Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page vii.


This is a major revision of, and obsoletes, SH12-5810-01. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

This edition applies to Release 1 Modification Level 1 of NetView Access Services Version 2 (MVS/ESA) (Program Number 5695-036) and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers’ comments may be provided at the back of this publication, or you may address your comments to the following address:

NVAS Information Development
Rome Tivoli Laboratory
IBM Italia S.p.A.
Via Sciangai, 53
00144 Rome
Italy

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1987, 1997. All rights reserved.
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.
Contents

Notices ................................................................. vii
Trademarks ............................................................ vii

Year 2000 Considerations ........................................... ix

About This Book ....................................................... xi

What Is New in NetView Access Services Version 2.1.1 ........... xiii
  External Application Authorization ........................... xiii
  Direct Logon ....................................................... xiii
  Compact Application Selection Panel ........................ xiii
  Logmode Override ................................................ xiii
  REXX API Extensions ............................................. xiv

Part 1. Introduction .................................................. 1

Chapter 1. Introducing NetView Access Services .................. 3
  Functional Overview of NetView Access Services ............... 3
  The Administrators ................................................. 4
  Administration Hierarchy ......................................... 4
  Modes of Access .................................................... 5
  Relay Mode Access Parameters .................................. 5
  The Group Concept ................................................ 5
  Types of Groups .................................................... 6
    Public Groups .................................................... 6
    Normal Groups ................................................... 6
    External Groups ................................................ 6
  External Application Authorization ........................... 7
  Application Names ................................................ 8
  Application Fallback Function .................................. 8
  Planning Overview ................................................ 9

Chapter 2. The Pseudo Terminal Concept and the Logical Unit Names
  Table ............................................................... 11
  Pseudo Terminals ................................................. 11
    Pseudo Terminal Names ......................................... 11
  Shared ACBs ...................................................... 12
  Unique ACBs ...................................................... 13
  Individual ACBs ................................................ 14
  Pseudo Terminal Prefix and Maximum Sessions .................. 15
  The Logical Unit Names Table .................................. 17
  Nonshared LUNT Queues ......................................... 17
  Shared LUNT Queues .............................................. 17
  Dynamic Modification of LUNT Queues .......................... 18
  Adding a New Application ....................................... 18
  Deleting an Application or Removing It from the LUNT ......... 18

Part 2. Administration ................................................ 19
### Chapter 3. Planning the NetView Access Services Administration

- Preparing for a New Installation .................................................. 21
- System Administration ................................................................ 23
- Group Administration .................................................................. 25

### Performing the Initial Administration ........................................ 26

### Invoking the Administration Functions ....................................... 28
- Getting to the Administration Selection Panel ............................... 28
- Using Commands on the Administration Panels .............................. 29
- User Administration Tasks ............................................................. 29

### Chapter 4. System Administration Tasks ..................................... 31

- Defining an Application for the System ....................................... 31
  - Explanation of the Fields ......................................................... 32
- Displaying Data for an Application ............................................ 38
- Adding a New Application .......................................................... 38
- Deleting an Application ............................................................ 38
- Updating Data for an Application .............................................. 38
- Listing Applications .................................................................... 38

- Defining a Group .......................................................................... 38
  - Explanation of Fields ............................................................... 39
- Displaying the Characteristics of a Group .................................... 42
- Adding a New Group ................................................................... 42
- Updating the Characteristics of a Group ...................................... 42
- Listing the Groups That Are Defined to NetView Access Services .... 42
- Deleting a Group ......................................................................... 43
  - Criteria for Defining Groups ................................................... 43

- Assigning an Application to a Group .......................................... 44
  - Explanations of the Fields ....................................................... 44
- Displaying the Attributes of a Group Application ......................... 47
- Adding an Application for a Group ............................................ 47
- Deleting an Application from a Group ....................................... 47
- Updating an Application for a Group ......................................... 47
- Listing Applications .................................................................... 47
- Listing Groups ............................................................................ 47
  - Providing a Free Selection Field .............................................. 48
  - Criteria for Assigning Applications to Groups ........................... 48

- Defining an Administrator ............................................................ 48
  - Explanation of Fields ............................................................... 49
- Displaying Whether a User Is an Administrator .......................... 50
- Defining Administrators ............................................................. 50
- Updating the Characteristics of an Administrator ....................... 50
- Deleting Administrators ............................................................ 51
- Listing Administrators ............................................................... 51
- Listing Groups ............................................................................ 51

- Sending a General Broadcast Message ....................................... 51
  - Explanation of Fields ............................................................... 52
- Entering a General Broadcast Message ....................................... 52
- Displaying a General Broadcast Message .................................... 53
- Updating a General Broadcast Message ...................................... 54
- Deleting a General Broadcast Message ....................................... 54

- Sending Selective Broadcast Messages ...................................... 54
- Defining BIND User Data for Applications ................................. 54
  - Explanation of Fields ............................................................... 55
  - Displaying BIND Data ............................................................. 55
Activating a Recording as a Group-Wide or System-Wide Profile ........  95

Chapter 9. Using BIND User Data to an Application ....................  97
What BIND User Data Is ........................................  97
Defining BIND User Data ..........................................  97
  Structured BIND User Data ...................................  98
  Unstructured BIND User Data ..................................  100
Entering BIND User Data ...........................................  101
Variables for BIND User Data ....................................  101

Part 3. Batch Load and Reporting Utility ..................................  103

Chapter 10. Using the Batch Load and Reporting Utility .................  105
Functional Summary ..............................................  105
Running the Batch Load and Reporting Utility ..........................  106
Input Parameter Data Set ............................................  109
Starting Batch Load ................................................................  109
Batch Load Return Codes .............................................  109
Batch Load Restrictions ..................................................  109
Batch Load Options .....................................................  110
Command Statements .....................................................  111
  Reading the Syntax Diagram ......................................  111
  Rules for Writing Batch Load Commands ..........................  114
  Commands for the System Application Profile Data Set EMSSRTS ....  116
  Commands for the Group Profile Data Set EMSGPRF ..............  119
  Commands for the Group Application Profile Data Set EMSSRTG ....  123
  Commands for the User Profile Data Set EMSSRTU ...............  128
  Commands for the Administrator Authorization Profile Data Set EMSGAL  136
  Commands for the BIND User Data Profile Data Set EMSPLDT ......  138
LIST Output Formats ......................................................  139
  SYSTEM_APPLICATION Profiles EMSSRTS .......................  139
  GROUP Profiles EMSGPRF .........................................  140
  GROUP_APPLICATION Profiles EMSSRTG .........................  141
  USER Profiles EMSSRTU ............................................  142
  ADMINISTRATOR Profiles EMSGAL ..................................  144
  BIND_USER_DATA Profiles EMSPLDT ..................................  144

Chapter 11. Summary of Dependencies ..................................  145

Part 4. Appendix ..............................................................  147

Appendix. Forms to Help You Plan for Your Installation ...............  149

Part 5. Glossary, Bibliography, and Index ..................................  153

Glossary ...........................................................................  155

Bibliography ......................................................................  159

Index ................................................................................  161
Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594, USA.

Trademarks

The following terms, denoted by an asterisk (*) in this publication, are trademarks of IBM Corporation in the United States or other countries or both:

- ACF/VTAM
- CICS
- IMS
- MVS/ESA
- OfficeVision/MVS
- OS/390
- System/370
- VTAM
- IBM
- NetView
- RACF

Tivoli is a trademark of Tivoli Systems, Inc.

Other company, product, and service names which may be denoted by a double asterisk (**), may be trademarks or service marks of others.
NetView Access Services is able to handle dates between the 20th and 21st centuries, and to provide uninterrupted functionality across the year 2000 boundary.

On the Broadcast panel, where the user is asked to enter a date, NetView Access Services provides a 4-digit field.

When, instead, a last update date for each NetView Access Services resource (applications, groups, and users) is included on a panel, this is a 2-digit field. This does not create ambiguity as the last update date is always prior to the current date.

A 2-digit year field is also used on the Logon and Application Selection panels. This refers to the current date and therefore creates no ambiguity.
About This Book

This book shows you how to administer the IBM* licensed program NetView Access Services Version 2 running under the MVS/ESA* operating system. NetView Access Services Version 2 is a member of the NetView* family of IBM licensed products. It provides a single access control system for users of 3270-type terminal devices in a Systems Network Architecture (SNA) network and supports the management of a number of applications from a single terminal.

This book is intended for systems engineers, installation personnel, and staff supervisors who administer NetView Access Services Version 2 in an SNA network.

It contains information about planning for the installation and the administration of NetView Access Services Version 2.

You should have some knowledge of Virtual Telecommunications Access Method (VTAM*) and be familiar with the applications that are in use in your installation. If you do not yet know NetView Access Services, you should read the NetView Access Services Version 2 User’s Guide before you start any administration tasks.

What Is New in NetView Access Services Version 2.1.1

Four new features have been included in NetView Access Services Version 2 Release 1 Modification Level 1. These are:

- External Application Authorization
- Direct Logon
- Compact Application Selection panel
- Logmode override.

The set of functions available with the REXX API feature has been extended.

