------------------------------------------
TNCADMC              Ruletest Component Administration              RULETEST

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test




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

Figure 106. The Ruletest Component Administration Panel (TNCADMC)

The menu choices contain all of the same tools as operational Network Center Components, including creating, modifying, and activating Rules, Rulesets, and Groups.

8. After testing your Rules and making any necessary changes, you can copy your Rule records back to Access by using the 'Copy Record Data Files' function. For example, the following definitions would copy back all of the Records from the Ruletest Component to the Access Rule records:

   From component Id RULETEST
   From record key(mask) R*

   To component Id ACCESS
   To record key(mask)

The panel would appear as follows:

```
TNCMOVF                       Copy Data File Records

Enter the desired From and To record keys and component Ids to copy records

From component Id . . RULETEST
From record key(mask) R*_______________

To component Id . . . ACCESS__
To record key . . . . _________________




 Enter  F1=Help  F3=Exit  F11=Copy  F12=Cancel  F13=Keys  F21=Command
```

Figure 107. Copying Records Back to Access

9. Press F11 (Copy) to copy the record from the Network Data File to the Ruletest Component; a confirmation message appears:

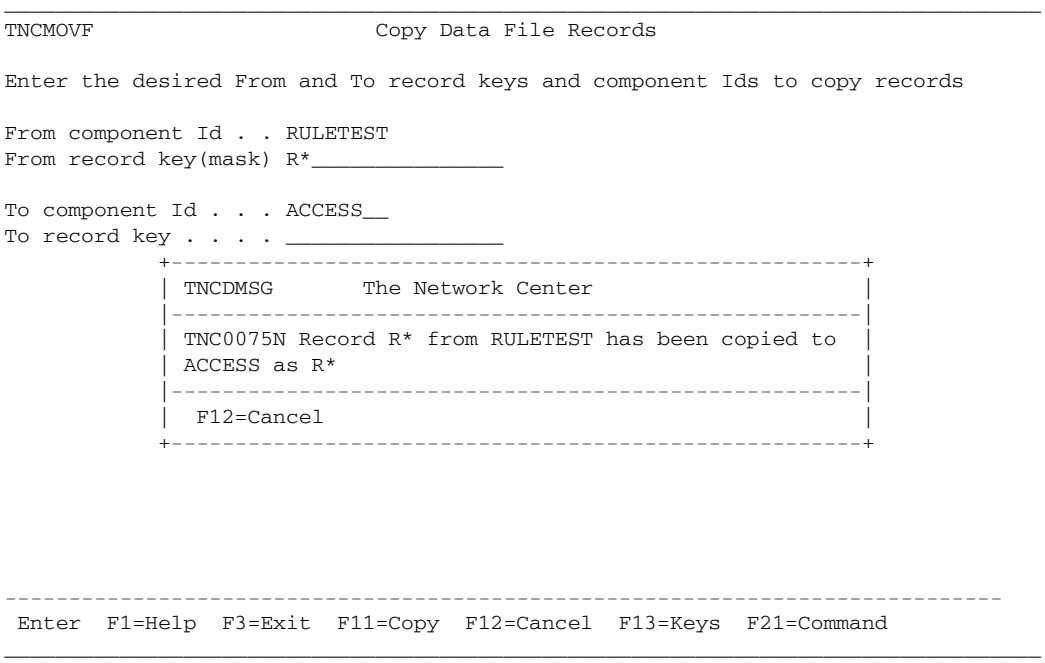

Figure 108. Copy Data File Confirmation Message

Chapter 6. Tracking Session Approval and Denial

This chapter guides you in using the different functions available from the Network Center for viewing session, Rule, and Component information. Topics include:

- "Viewing Session Statistics"
- "Viewing Rule Messages" on page 137
- "System Accounting" on page 141

Viewing Session Statistics

The 'Statistics' choice lists recent session activity that has been processed by Access, including the number of requested sessions, denied sessions, approved sessions, allowed sessions (in warn mode) terminated sessions, and currently active sessions.

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
  Options  Exit  Help  Component
--------------------------------------------------------------------------------
TNCADMC              Access Component Administration                  ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 109. Access Component Administration Menu (TNCADMC)

2. Select choice 10, 'Statistics'; a list of current session statistics appears:

```
 TNCSTAT               Network Center Statistics                    ACCESS

 Sessions requested . . : 6482
 Sessions denied  . . . : 1041
 Sessions approved  . . : 5207
 Sessions allowed(warn) : 0
 Sessions terminated  . : 5430
 Sessions active  . . . : 818









--------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F12=Cancel
```

Figure 110. Network Center Statistics Panel (TNCSTAT)

Note: You can also use the Active rules function to view how often a particular Rule has been matched. (See "Verifying the Operation of the Active Rules" on page 121 for more information.)

Viewing Rule Messages

All Access activities are recorded and sent to the Message Queue. You can use the 'Rule counts' function to update the Message Queue with information on how often each Access Rule has been used. This information can help you to gauge a Rule's effectiveness and its frequency of use.

Steps:

1. Go to the Access Component Administration menu (see "Opening the Access Menu" on page 86):

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMC               Access Component Administration                ACCESS

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

__  1.  Active rules
    2.  Component options
    3.  Define (value) Group
    4.  Display (value) Group
    5.  Rule counts
    6.  Rule definition
    7.  Rule display
    8.  Rule reload
    9.  Rule test
    10. Statistics




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

Figure 111. Access Component Administration Menu (TNCADMC)

2. Select choice 5, 'Rule counts'; a message appears stating that the Access Rules have been logged:

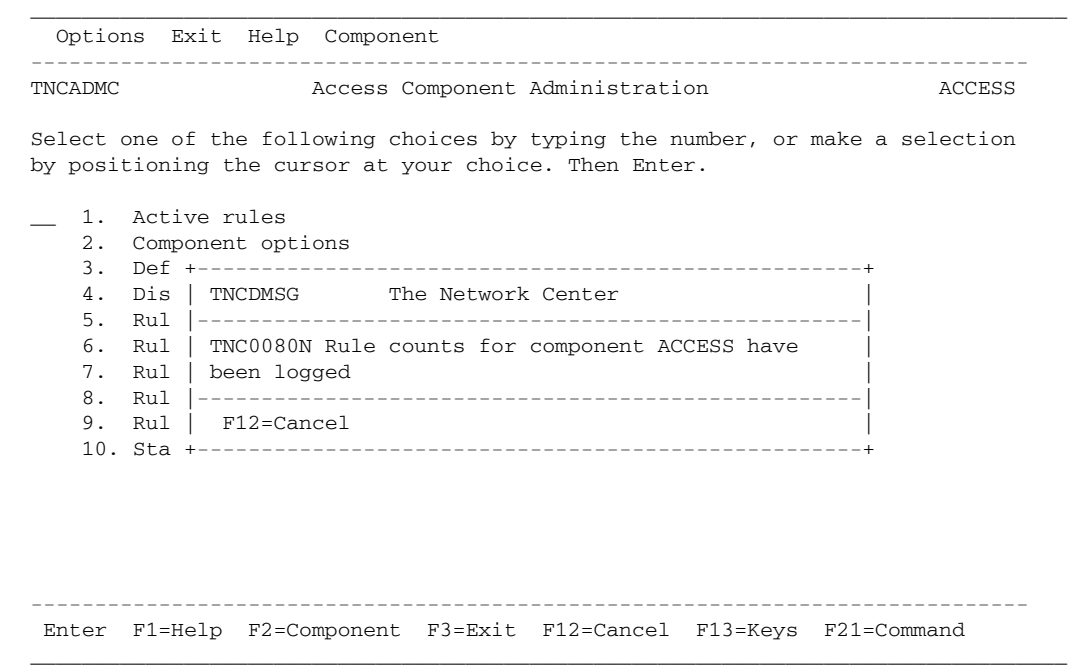

Figure 112. Rule Counts Panel

3. To view the results, look in the Message queue. To access the Message queue, return to the Network Center menu (TNCMENU) and select choice 1, 'Administration' to open the Network Center Administration menu. The following figure shows the Administration menu:

```
  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 113. Network Center Administration Menu

From the Network Center Administration menu, select choice 6, 'Message queue' to open the Message Queue:

```
TNCMSGQ                 Network Center Message Queue              More:  -
------------------------------------------------------------------------------
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Read rule definitions
TNC0136N TSO User EXAMPLE requested File Request FAB information
TNC0136N TSO User EXAMPLE requested NDF Log rule counts
TNC0239N ACCESS rule ACCESS was matched 0 times
TNC0239N ACCESS rule DIRECTOR was matched 29,252 times
TNC0239N ACCESS rule LOGAPPL was matched 2,164 times
TNC0239N ACCESS rule TSO was matched 10,368 times
TNC0239N ACCESS rule TCAS was matched 10,368 times
TNC0239N ACCESS rule HDQTRS was matched 4,144 times
TNC0239N ACCESS rule CICS was matched 12,352 times
TNC0239N ACCESS rule PRINTERS was matched 2,064 times
TNC0239N ACCESS rule SYSTEMS was matched 1,056 times
TNC0239N ACCESS rule OUTSIDE was matched 775 times
------------------------------------------------------------------------------
 F1=Help  F2=Prefix  F7=Bkwd  F8=Fwd  F11=Find  F12=Cancel  F19=Left  F20=Right
```

Figure 114. Network Center Message Queue

You can now view Rule messages. To scroll through the messages, use the Backward (F7) and Forward (F8) actions. To display only particular messages, use the F2 (Prefix) action. To locate messages, use the F11 (Find) action. See the *Installation and Operations* manual (TNC-0003) for more information.

System Accounting

Access can also be configured to produce a general accounting of the actions that occur while it is operating. The Network Center "records" this accounting information as a result of an "event", which is identified by a unique Network Center message.

To do this, simply activate the accounting option for one or more specific Network Center or Access messages. When the message is issued, the Network Center Server will produce an SMF record (for z/OS systems), a z/VM account record (for z/VM systems), or a sequential output record (for either system). Consult the *Installations and Operations* manual (TNC-0003) for information about the Account action on the Message Text panels.

The Network Center allows you to record any event that occurs while it is operational. The precise "events" you choose to activate should be a function of what you are trying to record. For example, setting Account for TNA1002 will record when a session is approved. Setting Account for TNA1003 will record when a session is rejected. Setting Account for both messages will produce a record for both conditions.

Steps:

1. Go to the Network Center Administration menu (TNCADMN):[3]

```
  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 115. The Network Center Administration Menu

[3] To jump to this panel, enter "**ADM**IN" in the Command area (press F21 (Command) to activate the Command area), or, go to the main Network Center menu (TNCMENU) and select choice 1, 'Administration'.