External Application Authorization

This feature enables NetView Access Services to use the application access information defined in the RACF database when building the Application Selection Panel for each user. The NetView Access Services administrator, therefore, need no longer create security definitions for applications in NetView Access Services as all this information will be taken from the RACF definition for the application.

This enhancement improves the synergy between NetView Access Services and RACF, reduces the NetView Access Services administration time, and hence improves the usability of the NetView Access Services product.

Direct Logon

This feature introduces the ability to define terminals that are to be logged on to NetView Access Services without the logon panel being displayed. This feature allows the NetView Access Services Application Selection panel to be displayed directly when terminals are powered on.

Compact Application Selection Panel

This is an additional format in which to display the NetView Access Services Application Selection panel. With this new format you can display up to 42 applications on a single screen. There is no longer a maximum limit of 99 applications. The use of this new format can be configured for each group.

Logmode Override

This feature allows the NetView Access Services administrator to explicitly specify a logmode to be used by NetView Access Services when establishing a session with an application.
REXX API Extensions

Three new REXX API calls have been added to allow users to accomplish the following tasks from REXX execs:

- Get a list of all the terminals attached to NetView Access Services, regardless of which screen they are currently displaying.
- Get a list of all the terminals that are currently displaying the NetView Access Services Logon Panel.
- Send a message to all the terminals attached to NetView Access Services, regardless of which screen they are currently displaying.
Part 1. Introduction

This part describes what NetView Access Services is, and describes the NetView Access Services pseudo terminal and group concepts.
Chapter 1. Introducing NetView Access Services

NetView Access Services is designed to make it easier for users of 3270-type terminals in an SNA network to gain access to applications while ensuring data security in the network. The user can gain concurrent access to several applications, and easily move between them.

Applications handled by NetView Access Services can be systems such as Customer Information Control System (CICS*) or Information Management System/Virtual Storage (IMS/VS), subsystems such as OfficeVision/MVS*, or transactions in a subsystem. For simplicity, the term application is used throughout this book.

Functional Overview of NetView Access Services

NetView Access Services runs under MVS/ESA and uses VTAM to communicate with applications. It provides the following functions for terminal users:

- Simplified application selection
- Multiple concurrent application sessions
- Application status indication
- Automatic logon to, and logoff from, applications
- Disconnect and keep sessions active
- Data copy from one application to another
- Panel copy to printer
- Shared sessions with another user
- Multiterminal sessions
- Dynamic multilingual support
- Broadcast and application message indication
- Online Bulletin Board
- Compact Application Selection panel.

For further information, refer to NetView Access Services Version 2 User’s Guide.

The following functions secure the network and applications against unauthorized use:

- Single access point for all applications
- User access administration
- Additional installation-wide exits for logon authorization and session initialization
- Security time-outs for terminal and applications
- Direct logon for access control policy based on terminal ID.

NetView Access Services also provides the following additional features:

- Resource sharing
- Customization of message and panel text
- Interface to NetView Performance Monitor
- NetView alert in case of an abend
- VSAM locking when updating VSAM data sets
- Refresh function for activating external changes to VSAM data sets while NetView Access Services is running
- Application fallback processing to provide a backup application for an application that is not available
• Inactivity timeout for terminals displaying the NetView Access Services Logon panel
• Selective broadcast authorization for any user who is not a system administrator
• REXX Application Programming Interface for automated user actions such as automatic logon to several applications.

The Administrators

Each NetView Access Services provides for the following types of administrator:

System Administrator
A system administrator performs general administration for the whole NetView Access Services system. The system administrator’s tasks include defining each application to NetView Access Services, deciding how many and what types of groups there will be, assigning the applications to be used by each group, and defining one or more administrators for each group. The system administrator is also responsible for sending general broadcast messages and refreshing profiles. The system administrator can also send selective broadcast messages and can authorize any user to use this function.

Group Administrator
One or more group administrators are responsible for all information necessary for the running of a group. The group administrator’s tasks include assigning users to the group, and setting up access parameters for the applications they are authorized to use.

Broadcast Only Administrator
The system administrator can authorize any user to be a broadcast only administrator. This allows the user to send selective broadcast messages.

Administration Hierarchy

Several NetView Access Services application access parameters are defined on different administration levels. For example, the mode of access for an application can be defined at system administrator, group administrator, and user levels. A parameter defined on an upper administration level can restrict the validity of the same parameter defined at a lower administration level. NetView Access Services does not check the validity of a defined parameter across the administration levels.

For parameters related to security, for example, authorization to record logon profiles, or to gain access to applications in different modes, the definition at the higher administration level overrides any definition at a lower administration level during the time that NetView Access Services is running. For other parameters, such as application selection ID or message received indication, the user-defined values take effect. The group defaults are then used only for those users who have not defined their own values.

Any redefining of parameters at system or group level takes effect only for those users who log on to NetView Access Services after the changes have been processed. Users who are already logged on to NetView Access Services continue working with the old parameter definition until they log off.

Refer to Part 2, “Administration” on page 19 for detailed descriptions of the various application access parameters that can be defined at system and group adminis-
trator levels. Refer to NetView Access Services Version 2 User’s Guide for those that can be defined at the user level.

Modes of Access

NetView Access Services offers two types of access a user can have to an application. These are relay mode and pass mode.

Relay Mode

In relay mode, all communication with an application is controlled by NetView Access Services. All the NetView Access Services functions such as jumping among applications and copying data from one application to another are available to the user.

Pass Mode

Using an application in pass mode bypasses NetView Access Services and therefore all relay functions. This mode can be used when a user only needs to use a particular application and also to save system resources.

Whether an application can be used in pass mode, relay mode, or both modes is defined by the system and group administrators. The system administrator defines the access mode for applications when defining each application to NetView Access Services, and assigning an application to a group. The group administrator defines the access mode when defining a user to a group.

Relay Mode Access Parameters

NetView Access Services has some access parameters that can be used only when an application is in relay mode. For pass mode, any values for these parameters are ignored. The following is a list of these parameters in alphabetical order:

- ACB type
- Active profile
- Alternative sequences
- Automatic logon
- Command key
- Command prefix
- Copy keys
- Escape key
- Idle time
- Interruptive broadcast messages
- Jump key
- Logon profile type
- Maximum sessions
- Printer
- Print key
- Pseudo terminal name
- Pseudo terminal prefix
- Record authorization
- Shareable

The Group Concept

The users of NetView Access Services are assigned to use applications in one or more groups. As shown in Figure 1, each group has a particular set of applications assigned to it. Through this group concept, the administration work can be divided among a number of administrators, and access to applications and authorizations can be given to, or restricted from, a set of users. As the person responsible for defining groups, the system administrator must determine the criteria used to do this. For example, all applications used in a department could be assigned to
one group, and the users in that department assigned to use particular applications in the group.

Types of Groups

The system administrator must specify a group type when defining a group to NetView Access Services. The following group types exist in NetView Access Services:

- Public groups
- Normal groups
- External groups

Public Groups

Users of a public group do not need to be defined explicitly to that group before they can log on to it. Once logged on to a public group, users can get access to all applications in this group.

You can specify the way users navigate among the applications, that is, the set of values defined in NetView Access Services for certain access parameters. However, users can change some of these parameters for the duration of the current session; such changes are not stored permanently and therefore do not require additional storage space.

Public groups are particularly suited for large, fast-changing numbers of users; for example, for demonstration or training purposes. Generally, such groups do not need to make use of all the security features offered by NetView Access Services.

Normal Groups

Normal groups must be defined to NetView Access Services by an administrator. When this is done, the administrator defines the applications to be contained in each group and, finally, the applications each user can use within each group. If the administrator has defined session parameters for users and applications, users have the opportunity to change these if they wish. These changes can be made permanent and can be stored in the control files of NetView Access Services and reused at any time.

Normal groups offer a high degree of security. They are suited for installations that want to make full use of the security features built into NetView Access Services. The use of Normal groups is also suitable for installations not wishing to use an external security manager for additional NetView Access Services administration, or wanting to separate the NetView Access Services definitions from their external security manager, for example, Resource Access Control Facility (RACF*).

External Groups

These groups work together with an external security-management program, such as RACF, to identify the applications to which a user can get access. The association of users to groups can be defined in an external database rather than within NetView Access Services.

External groups are particularly suited for installations that already maintain a large database of users and that do not want to duplicate this information for NetView Access Services. NetView Access Services provides a user exit (EMSEADEX) for
this purpose. For information on this user exit, refer to *NetView Access Services Version 2 Customization*. Different group types can coexist in NetView Access Services, but each group can have only one group type at a time. The system administrator must define applications for each type of group.

The following shows an example of a setup for a normal or external group. As can be seen, user A has access to application 1 and 2 in group 1, and applications 2, 3, and 4 in group 2.

![Diagram of group concept in NetView Access Services](image)

*Figure 1. The Group Concept in NetView Access Services*

---

**External Application Authorization**

If the External Application Authorization feature is used, the RACF access information is used to build a list of applications for each user, instead of the NetView Access Services definitions. This list includes all the applications, among the ones defined to NetView Access Services, that meet the following criteria:

- The user is on the RACF access control list for the Generic Resource Profile of class APPL for the application.