2. Select choice 7, 'Network data file'; the Network Data File Administration panel appears:

```
_____________________________________________________________________________
  Options  Exit  Help  Component
-----------------------------------------------------------------------------
TNCADMF               Network Data File 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.  Copy records
      2.  Data area offsets
      3.  Data area definitions
      4.  Data area identifiers
      5.  Data area tables
      6.  Data file records
      7.  Help text
      8.  Message text
      9.  Status of file
     10.  Summary report
     11.  Switch file mode




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

Figure 116. The Network Data File Administration Menu

3. Select choice 8, 'Message text'; a pull down window listing the active Components appears, as in the following example:

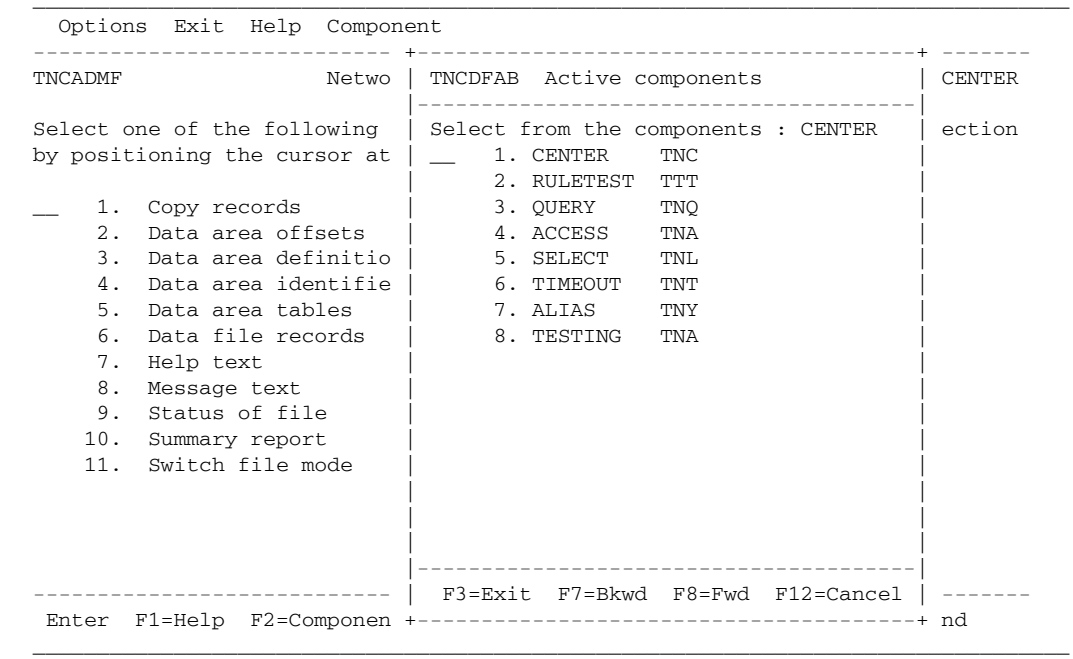

Figure 117. Active Components Select List

4. Select the Component that you wish to set the message account option for; the Network Center Message Numbers panel appears. The following figure shows the Message Numbers panel for Access:

```
TNCMSGT                  Network Center Message Numbers                ACCESS

Select a message by typing the number, or position the cursor at your choice.
Then Enter. The selected message will be displayed.

__    1. TNA1001  Access Component &comp is now active
      2. TNA1002  Session approved between &4 &6 : &1 < &8(16) > and &5 &7 : &
      3. TNA1003  Session rejected between &4 &6 : &1 < &8(16) > and &5 &7 : &
      4. TNA1005  No rule match, session between &3 &5 : &1 < &7(16) > and &4
      5. TNA1007  &1 IPaddr: &2(16) Port : &3 DNSname: &4(16)&5(16)
      6. TNA1008  &1 Name: &2 , Netid: &3 , Subarea: &4
      7. TNA1009  &1 Sscp: &2 , Alias: &3 , Aliasnet: &4
      8. TNA1010  Session allowed between &3 &5 : &1 < &7(16) > and &4 &6 : &2

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

Figure 118. Message List Panel for Access

This panel allows you to modify any Network Center message for Access. To scroll through the messages, use the F7 (Backward) and F8 (Forward) actions.

5. Select the message that you wish to add the account option to by placing the cursor on the desired message and pressing Enter; the message's Network Center Message text panel appears. The following example shows the Message Text panel for TNA1002:

```
TNCMSGR                  Network Center Message Text                  ACCESS

Type desired modifications in the displayed entry fields. Then Enter.

Message number   1002

Actions  . . .   Options _______ _______ _______ _______ _____

Class  . . . .   Notification

Language . . .   A US.English

Route codes  .   __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Descript.codes   __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Text . . . . .
Session_approved_between_&4_&6_:_&1_<_&8(16)_>_and_&5_&7_:_&2_by_rule_&3_____



------------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F12=Cancel   F16=Save  F20=Delete  F21=Command
```

Figure 119. Example Network Center Message Text Panel

6. Enter "Account" in the 'Actions' field, as in the following example:

```
_____________________________________________________________________________
TNCMSGR                  Network Center Message Text                  ACCESS

Type desired modifications in the displayed entry fields. Then Enter.

Message number   1002

Actions  . . .   Options Account _______ _______ _______ _____

Class  . . . .   Notification

Language . . .   A US.English

Route codes  .   __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Descript.codes   __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Text . . . . .
Session_approved_between_&4_&6_:_&1_<_&8(16)_>_and_&5_&7_:_&2_by_rule_&3_____



-----------------------------------------------------------------------------
 Enter  F1=Help  F3=Exit  F12=Cancel   F16=Save  F20=Delete  F21=Command
_____________________________________________________________________________
```

Figure 120. Network Center Message Text Panel with Account Option

Note: You can set the type of accounting record that is produced by the Network Center in the 'Accounting' field in the Center Options record. (To access the Center Options record, select choice 3, 'Center options' from Network Center Administration panel (TNCADMN).)

7. Press F16 (Save) to save the changes; a message appears stating that the record updated successfully, as in the following example:

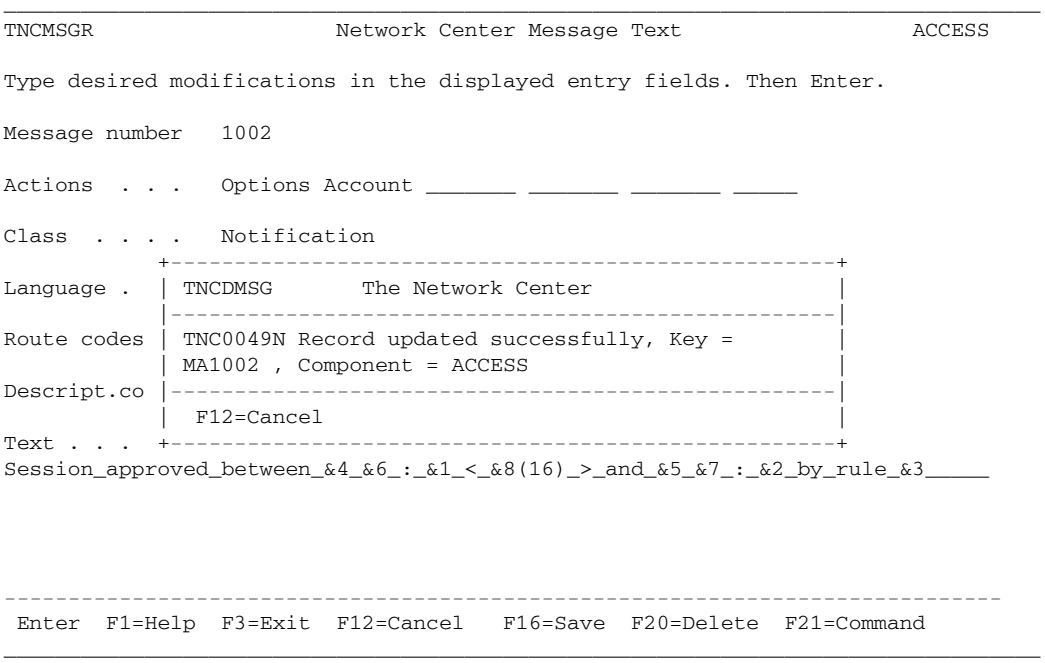

Figure 121. Confirmation Message

Note: For more information on modifying Messages, see the *Installation and Operations* manual (TNC-0003).

Part Two: Access Reference

Chapter 7. Access Administration Menu Choices

This chapter contains information for users who want to look up specific menu choices and functions within Access.

Menu choices are arranged alphabetically, as they appear on the Access Component Administration panel (TNCADMC). When applicable, each section in this chapter contains the following subsections:

(Title): (The Name of the menu item/function, followed by the tasks it lets you perform)

Definition: (What the menu item/function does)

Starting state: (Any prerequisite for using the menu item/function)

Access: (The keystrokes or commands that will get you to the menu item/function)

Step-by-step: (Abbreviated steps for using the menu item/function)

Tips: (Advice for increasing your efficiency when using this menu item/function)

Warnings: (Problems that might arise when you are using this menu item/function)

See also: (Where to go for more information)

Active Rules

Definition:
"Active Rules" lists the Rules, Rulesets, or Groups that have been activated in Access via the "Component Options" function. The list is displayed according to the Rule processing order. You may select any of the list items for viewing. The Rule and Ruletest definition panels display an additional field called 'Count', which displays the number of times a Rule has been matched since the last Rule reload.