There is no need to assign the applications to groups and to users, as only the RACF information is used. In this way, the time required to administer the system is considerably reduced, as the access control information is stored in only one place. NetView Access Services uses the default values for the parameters on the
When defining applications to the system, the system administrator must provide the following information:

- **System-Internal Name**
  A name that associates the application with the VTAM application name. This name is maintained by NetView Access Services and does not have to be the same as the name specified on the APPL definition statement used by VTAM. For example, a CICS application with the VTAM application name IABCXYZ can be given the system-internal name CICS.

- **Primary LU Name**
  The VTAM application network name as defined by the APPL definition statement.

When assigning applications to the groups, the system administrator must provide the following information:

- **Application Name**
  The group-wide name of the application. This is the name of the application as it is known to the group. This name can be different from the **System-Internal name** that is used to define the application on the Define an Application for the System panel. For example, the application with the system-internal name TSO can be given the application name YOURTSO.

- **System-Internal Name**
  The application name as it is known to the NetView Access Services system.

The group administrator and the users enter the application name on a number of panels. It is the group-wide name of an application, as set by the system administrator when assigning an application to a group. This name must then be used to refer to the application within the group.

For further information, refer to *NetView Access Services Version 2 Customization*.

**Application Fallback Function**

NetView Access Services provides an Application Fallback Function (AFF) that allows an application to be defined as a backup for another application. In turn, a backup application can be defined for the backup application itself so that a chain or ring of applications can provide backup support for each other. A backup application can be defined for each application regardless of whether the application is run in pass mode or relay mode.

If a user tries to request a session with an application and the application is currently not available, the session request is automatically routed to the backup application. If the backup application is not available, the session request is routed to...
its backup application, if one has been defined, and so on. If users logging on to
an application are to be made unaware of the fallback processing, identical applica-
tions must be used to give backup support to each other. These applications must
share a common security database, or provide a means of routing a new password
to each other.

Planning Overview

Before NetView Access Services is installed, it is important that the system admin-
istrator and the installer know the following:

- How many applications will be defined
- What the network names are for the applications
- How many pseudo LUs are to be defined to VTAM and what their names are
- How the applications will be assigned to groups
- How many groups there will be
- The group types to be used
- Who will be the administrator for each group
- How many users there will be and how they should gain access to the applica-
tions
- Which terminals are to be used and how they are identified.
Chapter 2. The Pseudo Terminal Concept and the Logical Unit Names Table

This chapter contains information on the pseudo terminal concept used in NetView Access Services. It also provides information on the Logical Unit Names Table (LUNT).

Pseudo Terminals

NetView Access Services emulates a 3270-type terminal for each relay-mode session with an application. This emulated terminal is an Access Method Control Block (ACB), and is called a pseudo terminal.

Pseudo Terminal Names

Each pseudo terminal has its own name that is used when establishing a session with the application. NetView Access Services interacts with an application as if it were a user's terminal. Figure 2 shows a user's terminal connected to three applications using a Unique ACB. Unique ACBs are described in “Unique ACBs” on page 13.

Figure 2. Pseudo Terminals for a Unique ACB. The user has access to three applications, each of which has a pseudo terminal with a unique name.

What the pseudo terminal is capable of depends on the type of ACB that the application can support and on how this ACB is defined to NetView Access Services.
Shared ACBs

If an application can support parallel sessions using a single ACB, the system administrator must specify this to NetView Access Services. An example is TSO, as shown in Figure 3. This is only possible when several users can use the same ACB to gain access to the application, in which case it is referred to as a Shared ACB.

![Diagram of Using a Shared ACB to Gain Access to TSO]

Figure 3. Using a Shared ACB to Gain Access to TSO

If the application cannot support this capability, NetView Access Services uses either a Unique or Individual ACB for each relay-mode session with the application.
Unique ACBs

You define an ACB type of Unique when the ACB can be used for only one session with one application, as shown in Figure 4.

The system administrator specifies a pseudo terminal prefix that is used to form a pool of pseudo terminal names. The names are created by taking this prefix and adding digits to get 8-character names. The number of digits added depends on the number of characters in the prefix. For example, if the prefix is 5 characters long, the numbers span from 1 to 999. For information on the maximum sessions value, refer to “Maximum Sessions” on page 35.

The same pseudo terminal prefix can be used for several applications with ACB type Unique. In this case the applications share the pool of pseudo terminal names. The number of names in the pool is determined by the number of maximum sessions of the application with the highest number of maximum sessions.

![Figure 4. Using Unique ACBs](image-url)
Individual ACBs

Individual ACBs allow simultaneous access to several applications using a single pseudo terminal, as shown in Figure 5. A pool of pseudo terminal names is formed from the specified terminal prefix. A pseudo terminal name with the following properties is assigned to a user:

- A pseudo terminal name in the pool is used for concurrent access to all the user’s applications with ACB type Individual.

- A pseudo terminal name is assigned to a user when the user selects the first application session. It is released when the last session of that user is terminated.

- The user has exclusive use of the name at this time. Another pseudo terminal name is used if the user selects a second session with the same application.

Figure 5. Using Individual ACBs

Therefore, the type of ACB that you select depends on the characteristics of the application. Because most applications cannot share the ACB (NetView Access Services and TSO being exceptions), most ACB types will be Unique or Individual.
Pseudo Terminal Prefix and Maximum Sessions

When defining an application to NetView Access Services, the system administrator specifies values for the Pseudo Terminal Prefix and the Maximum Sessions. For Shared ACBs, the pseudo terminal prefix is used as the pseudo terminal name for all relay mode sessions with the application. The Maximum Sessions value controls the number of sessions that can be established using that single ACB. For Unique or Individual ACBs, these two parameters are used to derive the pseudo terminal names.

A generic pseudo terminal name can also be specified. This enables the pseudo terminal name for an application to be derived from the name of the terminal that requests the session. A pool of pseudo terminal names is not generated.

For further details of these parameters, see “Defining an Application for the System” on page 31.

Assigning Pseudo Terminal Names

There are several methods that can be used to assign pseudo terminal names for users, as shown in the following. Figure 6 on page 16 gives an overview:

1. Using Shared ACBs

   If an application can support parallel sessions using a single ACB, as shown in Figure 3 on page 12, and ACB type of Shared is specified, then a pseudo terminal name can be entered in the Pseudo Terminal Prefix field.

2. Sharing Pseudo Terminal Names

   For ACB types of Unique and Individual, the pseudo terminal name is formed from a pool of names derived from the pseudo terminal prefix. This can be:

   a. A pseudo terminal prefix for each application. This means that each application is assigned a pool of pseudo terminal names that is shared among the users to establish sessions with that specific application.

   b. A single prefix for all, or a subset of, NetView Access Services applications. This means that all applications share one single pool of pseudo terminal names. To take advantage of ACB type Individual, a shared pool of pseudo terminal names must be used.

3. Using a Generic Pseudo Terminal Name

   A generic name can be specified in the Pseudo Terminal Prefix field when defining an application for a system, using one or more asterisks. This name is then combined with the actual terminal name to form the pseudo terminal name.

4. Assigning a Pseudo Terminal Name to a User

   The group administrator assigns a pseudo terminal name to a user for a specific application. Therefore, each user can have a set of unique pseudo terminal names that are used to gain access to applications.

   A session establishment user exit routine EMSESEEX can also be written to assign a pseudo terminal name. For further information, refer to NetView Access Services Version 2 Customization.
Advantages and Disadvantages

Each of these techniques has advantages and disadvantages. The following lists some of these:

- Sharing a pool of pseudo terminal names has the following advantages:
  - It requires less administrative coordination
  - It reduces the potential impact of application subsystem definitions
  - It potentially saves VTAM virtual storage and network resources
  - It potentially improves access to applications due to the availability of pseudo terminal names in the pool.

- Sharing a pool of pseudo terminal names has the following disadvantage:
  - It does not provide a permanent association between the pseudo terminal and a user.

- Dedicating pseudo terminal names to users has the following advantages:
  - Secure access to applications is guaranteed, because pseudo terminal names are always associated with the user
  - It provides a permanent association of a user to a pseudo terminal name.

- Dedicating pseudo terminal names to users has the following disadvantages:
  - Considerable administrative effort and coordination is required
  - It requires many VTAM definitions.
The Logical Unit Names Table

NetView Access Services maintains a list of all the secondary logical unit (SLU) names available for use with a relay mode application with an ACB type of Unique or Individual. This list is known as the Logical Unit Names Table (LUNT). It is an internal table used by NetView Access Services, and is subdivided into three queues:

- Unused LU names
- Used LU names
- LU names that have had a problem detected against them.

**Unique ACBs:** When the LUNT is initially built, a chained list of all the possible LU names is created. This is the unused queue. The problem and used queues are empty at this point. When a user logs on to a relay mode application, the first entry is taken off the unused queue and the name is suffixed to the pseudo terminal prefix. The name achieved is used to allocate the session. The name is then removed from the unused queue and placed on the used queue. When a user next logs on to an application, the next entry is taken from the unused queue to form the secondary logical unit (SLU) name.