Starting state:
Rules, Rulesets, and/or Groups have been activated via the "Component Options" function.

Access:
Select choice 1, 'Active Rules', from the Access Component Administration panel, TNCADMC; the TNCRULS panel appears.

Step-by-step:

1. Select a Rule, Ruleset, or Group from the list to display its definition panel. Use F7=Backward and F8=Forward to scroll through lists that exceed the screen. Use F11=Find to find a particular list item.

2. After selecting a list item, use F12=Cancel to exit the panel.

Tips:
To get help on an operand, place the cursor on the operand field and use the F1=Help action

Warnings:
If there are no active Rules, Access will issue an error message. Cancel the message if it is in a pop up window. You may then proceed as normal.

See also:
See "Component Options" on page 153 for information on defining the active Rules. See "Rule Processing" on page 26 for a definition of Rule processing.

Component Options

Definition:
"Component options" lets you specify the Rule, Ruleset, or Group that Access will use when processing session requests. This Rule, Ruleset, or Group is active when the Network Center initializes or restarts, and after a Rule Reload.

Most likely, you will use "Component Options" to specify a Group that contains all of the Rules, Rulesets, and Groups that you want to use to allow or deny session establishment.

"Component options" also contains a mode field that sets the Rules as active, dormant, or warn. (In "warn" mode Access issues messages but does not perform the action specified in the Rules while processing session requests.)

Starting state:
One or more Rules, Rulesets, or Groups have been defined via the "Rule definition" or "Define (value) Group" function.

Access:
Select choice 2, 'Component options' from the Access Component Administration panel, TNCADMC. The Component options panel appears.

Step-by-step:

1. In the 'Definition entity' field, enter the Rule, Ruleset, or Group that will be active. You may use a character mask (pattern matching);
2. In the 'Mode' field, enter the method of operation for the Active Rule, Ruleset, or Group.
3. Use F16=Save to save the options; a message should appear stating that the record updated successfully. You can also save the record using F3=Exit and selecting choice 1. If you do not wish to save the record at this time, do one of the following:
   - Use F3=Exit and select choice 2 to exit and return to the main menu.
   - Use F3=Exit and select choice 3 to return to the current panel.
   - Use F12=Cancel to return to the Access Component Administration panel.

Tips:

- To make the Component options active, use the "Rule Reload" function.
- For help, use the F1=Help action
- If you use a character mask in the 'Definition entity' field, any Rule, Ruleset, or Group that matches the mask will be included in the Rule hierarchy. However, pattern matching only applies to the first level that is satisfied. For example, if a Group matches the pattern mask, no pattern matching will be done for subordinate Rulesets or Rules.

Warnings:
Using the "active" mode causes Access to perform the action specified in each Rules Action operand: This will affect the processing of your system. If you have not yet tested the Rules, we recommend placing them in "warn" mode first.

See also:
See "Pattern Matching: Creating Rule Operand Masks" on page 27 for information on identifying a character mask.

Define (value) Group

Definition:
"Define (value) Group" produces a Group definition panel, which you can use to create a Group or Value Group. You can think of a Group as a container that allows you to place any combination of Rules, Rulesets, and Groups into order from the first Rule, Ruleset, or Group that you wish to be processed to the last. (In other words, a Group sets the Rule processing order for the items that it contains.)

A Value Group is a symbolic value that references a group of values. For example, you can create a Value Group to reference operands that are too diverse for pattern matching. Using Value Groups can reduce the need for creating or changing a Rule, Ruleset, or Group.

Access:
Select choice 3, 'Define (value) Group' from the Access Component Administration panel (TNCADMC); The Group definition panel appears.

Defining a Group

Starting state:
One or more Rules, Rulesets, and/or Groups have been defined via the "Rule definition" or "Define (value) Group" function.

Step-by-step:

1. Enter the name in the 'Name' field
2. Enter the title in the 'Title' field
3. In the numbered fields, enter the Rules, Rulesets, and/or Groups that you want the Group to contain according to their processing order.
4. After entering the values, use the F16=Save action to save the Group. You can also save the Group by using Exit=3 and selecting choice 1. If you do not wish to save the record at this time, do one of the following:
   - Use F3=Exit and select choice 2 to exit the panel
   - Use F3=Exit and select choice 3 to return to the Group definition panel
   - Use F12=Cancel to cancel the Group Definition panel and return to the Access Component Administration panel

Defining a Value Group

Starting state:
You have a group of Rule operands that are too diverse to match with pattern matching characters.

Step-by-step:

1. Decide which values need to be included in the Value Group. They can be operand values, Rule names, Group names, or other Value Group names.
2. In the 'Name' field, enter an ampersand ("&") immediately followed by the name for the Value Group.
3. In the 'Title' field, enter the title for the Value Group.
4. In the numbered fields, enter the Value Group's values. You may use pattern matching masks.
5. After entering the values, use the F16=Save action to save the Value Group. You can also save the record by using F3=Exit and selecting choice 1. If you do not wish to save the record at this time, use one of the following methods:
   - Use F3=Exit and select choice 2 to exit and return to the Access Component Administration panel
   - Use F3=Exit and select choice 3 to return to the current panel
   - Use F12=Cancel to cancel the Group Definition panel and return to the Access Component Administration panel.
6. If necessary, use the Value Group's 'Name' in the Rule operand, Ruleset, Group, or Value Group field that references the Value Group.