When a user logs off the relay session, or it is timed out, the LU name is removed from the used queue and returned to its place in the unused queue. If, however, the session could not be bound or terminates in error, then the LU name is taken from the used queue and placed at the end of the problem queue.

When the unused queue has been exhausted, the first entry of the problem queue is taken and put back to the used queue. If both the problem and unused queues are empty, then further logons are rejected. The operator and user are informed that maximum sessions have been reached for the application.

**Individual ACBs:** For ACB type Individual, NetView Access Services first searches for a reusable ACB before selecting the next unused one.

**Nonshared LUNT Queues**

Each application defined to NetView Access Services can be given its own unique pseudo terminal prefix. This means that each application has its own LUNT and the system programmer must define all the possible LU names to VTAM.

**Shared LUNT Queues**

It is possible for several applications to point to a single LUNT and to use entries from it on a first in, first-out (FIFO) basis. To set up such a queue, each application must be defined with the same pseudo terminal prefix. They must all have ACB type defined as U or I and Access Mode as R or B.

Certain applications, for example CICS, require that all terminals that can be logged on to are defined in a table to that application. CICS uses the Terminal Control Table (TCT) for this purpose. When an installation has several CICS systems, it is common practice for them to share the same TCT. Each system is then defined separately to NetView Access Services. If each one had a different pseudo terminal prefix, then CICS TCT does not need to have each set of NetView Access Services SLU names defined to it. This can be achieved by the use of shared queues.
**Note:** The LUNT is large enough to accommodate the highest maximum sessions of an application sharing it. For example, if applications are defined with maximum sessions of 20, 15, and 40, then the LUNT is built with 40 entries. In the first instance the maximum sessions message can be given if 20 sessions are already active or if a total of 40 sessions had been bound for all applications sharing the queue. The maximum sessions value can be more than 40 if ACB type Individual is used.

**Dynamic Modification of LUNT Queues**

A LUNT is built whenever an application is defined with ACB type U or I and access mode R or B. After that, it is built whenever NetView Access Services is started up.

**Adding a New Application**

If a new application is defined to share a LUNT that is already in use, it is simply attached to it. If a user then logs on to the new application, the next available number is used for this user. If the new application has a maximum sessions value greater than the size of the existing LUNT, then the LUNT is extended, and these additional entries are available to all applications sharing the LUNT.

**Deleting an Application or Removing It from the LUNT**

If an application is deleted, or the pseudo terminal prefix is changed, or its access mode or ACB type is altered, then its LUNT is deleted. The LUNT is only physically removed from storage if no more applications are sharing it.

If the application with the largest maximum sessions value is deleted, the LUNT is shortened to the size of the next largest maximum sessions value. Any LU numbers greater than this new limit, that are in use, are discarded when they are logged off.
This part of the book describes how to plan the initial administration of NetView Access Services and how to carry out the tasks of system and group administrators. It also contains information on security and user profiles. Examples of administration show you how the tasks are carried out.
Chapter 3. Planning the NetView Access Services Administration

The following provides an example of planning the administration for a NetView Access Services installation. Forms to organize the necessary information are provided in Appendix, “Forms to Help You Plan for Your Installation” on page 149. This includes:

- Preparing for a new installation
- Performing the initial administration
- Invoking the administration functions.

Preparing for a New Installation

When NetView Access Services is installed for the first time, you must define applications to the system, and specify which users are to have access to those applications. This is a system administrator task and requires some planning for your NetView Access Services installation.

If using External groups, then your installer may have allowed access to an existing list of users. For Public groups no definition of users is necessary.

Here is an example of planning for an imaginary environment using Normal groups. In this environment there are seven applications, arranged into two groups. One group is called GROUP1 and the users assigned to use the applications in the group are mostly end users. They have access to the following applications:

- DWCICS
- IMS
- TSO
- OFFICE
- VM1.

The other group is called SYSP1. The users assigned to use applications in this group are mostly system programmers. They have access to the following group of applications:

- TSO
- IMS
- CICS
- NetView.

In this example, there is to be one group administrator for each group, and two system administrators.

Appendix. “Forms to Help You Plan for Your Installation” on page 149 contains forms you can use to prepare for your installation. This example shows you how to use these forms.
Figure 7 shows briefly how administrators would set up the system for the imaginary environment previously described.

Define the applications to NetView Access Services

Define group GROUP1 and its administrator

Assign applications to GROUP1 and give them group-wide access parameters

Assign the users to GROUP1, and give them access parameters. Define logon profiles.

Define group SYSP1 and its administrator

Assign applications to SYSP1 and give them group-wide access parameters

Assign the users to SYSP1, and give them access parameters. Define logon profiles.

Figure 7. Planning for Your New Installation
System Administration

Note: The values used in the tables are only examples.

1. First decide which applications will be used, and which system parameters apply to each. In the following tables, the column names relate to the fields of the panel you get when you choose option 4, Define an Application for the System, on the Administration Selection panel. This option is described in “Defining an Application for the System” on page 31.

<table>
<thead>
<tr>
<th>Application</th>
<th>System Internal Name</th>
<th>Primary LU Name</th>
<th>ACB Type</th>
<th>TPN of ASR</th>
<th>Pseudo Terminal Prefix</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWCICS</td>
<td>CICS1</td>
<td>ACB CICS1</td>
<td>U</td>
<td>–</td>
<td>EMSYAC</td>
<td>R</td>
</tr>
<tr>
<td>IMS</td>
<td>IMSP</td>
<td>ACB IMS</td>
<td>U</td>
<td>–</td>
<td>EMSYAI</td>
<td>R</td>
</tr>
<tr>
<td>TSO</td>
<td>TSOP</td>
<td>ACB TSO</td>
<td>U</td>
<td>–</td>
<td>EMSYAT</td>
<td>R</td>
</tr>
<tr>
<td>OFFICE</td>
<td>VM2</td>
<td>ACB VM2</td>
<td>U</td>
<td>–</td>
<td>EMSYAT</td>
<td>R</td>
</tr>
<tr>
<td>VM1</td>
<td>VM1</td>
<td>ACB VM1</td>
<td>U</td>
<td>–</td>
<td>EMSYAT</td>
<td>R</td>
</tr>
<tr>
<td>CICS</td>
<td>CICS2</td>
<td>ACB CICS2</td>
<td>U</td>
<td>–</td>
<td>EMSYAC</td>
<td>B</td>
</tr>
<tr>
<td>NetView</td>
<td>NETVIEW</td>
<td>ACB NETV</td>
<td>U</td>
<td>–</td>
<td>EMSYAF</td>
<td>B</td>
</tr>
</tbody>
</table>

2. Next define each group and the characteristics of the group. The column names in the following tables relate to the fields of the panel you get when you choose option 5, Define a Group, on the Administration Selection panel. This option is described in “Defining a Group” on page 38.

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Account Number</th>
<th>ASP Format</th>
<th>Number of Sessions</th>
<th>Multi-terminal Access</th>
<th>Shared Session Response</th>
<th>Logon REXX Exec</th>
<th>Logoff REXX Exec</th>
<th>Printer</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUP1</td>
<td>N</td>
<td>U123</td>
<td>N</td>
<td>N</td>
<td>G</td>
<td>TOM</td>
<td>REGGY</td>
<td>3286A</td>
</tr>
<tr>
<td>SYSP1</td>
<td>N</td>
<td>P123</td>
<td>N</td>
<td>Y</td>
<td>S</td>
<td>SMITHY</td>
<td>BOBBY</td>
<td>3286B</td>
</tr>
</tbody>
</table>
3. When you have defined the applications and the groups, you must assign applications to each group. You do this using option 6, Assign an Application to a Group, as described in “Assigning an Application to a Group” on page 44.

4. Define a group administrator for each group, any other system administrators and those users that can broadcast selective broadcast messages, using option 7, Define an Administrator. This option is described in “Defining an Administrator” on page 48.
Group Administration

Note: The values used in the tables are only examples.

1. As group administrator, for each application decide on certain group parameters. Use option 2, Maintain Group Parameters, on the Administration Selection panel, as described in “Maintaining Group Parameters” on page 64. The following example shows parameters for GROUP1.

<table>
<thead>
<tr>
<th>GROUP1</th>
<th>Application Description</th>
<th>Default ID</th>
<th>Jump Key</th>
<th>Msg. Received Indicator</th>
<th>Logon Profile Type</th>
<th>Automatic Logon</th>
</tr>
</thead>
<tbody>
<tr>
<td>DWCICS</td>
<td>DW/CICS Relay mode</td>
<td>1</td>
<td>PF18</td>
<td>N</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>IMS</td>
<td>IMS Relay mode</td>
<td>2</td>
<td>PF17</td>
<td>N</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>TSO</td>
<td>TSO Relay mode</td>
<td>3</td>
<td>PF12</td>
<td>J</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>OFFICE</td>
<td>OFFICE Relay mode</td>
<td>4</td>
<td>PF18</td>
<td>J</td>
<td>G</td>
<td>Y</td>
</tr>
<tr>
<td>VM1</td>
<td>VM Relay mode</td>
<td>6</td>
<td>PF18</td>
<td>J</td>
<td>G</td>
<td>Y</td>
</tr>
</tbody>
</table>

2. Now the parameters for each application in the group have been defined, the remaining work involves assigning applications in the groups to users. Use option 3, Assign a User to a Group, on the Administration Selection panel, as described in “Assigning a User to a Group” on page 69. The following shows an example of assigning SYSP1 group applications to users. The column names in the tables relate to the fields on the Assign a User to a Group panel.