Tips:
For help on a field, use the F1=Help action

See also:
See "Pattern Matching: Creating Rule Operand Masks" on page 27 for information on defining pattern masks. See "Value Groups: Creating Symbolic Rule Operand Values" on page 29 for detailed information on defining and using Value Groups.

Display (value) Group

Definition:
The "Display (value) Group" function produces an alphabetical list of all the Groups defined within Access. You can select the Groups for viewing and modification: add or delete Groups or Value Groups, or simply browse to see which elements are defined within a Group or Value Group.

Starting state:
One or more Groups or Value Groups have been defined.

Access:
Select choice 4, "Display (value) Group" from the Access Component Administration panel (TNCADMC); the Group definition panel (TNCGRPS) appears.

Step-by-step:

1. Select the desired Group or Value Group from the list; its definition panel (TNCGRPD) appears. Use F7=Backward and F8=Forward to scroll through lists that exceed the screen.
2. If desired, delete or modify the Group or Value Group:
   - To delete the Group or Value Group, use the F20=Delete action.
   - To modify a field, overtype it with the new value.
   - To insert additional fields, use the '.I' prefix command.
   - To display a Rule, Ruleset, Group, or Value Group defined within the Group, place the cursor on its name and use the F11=Select action.
3. After modifying the Group or Value Group, use F16=Save to save the changes. You can also save the record by using F3=Exit and selecting choice 1. If you do not wish to save the record at this time, use one of the following methods:
   - Use F3=Exit and select choice 2 to exit the panel without saving changes.
   - Use F3=Exit and select choice 3 to return to the Group definition panel.
   - Use F12=Cancel to cancel the Group Definition panel and return to the Access Component Administration panel.

Tips:
For help, use the F1=Help action.

See also:
See "Modifying or Deleting Groups and Value Groups" on page 110 for details on modifying Groups.

Rule Counts

Definition:
"Rule Counts" displays how many times Access Rules have been matched (used) and places the results in the Message Queue for viewing. This helps you to gauge a Rule's frequency of use.

Starting state:
The active Rules must be in "active" or "warn" mode.

Access:
Select choice 5, 'Rule Counts' from the Access Component Administration panel; a message appears on the command line or in a pop up window stating that the Rule counts for Access have been logged.

Step-by-step:
After invoking the Rule counts function, go to the Message Queue to view the results. To access the Message queue:

1. Go to the main Network Center menu (TNCMENU) and select choice 1, 'Administration' to open the Administration menu.

2. From the Administration menu, select choice 6, 'Message queue'; the Message queue panel will appear. To scroll through the Message queue panels, use F7=Backward and F8=Forward. To reformat the message display, use F2=Prefix. To find a specific message, use F11=Find.

See also:
See the *Installations and Operations* manual (TNC-0003) for more information on using the Message Queue and other Administration panel choices.

Rule Definition

Definition:
The Rule definition panel contains operands that allow you to specify exactly which characteristics a particular VTAM session must match in order for it to be denied access or allowed access to a particular network resource.

Additionally, the Rule definition panel allows you to create Ruleset Rules using the Ruleset operand. A Ruleset Rule is a Rule that contains other Rules. It acts as a gateway for the Network Center to process the Rules it contains. Rulesets can decrease the time it takes to process Rules.

Access:
Select choice 6, "Rule definition", from the Access Component Administration panel; The Network Center Rule Definition panel (TNCRULD) appears.

Step-by-step:

1. Enter the Rule's name in the 'Name' field.

2. Enter the Rule's title in the 'Title' field.

3. Modify the operands. You may use pattern matching.

   To specify IP data: Enter "yes" in the IP data field. Keep the cursor pointed at the IP data field and use the F11=Selection action; the IP Data Display window appears. Enter the desired IP data. Then, use F16=Save to save the IP data information. Use F12=Cancel to cancel the message and return to the Rule definition panel.

   To define a Ruleset: Use the F11=Select action; the Ruleset Rule Name List panel appears. Enter the names of the Rules to be included in the Ruleset in the numbered fields, according to their processing order. Then, use F16=Save to save the Ruleset Rule Name List. Use F12=Cancel to return to the Rule definition panel.

   Note: You can also open the Ruleset Rule Name List panel by entering "yes" in the 'Ruleset' field in the Rule definition panel; the 'select' field appears. Enter any keyboard character into the select field; the Ruleset Rule Name List panel will then appear.

4. After defining the fields, use F16=Save to save the Rule. You can also save the Rule by using F3=Exit and selecting choice 1. If you do not wish to save the record at this time, do one of the following:

   - Use F3=Exit and select choice 2 to exit the panel without saving the changes
   - Use F3=Exit and select choice 3 to return to the Rule definition panel
   - Use F12=Cancel to exit the Rule definition panel

Tips:

- For help with operands, place your cursor on the field and use the F1=Help action.
- The Rule will not be active unless you make it part of the Rule hierarchy using the "Component options" function.
- If you define a Ruleset, you can display the Rule list whenever you open the Rule by placing your cursor on the 'Name' field and use the F11=Select action.