<table>
<thead>
<tr>
<th>SYSP1</th>
<th>User</th>
<th>Default Group</th>
<th>Access Mode</th>
<th>Terminal Assume</th>
<th>Record Authorization</th>
<th>Shareable</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSO</td>
<td>JOHN</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>IMS</td>
<td>JOHN</td>
<td>Y</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>CICS</td>
<td>FRED</td>
<td>N</td>
<td>R</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>NetView</td>
<td>FRED</td>
<td>Y</td>
<td>B</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Table 10. Continuation of Fields on the Assign a User to a Group Panel

<table>
<thead>
<tr>
<th>SYSP1</th>
<th>User</th>
<th>Pseudo Terminal Name</th>
<th>Logon Variables</th>
<th>Admin Exit Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSO</td>
<td>JOHN</td>
<td>PSEUDO1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>IMS</td>
<td>JOHN</td>
<td>PSEUDO1</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>CICS</td>
<td>FRED</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>NetView</td>
<td>FRED</td>
<td>PSEUDO2</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

### Performing the Initial Administration

When you have planned your NetView Access Services installation, you can perform the initial administration.

A default user ID, PUBUSER, is provided with NetView Access Services. If you are a system administrator, you use this user ID for the initial administration. You log on as PUBUSER and can define other administrators, applications, users, and groups. If your installation uses an external security system for user authentication, the logon authorization installation-wide exit EMSELGNX must be customized. This exit must not supply a default group ID for PUBUSER. How to do this is described in *NetView Access Services Version 2 Customization*. Initial administration can also be performed using PUBUSER with user authentication disabled in EMSELGNX.

It is not necessary to make PUBUSER a group administrator, because PUBUSER can define other user IDs as administrators. PUBUSER cannot be deleted from NetView Access Services. However, it is recommended to revoke it from the external security management program, which means that it can no longer be used if user authentication is enabled. This ensures the security of the system. If, by accident, all the administrators are deleted from NetView Access Services, PUBUSER can be resumed in the external security management program and the administrators can then be reassigned. These steps are described in detail in *NetView Access Services Version 2 Customization*.

Another user ID provided with the system, EMSUSER, is defined as a user with no administrator authorization. This must also be defined to the external security management program. When the system is first installed, EMSUSER can be used to verify the installation. It can be deleted from the external management program, in which case it can no longer be used.

The system administrator sets up NetView Access Services during the installation in the following order:

1. Defines one or more system administrators
2. Defines the applications to the system
3. Defines the groups
4. Assigns applications to each group and defines group-wide characteristics for each application
5. Defines one or more administrators for each group.
One or more group administrators can then define and maintain more group-wide characteristics. Figure 8 shows how these tasks are carried out.

The administrators carry out their tasks by using panels that can be selected from the Administration Selection panel. The system and group administrator tasks are described in detail in Chapter 4, “System Administration Tasks” on page 31 and Chapter 5, “Group Administration Tasks” on page 63 respectively.

![Diagram of Administrator Tasks]

- **Define each application that needs to be accessed**: You specify the name of the applications and define data related to the applications.

- **Define each group**: You specify the name of a group and define data related to the group.

- **Assign applications to each group**: You specify applications for the group and define data related to each application.

- **Assign users to each group**: If you have not defined the group type as "Public", you specify users for a group. External-type groups might or might not need users.

*Figure 8. Administrator Tasks*
Invoking the Administration Functions

The following describes how to get to the Administration Selection panel and how to use commands on the administration panels.

**Note:** NetView Access Services in general does not accept graphical input on its administration panels (for example, A Programming Language (APL) characters).

Getting to the Administration Selection Panel

Log on to NetView Access Services and enter the ADM command on the Application Selection panel. The Administration Selection panel is displayed.

The Administration Selection panel displays the administration options. These options cover the administration tasks of NetView Access Services.

Figure 9 shows the complete Administration Selection panel in more detail. To select an option, enter the number of the option in the Command line.

Option 1 is an end-user function. You use this option to define the jump keys, logon profiles, and other parameters for the applications that you are assigned to use. This is described in *NetView Access Services Version 2 User's Guide*.

Options 2 and 3 are group administrator options. They are described in Chapter 5, “Group Administration Tasks” on page 63.

Options 4 through 11 are system administrator options. With the exception of Option 9, they are described in Chapter 4, “System Administration Tasks” on page 31.
Option 9 is described in Chapter 6, “Broadcast Administration Tasks” on page 77. The system administrator can select this option from the Administration Selection panel, or can enter the BMSG command on the Application Selection panel in the same way as any user authorized by the system administrator to be a broadcast-only administrator.

For group administrators, only the first three options are visible on the Administration Selection panel. For system administrators, all options are displayed. Users that are not administrators do not see this panel at all. They see the Maintain User Parameters panel when they use the ADM command. The system administrator can invoke the refresh function (option 11 on the Administration Selection panel), but this function is only available if the VSAM locking option has been enabled. For further information on the VSAM locking option, and the refresh function, refer to NetView Access Services Version 2 Customization.

**Using Commands on the Administration Panels**

You can use the following commands on the panels:

- **DISPLAY (or D)**
- **ADD (or A)**
- **DELETE**
- **UPDATE (or U)**
- **LIST (or L)**
- **HELP**
- **END**

The commands that can be used on each panel are displayed on the panel. You can enter the commands in lowercase or uppercase.

On most panels, there are key input fields. The field descriptions are highlighted on the panel and tell NetView Access Services which application, user, or group you want to administer. Filling in the key input fields of a panel, leaving the Command line blank, and pressing ENTER has the same effect as the DISPLAY command. For the LIST command, if there is more than one key input field, you must enter a question mark in the field for which you want a list.

When you enter the UPDATE, ADD, or DELETE command, NetView Access Services prompts you to press ENTER to confirm it. If you do not want to confirm it, press any other function key. You can enter the END command or the HELP command on the Command line of any of the administrator panels.

NetView Access Services provides a two-level help facility. First level help is provided when the Help PF key is pressed or the HELP command is entered. Second level help is provided by pressing the Help PF key again or by entering the HELP command twice. You can use the Help PF key when the cursor is positioned in any input field to get help for that field.

**User Administration Tasks**

The user-performed administration is described in the NetView Access Services Version 2 User’s Guide. The user carries out this administration using the Maintain User Parameters and the Redefine Keys panels.

Administrators can perform user-administration tasks only for their own user ID.
Chapter 4. System Administration Tasks

This chapter describes the system administrator tasks in detail. Figure 10 shows the Administration Selection panel as the system administrator sees it.

<table>
<thead>
<tr>
<th>Select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Maintain User Parameters</td>
</tr>
<tr>
<td>2 - Maintain Group Parameters</td>
</tr>
<tr>
<td>3 - Define a User to a Group</td>
</tr>
<tr>
<td>4 - Define an Application for the System</td>
</tr>
<tr>
<td>5 - Define a Group</td>
</tr>
<tr>
<td>6 - Assign an Application to a Group</td>
</tr>
<tr>
<td>7 - Define an Administrator</td>
</tr>
<tr>
<td>8 - Broadcast a Message</td>
</tr>
<tr>
<td>9 - Broadcast Selectively</td>
</tr>
<tr>
<td>10 - Define BIND User Data for Applications</td>
</tr>
<tr>
<td>11 - Refresh Profiles from VSAM Data Sets</td>
</tr>
</tbody>
</table>

Figure 10. Administration Selection Panel for the System Administrator

This chapter explains options 4 through 8, and options 10 and 11. You must be authorized as a system administrator to select these options.

Option 9, which you can select from the Administration Selection panel, or by entering the BMSG command on the Application Selection panel, is described in Chapter 6, “Broadcast Administration Tasks” on page 77.

**Note:** NetView Access Services does not support APL (A Programming Language) characters.

**Defining an Application for the System**

Before an application can be used by any user of NetView Access Services, it must be defined to the NetView Access Services system. To define an application to NetView Access Services, choose option 4, Define an Application for the System, on the Administration Selection panel. The panel shown in Figure 11 is displayed.
Figure 11. Define an Application for the System Panel

Explanation of the Fields

System-Internal Name
The NetView Access Services system-wide name of an application, which associates the application with its VTAM application name. It might be given different names in each group (see “Assigning an Application to a Group” on page 44), but this is the name by which NetView Access Services knows it. It can contain up to 8 alphanumeric characters.

Last Update
When the System-Internal Name field is filled in and the DISPLAY (D) command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you add or update an application, the field displays your user ID and the date and time of the update.

Primary LU Name
The network name as known to the VTAM that owns the application. This is the name (the VTAM application name) that SNA uses to find the application. NetView Access Services can be running on a different operating system than the application. The name can be up to 8 alphanumeric characters.

A primary LU name is not required for ASR-ASR communication.

ACB Type
Specifies the type of ACB that will be used as a pseudo terminal by the application. This can be unique (U), shared (S), or individual (I). What you can specify depends on the application. The default is S. “Pseudo Terminals” on page 11 provides information on pseudo terminals and ACBs.

If a Shared or Individual ACB is used, the VTAM APPL statement that defines the pseudo terminal name must specify parallel session support by means of the PARSESS=YES operand in the VTAM APPL statement. See NetView Access Services Version 2 Operation for information on this operand.
The ACB type is used only for relay mode applications. For pass mode applications it is ignored. No ACB is required for ASR-to-ASR communication. In that case, specify N in this field. The name of the ASR must be entered in the TPN of ASR field.

TPN of ASR
The transaction program name of the application service routine (ASR) for ASR-to-ASR communication. ASR-to-ASR communication implements a link between ASRs in the same address space of NetView Access Services through Communication Services without traversing VTAM. This field can be up to 8 characters and need only be filled in if an ASR is defined. In this case no ACB is required.

Pseudo Terminal Prefix
NetView Access Services uses the value entered here to identify pseudo terminals as NetView Access Services terminals. It can contain up to 8 alphanumeric characters. Each name must also be defined by the NetView Access Services installer in a VTAM APPL statement. If the value contains one or more asterisks, it is identified as a generic pseudo terminal name.

- Specifying the Pseudo Terminal Prefix
  For applications in relay mode with an ACB type of Shared, this prefix is used as the pseudo terminal name.
  For applications with an ACB type of Unique or Individual, the pseudo terminal prefix defines a pool of pseudo terminal names. The names are created by combining this prefix with digits to get 8-character names. The number of digits added depends on the number of characters in the prefix.
  For example, if the prefix is 5 characters long, the numbers are from 1 to 999. The actual upper limit is determined by the maximum sessions value. You can use the same pseudo terminal prefix for more than one application that has ACB type Unique or Individual. In this case the applications share the pool of pseudo terminal names. The number of names in the pool is determined by the number of maximum sessions of the application with the highest number of maximum sessions.
  The group administrators should also be aware of all possible pseudo terminal prefixes, as they should not define a pseudo terminal name that is the same as one from a pool. The order for selecting pseudo terminal names is as follows:
  1. Session establishment exit EMSESEEX
  2. The value given on the Define a User to a Group panel by the group administrator
  3. The value given here.
  This field is only used with relay mode applications. For pass mode applications it is ignored.

- Specifying a Generic Pseudo Terminal Name
  A generic name is identified by one or more asterisks in the Pseudo Terminal Prefix field. To form the pseudo terminal name for all ACB types, NetView Access Services combines the value entered with the name of the terminal requesting the session.
  The characters form the pseudo terminal name as follows:
– If the entered character is not an asterisk (*), it is taken to form the pseudo terminal name.
– If the entered character is an asterisk (*), the corresponding character of the terminal name is taken to form the pseudo terminal name.

For example:

Generic pseudo terminal name  P**A****
Terminal name                  I4ZA100
Resulting pseudo terminal name P4ZA100

Note: A blank in the Pseudo Terminal Prefix name is not accepted.

The system administrator must ensure that the pseudo terminal names that can be derived from the generic name are different.

If the group administrator assigns a name in the Pseudo Terminal Name field on the Assign a User to a Group panel, NetView Access Services ignores the name that is created from the generic name. For further information, refer to Pseudo Terminal Name on page 71.

For an application with a generic pseudo terminal name the ACB type has the following meanings:

– Unique
  Indicates that each generic pseudo terminal name can be used for only one session.

– Individual
  Indicates that each generic pseudo terminal name can be used for concurrent access to more than one different VTAM application.

– Shared
  Indicates that the ACB associated with each generic pseudo terminal name is defined to support parallel sessions.

A pool of pseudo terminal names is not generated for an application with a generic pseudo terminal name.

If you use generic pseudo terminal names, and a user disconnects and leaves applications (using generic terminal names) active, then another user logging on at the same terminal is affected as follows:

– Unique
  The user will not be able to log on because the ACB is occupied by the previous user’s active session.

– Shared
  The user will be able to log on because more than one user can log on to this application.

– Individual
  The user is able to log on to all applications except to those where a session with the previous user exists.

Access Mode
Specifies the mode of access authorized for the application at system-wide level. This can be R (relay), P (pass), or B (both). The default is R. If you specify B, you can specify the mode of access (R, P, or both) for the users of applications in a particular group, when assigning an application to that group. If you specify B at that level, the group administrator can decide for each user
of the application in the group whether they can use relay mode, pass mode, or both modes.

Access mode R is required if ACB type N is specified.

**Shareable**

Specifies whether this application can be shared. The default is N. If you specify Y, a group administrator can restrict individual users from sharing sessions with an application in a group. If you specify N, definitions at group levels are ignored.

**Automatic Logon**

Specifies whether logon to this application can be automated. The default is Y, which specifies that automatic logon is allowed, and a logon profile can be used to provide logon and logoff information. N specifies that the user must perform the logon and logoff manually. If you specify Y, a group administrator can restrict individual users from performing automatic logon to an application in a group. If you specify N, definitions at group level are ignored. See Chapter 8, “Creating and Controlling Logon and Logoff Profiles” on page 91 for further information on automatic logon.

It is recommended to specify N for automatic logon if a REXX exec is to be used for automatic logon to the specified application.

**Alternative Sequences**

Defines the maximum number of alternative sequences allowed for each logon profile for an application in relay mode. It can be any integer between 0 and 10. The default is 5.

**Idle-Time Value**

To help protect against unauthorized access to an application that is not in use, NetView Access Services can disconnect relay-mode sessions with applications that have not sent data to NetView Access Services after a predefined period has elapsed. You can specify any integer between 0 and 999 minutes.

For example, if you specify a value of 20, the session is disconnected after 20 minutes if no data is sent from the application to NetView Access Services during this time period.

The default is 60.

A value of 997 indicates that the session must be dropped when the terminal session is dropped. A value of zero means that NetView Access Services will not disconnect the session, and inactivity with this application is allowed indefinitely. This is not used for pass-mode applications.

The idle-time value specified has nothing to do with the idle-time value for the NetView Access Services terminal sessions, which is set in the startup parameters when NetView Access Services is installed.

Any updates you make do not affect applications that are already active. The change is effective when a session with each of the applications is reestablished.

**Maximum Sessions**

This is the maximum number of sessions that can be active concurrently for this application in relay mode. The default is 999.

You can specify any number between 0 and 65534, if ACB type Shared is used.
If ACB type Unique or Individual is used, the number of maximum sessions is limited by the possible size of the pool. For example, for the pseudo terminal prefix IMSAB the number of maximum sessions can be any number between 001 and 999. If the generic pseudo terminal name is not used, the number of maximum sessions is limited by the size of the pool. If more than one application shares the same pool, then the application with the highest number of maximum sessions determines the size of the pool. For example, if application A has maximum sessions 20 and application B has maximum sessions 10, the pool contains 20 names. If B uses 9 of the names, A will have only 11 names before the user is notified of maximum sessions (B will not get more than 10). If the number of maximum sessions is exceeded, an error message is displayed. You must then increase this value on at least one of the applications sharing this pool. (To get a maximum of 20 applications for A and 10 for B, a solution would be to define a dummy application using the same pool with a maximum sessions value of 30.)

If the value 0 is specified, no access to the application is possible. This field is used only with relay mode applications. For pass mode applications it is ignored.

**Status Update**

This value defines the time interval between inquiries to check whether an application is online or not. The status is shown on the Application Selection panel next to the application. If the application is online, the status time is shown highlighted. If the application is offline, the status time is shown normal.

An application is perceived to be online if its ACB is in a state to accept session requests and offline if its ACB is in any other state. The application status is related to the individual application and not to NetView Access Services.

You can specify a value in minutes between 0 and 1440. A value of 0 means that no status inquiries are required for this application. This is the default. A value of 1 through 1440 means that inquiries are made for the application. For example, specifying 1440 minutes means an inquiry for the application every 24 hours.

No time is displayed in the Status field on the Application Selection panel if NetView Access Services is newly installed, 0 is specified in the Status Update field, or the application is an ASR.

The status update function works as follows. Every minute, a scan routine is scheduled. This scan routine checks every application to see if an inquiry is to be issued for it. This is the case if the inquiry interval has expired, and the application is flagged as not accessible. To prevent the VTAM network from processing unnecessary inquiries, it is assumed that the normal status for an application is online. Inquiries are therefore only issued for applications that are perceived to be offline. In this way, all applications coming online are trapped and handled.

If more than one application shares the same VTAM ACB, and different times are specified for the status update interval for the applications, the scan routine uses the lowest interval to check if an inquiry is to be issued for the applications.

When a session is established with a backup application, it is important that the application being backed up is shown as online. Therefore, you must
specify the same status update time for any application defined as a backup application in a chain. Otherwise, the application may not be highlighted even though it is online.

In addition to the timer-initiated scan, a change in the status of an application can be detected in one of the following ways:

- If a user logs onto an application that is perceived to be offline, the application status is changed to online (highlighted).
- If the user fails to log onto an application that was perceived to be online, the application status is changed to offline (normal).
- If a user’s session with an application is dropped by the application itself, the application status is changed to offline (normal) when any user tries to log on to that application.