Warnings:
Access will issue an error message if you do not define the 'Name' first. If you receive the message in a pop up window, use F12=Cancel to cancel the message. You may then proceed with Rule definition.

See also:
See "Rule Operand Definitions" on page 10 for detailed descriptions of the Rule operands. See "Ruleset Rules" on page 22 for example Rulesets. See "Pattern Matching: Creating Rule Operand Masks" on page 27 for information on creating pattern masks for operand fields.

Rule Display

Definition:
The "Rule display" function displays an alphabetical list of all of the Rules and Rulesets defined within Access. You can select the Rules and Rulesets for modification or deletion.

Starting state:
One or more Rules have been defined.

Access:
Select choice 7, "Rule display" from the Access Component Administration panel; a list of all the current Rule(set) definitions appears.

Step-by-step:

1. Select a Rule or Ruleset from the Network Center Rules panel; the Rule or Ruleset's definition panel appears.
2. If desired, you may delete or modify the Rule:
   - To delete the Rule, use the F20=Delete action.
   - To modify a field, overtype it with the new value.
   - To delete a field, overtype it with blanks.
   - To display a Value Group that has been identified in one of the Rule's operand fields, place the cursor on the Value Group's name and use the F11=Select action.
3. Use F16=Save to save any changes. You can also save changes by using F3=Exit and selecting choice 1. If you do not wish to save the record at this time, do one of the following:
   - Use F3=Exit and select choice 2 to exit the panel without saving the changes
   - Use F3=Exit and select choice 3 to return to the Rule definition panel
   - Use F12=Cancel to exit the Rule definition panel
4. Use F12=Cancel to cancel the panel and return to the Network Center Rules list. You can also return to the Network Center Rules List using F3=Exit and selecting choice 1. If you do not wish to save the record at this time, do one of the following:
   - Use F3=Exit and select choice 2 to return to the Access Component Administration panel without saving any changes.
   - Use F3=Exit and select choice 3 to Return to the Rule definition panel.

- Use F12=Cancel to cancel the panel and return to the Network Center Rules list.

See also:
See "Modifying or Deleting Rules and Rulesets" on page 100 for details on modifying Rules.

Rule Reload

Definition:
"Rule reload" allows you to refresh the active copy of the Rule hierarchy with any changes that you have made to the Rules. You do not need to restart VTAM to reload Access Rules.

Starting state:
The active Rules have been set via the Component options function.

Access:
Select choice 8, 'Rule reload' from the Access Component Administration panel; the 'Reload function' window appears.

Step-by-step:
From the 'Reload function' window, select choice 1 to reload the Rules; a message appears stating that the Rules were reloaded. (If the message is in a pop up window, use the F12=Cancel action to cancel the message.)

Warnings:
This function will replace any previously defined active Rules with the currently defined active Rules.

See also:
For more information on making Rules active and using the Rule reload function, see "Activating Rules" on page 115.

Rule Test

Definition:
The "Rule test" function lets you create a sample "session" to test against the active Rules. When you issue the test function, Access will compare the "session" against each Rule as in actual Rule processing. The first Rule that matches the session conditions will be noted in a message.

Access:
Select choice 9, 'Rule test' from the Access Component Administration panel; the Network Center Rule Match Test panel appears.

Step-by-step:

1. In the Network Center Rule Match Test panel, enter the operand values for the "session" that you wish to test against the active Rules. You may use pattern matching characters.
2. After defining the session parameters, use F16=Test; a message appears via pop up window stating which active Rule matched the session. If no Rule is found that matches, you will receive a message stating so.
3. Press F12 (Cancel) to cancel the message. If a Rule matched the session, you will receive a Display function window: select choice 1 to display the Rule that matched the session; select choice 2 to return to the Network Center Rule Match Test panel.

See also:
See "Testing Rules" on page 124 for more information and techniques for testing Rules.

Statistics

Definition:
"Statistics" lists recent session activity for Access, including the number of requested sessions, denied sessions, approved sessions, allowed sessions (in warn mode), and currently active sessions.

Access:
Select choice 10, 'Statistics' from the Access Component Administration panel; a list of current session statistics appears. Use F3=Exit or F12=Cancel to return to the Access Component panel.

Chapter 8. Messages

Access messages are listed in order by the messages unique four-character value.

Constant information is displayed in **bold font** and variable information (filled in during execution) is displayed in in standard font.

General Network Center messages are documented in the *User's Guide* (publication TNC-0002).

TNA1001N Access Component [logical name] **is now active**

Explanation: The identified logical Component has initialized and is active.

System Action: Session checking will now begin according to the active rules.

Operator Response: None

Network Administrator Response: None

TNA1002N Session approved between [type] [netid: luname] [ipaddress] **and** [type] [netid: luname] [ipaddress] **by rule** [rulename]

Explanation: The Access Component has allowed a session between the identified logical units as a result of the identified rule. The [type] identifies if the OLU or DLU is an Alias, SLU, or PLU name.