In all these instances, an inquiry is issued during the next application scan, regardless of the status-inquiry interval, to find out whether the application has changed its status or not. When the results of the inquiry are returned, the status is changed as necessary.

To establish an initial status for applications at NetView Access Services startup time, inquiries are made for all application for which the status update function has been requested. However, to prevent network flooding, a limit of fifty has been set. This is the maximum number of inquiries that can be active at any one time. Once this inquiry limit has been reached, no more inquiries are issued. Inquiries are only resumed when current inquiries are complete. This inquiry limit remains in force throughout all inquiry processing, and not only during initialization. It should be noted that there is an exception to this limit. If an application is suspected of going offline (in one of the ways previously mentioned), an inquiry is issued regardless of whether the inquiry limit has been reached or not.

**Backup Application Name**

Specifies the system-internal name of the application to be used as a backup application. It can be up to 8 alphanumeric characters including ampersand (&), number sign (#), and dollar ($). However, the first character must not be a digit.

A backup application name can be specified for pass or relay-mode applications.

This field is optional and can be left blank if no backup application is to be defined.

If you want the backup application to also have a backup, you can define it to the system with its backup application name. In this way you can provide a chain or ring of applications providing backup support for each other. For example, application A backed up by application B, application B backed up by application C, and application C backed up by application A. If users logging on to an application are to be unaware that a backup application is being used, identical applications must be used as backup applications.
Displaying Data for an Application
Fill in the system-internal name for the application, and enter the DISPLAY command. NetView Access Services fills in the current values for this application.

Adding a New Application
Fill in the system-internal name, the primary LU name, and the terminal prefix. The remaining fields have default values, which are supplied by NetView Access Services. If you want values different from the default values, fill in the fields as you require. Enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. The application is now defined for the system.

Deleting an Application
Fill in the system-internal name for the application. Leave the other fields blank. Enter the DELETE command. NetView Access Services prompts you to confirm the request. Press ENTER. The application is now deleted and no user can get access to it. All definitions for this application at group and user level are lost.

Note: You must ensure that the deleted application is no longer defined as a backup application for another application, because the Backup Application Name field is not automatically updated for those applications that used it as a backup.

Updating Data for an Application
Display the current data. Change the data as you require and enter the UPDATE (U) command. NetView Access Services prompts you to confirm the request. Press ENTER. The new values are now the current ones for the application.

Listing Applications
Enter the LIST (L) command. You do not have to fill in any fields. NetView Access Services lists all the applications on the system assigned to any group.

Defining a Group
For each group, you might want to define certain keys or certain characteristics that will be valid for every user of the group. To define group characteristics, select option 5, Define a Group, on the Administration Selection panel. The panel shown in Figure 12 on page 39 is displayed.
**Define a Group**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>The name of the group that you want to add to, or delete from, NetView Access Services, or whose characteristics you want to update. It can be up to 8 alphanumeric characters.</td>
</tr>
<tr>
<td>Last Update</td>
<td>When the Group field is filled in and the DISPLAY (D) command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you change the parameters for the group, the field displays your user ID and the date and time of the update.</td>
</tr>
<tr>
<td>Group Type</td>
<td>You can define three types of groups: Normal, Public, or External. See “Types of Groups” on page 6 for information on group types.</td>
</tr>
<tr>
<td>Account Number</td>
<td>A number that can be used by your installation to charge for all activities of a group. It can be up to 8 alphanumeric characters. The default is blank. It is an optional field.</td>
</tr>
<tr>
<td>Number of Sessions</td>
<td>(1-99) Concurrently used by user</td>
</tr>
<tr>
<td>Multiterminal Access</td>
<td>(Y=Yes/N=No/S=Secure)</td>
</tr>
<tr>
<td>Shared Session Response</td>
<td>(S=Systemwide/G=Groupwide/N=None)</td>
</tr>
<tr>
<td>Logon REXX Exec.</td>
<td>Logoff REXX Exec.</td>
</tr>
<tr>
<td>ASP Format</td>
<td>(N=Normal/C=Compact)</td>
</tr>
<tr>
<td>Printer</td>
<td>Printer LU name or SYSTEMPR</td>
</tr>
<tr>
<td>Print Key</td>
<td>Default for the group</td>
</tr>
<tr>
<td>Escape Key</td>
<td>Default for the group</td>
</tr>
<tr>
<td>Command Key</td>
<td>Default for the group</td>
</tr>
<tr>
<td>Command Prefix</td>
<td>Default for the group</td>
</tr>
<tr>
<td>CopyFrom Begin</td>
<td>Default for the group</td>
</tr>
<tr>
<td>CopyFrom End</td>
<td>Default for the group</td>
</tr>
<tr>
<td>CopyTo</td>
<td>Default for the group</td>
</tr>
</tbody>
</table>

**Figure 12. Define a Group Panel**

**Explanation of Fields**

**Group**

The name of the group that you want to add to, or delete from, NetView Access Services, or whose characteristics you want to update. It can be up to 8 alphanumeric characters.

**Last Update**

When the Group field is filled in and the DISPLAY (D) command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you change the parameters for the group, the field displays your user ID and the date and time of the update.

**Group Type**

You can define three types of groups: Normal, Public, or External. See “Types of Groups” on page 6 for information on group types.

If you specify the group as either external or normal, the Application Selection panel displays the applications that have been specified for each user assigned to use applications in the group by the group administrator.

If you specify the group as a public group, all applications that you assign to the group are displayed on the Application Selection panel for that public group.

**Account Number**

A number that can be used by your installation to charge for all activities of a group. It can be up to 8 alphanumeric characters. The default is blank. It is an optional field.

You can enter a default value to be used by the variable, &ACCNO, in this field. It can also be used by the installation-wide exit routine EMSENPMEM for

**ASP Format**
A parameter allowing the NetView Access Services administrator to specify which Application Selection panel format is to be used for the users in a particular group. The administrator can choose between the normal and the new compact format for all kinds of NetView Access Services group.

This is a one-character optional parameter. You can enter a value of 'N' for the normal format or 'C' for the new compact Application Selection panel. The default is 'N'.

**Number of Sessions**
The maximum number of relay application sessions that each user can use concurrently, that is, the number of applications the user can be connected to at one time. It is the same number for all users logging on in the group. It can be any number from 1 to 99, inclusive. The default is 10.

**Multiterminal Access**
Specifies whether each user of a group can log on to NetView Access Services at more than one terminal at a time, using this group name. This can be Y for Yes, N for No, or S for secure terminal. The default is N. If you specify S, then users of applications in the group can log on at another terminal, but the complete terminal session is taken over and the NetView Access Services Logon panel is displayed on the original terminal. This is to overcome any security exposure due to users leaving a location without disconnecting from NetView Access Services at that location.

However, it does not prevent simultaneous access from different terminals using different group names.

**Shared Session Response**
Specifies authorization to accept a request to share a session:

- **Systemwide (S)**
  The users assigned to use applications in the defined group are authorized to accept a request to share a session with all other users of the NetView Access Services system.

- **Groupwide (G)**
  The users assigned to use applications in the defined group are authorized to accept a request to share a session with all other users assigned to use applications in that group.

- **None (N)**
  The users assigned to use applications in the defined group are not authorized to accept a request to share a session. This is the default.

**Logon REXX Exec**
The name of the REXX exec to start during logon to the specified group. It can be up to 8 alphanumeric characters. The name must be the same as the name of the member in which the REXX instructions are located.

**Logoff REXX Exec**
The name of the REXX exec to start when a user enters the LOGOFF, EXIT, or DISC command within the specified group, and when the timeout value for the terminal session is reached. It can be up to 8 alphanumeric characters.
The name must be the same as the name of the member in which the REXX instructions are located.

**Printer**

Specifies the default printer name to which a user can send a copy of an application panel. One of the following can be specified:

- A VTAM line printer LU name. This can be a string of 1 to 8 characters.
- SYSTEMPR (system printer).

**Print Key**

This is a PF or PA key. The field can be left blank, if no Print key is to be defined. The default is PF24. Any user assigned to use applications in the group can use this key to print a panel of an application. The user can redefine the Print key on the Redefine Keys panel.

**Escape Key**

This is a PF or PA key, or the ATTN key. The field can be left blank, if no escape key is to be defined. The default is PA2. Any user assigned to use applications in the group can use this key to escape from a relay mode application to the Application Selection panel. The user can redefine the escape key on the Redefine Keys panel.

If the ATTN key is defined as the escape key, there are some important points that you must be aware of:

- The ATTN key can be pressed even if the keyboard is locked (X-CLOCK or X-SYSTEM symbol displayed). For example, if a transaction is started and the ATTN key is pressed to escape to the Application Selection panel before the transaction has completed, the transaction is not interrupted. An audible alarm is issued when the transaction has completed.