System Action: The session will continue normally.

Operator Response: None

Network Administrator Response: None

TNA1003W Session rejected between [type] [netid: luname] [ipaddress] **and** [type] [netid: luname] [ipaddress] **by rule** [rulename]

Explanation: The Access Component has rejected a session between the identified logical units as a result of the identified rule. The [type] identifies if OLU or DLU is an Alias, SLU, or PLU name.

System Action: The requested session will be rejected. The terminal operator will not receive the requested subsystem. The actual result at the rejected session end will be a function of how the request was made (terminal operator initiated request, third party request, etc.)

Operator Response: None

Network Administrator Response: None

TNA1005N No rules matched, session between [type] [netid: luname] [ipaddress] **and** [type] [netid: luname] [ipaddress] **rejected**

Explanation: No rules can be located by Access for evaluation of the pending session. The [type] identifies if the OLU or DLU is an Alias, SLU, or PLU name.

System Action: The pending session is rejected.

Operator Response: None

Network Administrator Response: Session was not matched by any Rule in the Active Rule structure. Define an additional Rule to handle the session.

TNA1007T [PLU|SLU] **IPAddr**: [ipaddress] **Port**: [portnumber] **DNSName**: [dnsname]

Explanation: The identified logical unit has had a session approved or denied and the accompanying information is associated with the session.

System Action: The session continues to be approved or denied (as indicated by TNA1002 or TNA1003).

Operator Response: None

Network Administrator Response: None

TNA1008T [PLU/SLU] **Name:** [luname] **Netid:** [netname] **Subarea:** [subarea]

Explanation: The identified logical unit has had a session approved or denied and the accompanying information is associated with the session.

System Action: The session continues to be approved or denied (as indicated by TNA1002 or TNA1003).

Operator Response: None

Network Administrator Response: None

TNA1009T [PLU/SLU] **Sscp:** [name] **Alias:** [name] **Aliasnet:** [alias name]

Explanation: The identified logical unit has had a session approved or denied and the accompanying information is associated with the session.

System Action: The session continues to be approved or denied (as indicated by TNA1002 or TNA1003).

Operator Response: None

Network Administrator Response: None

TNA1010W Session allowed between [type] [netid: luname] [ipaddress] **and** [type] [netid: luname] [ipaddress] **due to warn mode**

Explanation: The identified session has been permitted to proceed because the applicable Access Rule or global setting is Warn. The [type] indicates if the OLU or DLU is an Alias, SLU, or PLU name.

System Action: The session is permitted to continue.

Operator Response: None

Network Administrator Response: None

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.

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 (LU) or other network resource in another network, guaranteeing that values remain unique amongst network nodes.

CMS: See *conversational monitor system*.

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

control vector: A portion of a defined SNA structure or sub-structure that contains information about an activity occurring within the network.

conversational monitor system (CMS): A virtual machine (VM) operating system that provides general interactive time sharing and program development facilities.

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*.

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*.

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.

DNSName: The Domain Name Service defined name for a TCPIP resource.

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

IPAddress: The unique TCPIP address (specified as dotted decimal) for a specific Logical Unit

ISTEXCAA: The name of the VTAM Session Management Exit (SME). See *Session Management Exit*.

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

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.

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

Network Administrator: In the Network Center, the person responsible for the installation and operations.

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 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 via the Network Center Server or TNCUTIL.

Network Director: North Ridge Software's Network Management software that provides control over the logical aspects of a VTAM network.

OLU: See *origin logical unit*.

origin logical unit (OLU): Origin Logical Unit. 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 (SLU)*.

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

pattern-matching character: The special characters, 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.

PLU: See *primary logical unit*.

PortNumber: The TCPIP address extension identifying a specific service on a TCPIP host

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*.

Query: A Network Center Component that allows authorized users to display and interrogate operational VTAM.

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. For example, in Access a Rule can be set to deny the establishment of a particular session or a type of session.

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.

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 an SLU). Contrast with *primary logical unit*.

Select: A Network Center Component that provides control over which VTAM path will be selected for a particular session. It can also be used to balance session traffic across the available paths.

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 ISTEXCAA.

SLU: See *secondary logical unit*.

SME: See *Session Management Exit*.

SSCP: See *system services control point*.

subarea: Within an SNA network, the unique value that represents a unique processing location (host or front end processor). A subarea includes a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

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

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

system services control point (SSCP): The key processing point within a VTAM domain that manages session initiation and termination.

The Network Center: See *Network Center*.

The Network Director: See *Network Director*.

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.

TSO: See *Time Sharing Option*.

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 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/SNA Console Support (VSCS): A VTAM component for the VM environment that provides an interface between SNA devices and the VM Control Program (CP). It allows SNA terminals to be virtual machine consoles.

VSCS: See *VM/SNA Console Support*.

VTAM: See *Virtual Telecommunications Access Method*.

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 multi-server solutions with a broad support for operating system environments including z/OS, OS/390, TPF, VS/ESA, CMS, and LINUX.

Index

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

V

W

Z