- In a VTAM network, the ATTN key generates a signal that is routed with a higher priority than any PA or PF key, the CLEAR key, or the ENTER key. This means that the signal from the ATTN key may be processed first in NetView Access Services, even if it is pressed after another key. For example, if the user is working with an application and presses a PF key to save some data and then presses the ATTN key to escape to the Application Selection panel, it can be that escaping takes place, however, saving the data must still be performed by returning to the application. Therefore the user must be careful not to press the ATTN key immediately after pressing a PF key in an application. This ensures that the transaction with the application is carried out.

- Whether you can define the ATTN key as the escape key depends on the availability of the attention signal to NetView Access Services. The attention signal does not function on non-SNA terminals.

**Command Key**

A PF key or the ENTER key assigned as the command key. The default is PF10. If you use the ENTER key, you must type **entr**, as this is a 4-character field. Using Enter is convenient, but might slow down the response time. The command key is used to issue a NetView Access Services command on a panel of an application. The command must also follow the NetView Access Services Command prefix. This field is only used for relay-mode applications. The user can redefine the command key on the Redefine Keys panel.
Command Prefix
The Prefix that the users of this group must enter preceding a NetView Access Services command on an application panel. It is up to 8 alphanumeric characters. The default is the local currency symbol, for example, $$$. This field is only used for relay-mode applications. The user can redefine the prefix on the Redefine Keys panel.

Screen Copy Keys
- CopyFrom Begin
  A PF key assigned to start the copyfrom area. The default is PF2. This field is only used for relay-mode applications.
- CopyFrom End
  A PF key assigned to end the copyfrom area. The default is PF2. This field is only used for relay-mode applications.
- CopyTo
  A PF key assigned to start the copyto area. The default is PF2. This field is only used for relay-mode applications.

Admin Exit Data
This is a 60-character field in which you can enter data. The data entered in this field is only valid for external groups. It is passed directly to the administration exit, EMSEADEX. Refer to NetView Access Services Version 2 Customization.

Displaying the Characteristics of a Group
Fill in the Group field and enter the DISPLAY command. NetView Access Services displays the current values for that group.

Adding a New Group
Fill in the Group field. The remaining fields have default values. If you want different values from the default values, fill in the fields as you require. Enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. The group now exists and is ready for you to assign some applications to it.

Updating the Characteristics of a Group
Display the current values for the group. Change the data as you require and enter the UPDATE (U) command. NetView Access Services prompts you to confirm the request. Press ENTER. The new characteristics are now the current ones for the group.

Note: Any changes you make, do not affect users that the group administrator has already assigned to use applications in the group.

Listing the Groups That Are Defined to NetView Access Services
Enter the LIST (L) command. You do not need to fill in any fields. NetView Access Services lists the groups that are defined to the system.
Deleting a Group

Fill in the Group field. Leave the other fields blank. Enter the DELETE command. You are prompted to confirm the request. Press ENTER. For normal groups, NetView Access Services deletes the group and the users in the group. For external groups, the group is deleted only when the last user, including the group administrator, is deleted. If an application was assigned to this group only, it must be assigned to another group before it can be used again. This also deletes all logon profiles for all users assigned to use applications in the group.

Criteria for Defining Groups

To use applications, the applications defined to the system must be accessible by a group. In the simplest form, all applications defined to NetView Access Services can be associated with a single group. All users can be assigned to that single group, but each user’s application access can be restricted to only a subset of the group’s applications.

Part of the planning task is to establish criteria for grouping users. Proper grouping of users facilitates more efficient administration. Some of the criteria that might be used as a basis for grouping users are:

- Application access requirements
  These are based on the type of work each user performs, which in turn dictates the user’s application access requirements.

- Organization
  You could define and administer each department within the organization as a group.

- Accounting
  You can optionally assign a different account number to each group. Users that must perform work and gain access to applications based on an account code could be grouped together.

- Geography
  Users that reside at different locations within the organization might logically be associated with different groups.

- Type of application access
  Users can be grouped based on the need to maintain several concurrent sessions. Users that need only a single session at one time might be associated with one or more groups, while users that require several concurrent sessions, using relay mode, might be users assigned to use applications in another group or groups.

- Type of group
  NetView Access Services enables you to specify three types of groups. You can select the type to suit your installation requirements. For external groups, the administration exit EMSEADEX must be customized to interface with the external database. Refer to NetView Access Services Version 2 Customization.
Assigning an Application to a Group

When you have named a group and set up some keys for it, you then need to assign some applications to that group. To do so, choose option 6, Assign an Application to a Group, on the Administration Selection panel. The panel shown in Figure 13 is displayed.

![Figure 13. Assign an Application to a Group Panel](image)

Explanations of the Fields

**Group**

The name of the group to which you are assigning the application. It can contain up to 8 alphanumeric characters.

**Application**

The group-wide name of the application. It can contain up to 8 alphanumeric characters and can be any name. The name appears on the Application Selection panel. The name does not have to be the same as the system-internal name used when defining an application for the system. You can assign the same system-internal name several times to the same group using different group-wide application names. This enables the users assigned to use applications in the group to have several concurrent sessions with the same application when operating in relay mode.

You can specify that a free selection field is to be displayed on the Application Selection panel for the group. To do this, enter eight periods in this field and use the ADD (A) command. The eight periods appear on the Application Selection panel as the F field. The group administrator can specify this for individual users assigned to use applications in the group.

**Note:** Do not use a name for an application that can be interpreted as a NetView Access Services command. For example, A, because this is an abbreviation for the NetView Access Services ADD command.
**Last Update**

When the Group and Application fields are filled in and the DISPLAY (D) command is used, the Latest Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you change the parameters of an application, the field displays your user ID and the date and time of the update.

**System-Internal Name**

The system-wide name for the application. It can contain up to 8 alphanumeric characters. It must be the name that appears on the Define an Application for the System panel for this application. Leave this field blank for the F field to appear on the Application Selection panel.

**Access Mode**

This determines whether the users assigned to use applications in the group can use the application in relay mode, pass mode, or both. It can be R (relay), P (pass), or B (both). The default is R. What you can specify here depends on the access mode you specified when defining the system-wide application. If you specified B, and you specify here that the application can be used in both modes, the group administrator can specify in which mode, or modes, each user can gain access to the application.

**Shareable**

Specifies whether this application can be shared between two users:

- **Y** Specifies that users assigned to use applications in the group are authorized to share a session with this application with another user.

- **N** Specifies that this application cannot be shared by users assigned to use applications in the group. N is the default.

If you specify Y, a group administrator can restrict individual users assigned to use applications in the group from sharing sessions with an application. If you specify N, definitions at group level are ignored.

**Data Compression**

This specifies whether NetView Access Services is to compress data before it is sent. An advantage of data compression is to reduce transmission charges for a communication network.

You can specify Y for Yes (outbound-only compression), N for No, or F for Full (inbound and outbound compression). Full compression is possible only when Virtual Terminal option Y is specified for the application.

If you specify Y for Data Compression, NetView Access Services compresses the application data before it is sent to the users’s terminals. Y for Virtual Terminal can be specified, but is not required for this option. If you specify F for Data Compression, NetView Access Services compresses the data received from the application before it is sent to the users's terminal. In addition, NetView Access Services removes all MDT-bits (Modified Data Tag) from the field definitions sent to the real terminal. This reduces the inbound data because only the data entered is sent to NetView Access Services. NetView Access Services then adds the data from all other fields and sends it to the application.

If Virtual Terminal option Y is specified, the efficiency of data compression is considerably improved because a more efficient data compression algorithm is used. NetView Access Services compares the data received with the content of the virtual terminal buffer. Only the data that has changed is sent.
Note: Do not specify full compression if DBCS (Double Byte Character Set) is to be used. Unpredictable results can be expected.

Virtual Terminal
Specifies that the Virtual Terminal function for the specified application is enabled. This is a prerequisite for the NetView Access Services REXX Application Programming Interface (API), and if Data Compression option F (inbound and outbound compression) is specified. The default is Y. Virtual Terminal option Y should be specified for an application if a REXX exec is specified for logon or logoff from the application. However, it is not a prerequisite, because a REXX exec can obtain data from a NetView Access Services panel, which always has Virtual Terminal Y, or be used for accounting purposes. Any update you make is only effective after a relogan to NetView Access Services.

Logon REXX Exec
Specifies the name of the REXX Exec to start during logon. It can be up to 8 characters. The name must be the same as the name of the member in which the REXX instructions are located. The use of a REXX exec for logon to an application is only valid for applications used in relay mode. A REXX exec cannot be used for a free-selection application. Therefore a name specified in the Logon REXX Exec field is ignored. Any update you make takes effect immediately.

Logoff REXX Exec
Specifies the name of the REXX Exec to start during logoff from the application, or when the timeout for the application session is reached. It can be up to 8 characters. The name must be the same as the name of the member in which the REXX instructions are located. The use of a REXX exec for logoff from an application is only valid for applications used in relay mode. A REXX exec cannot be used for a free-selection application. Therefore a name specified in the Logoff REXX Exec field is ignored. Any update you make takes effect immediately. When the user issues a LOGOFF, DISC, or EXIT command on the Application Selection panel, or from a panel of an application together with the command prefix and the Command key, the REXX exec starts. The NetView Access Services function is not carried out, and the REXX exec must terminate the terminal session, application session, or both. However, if the started REXX exec itself issues one of these commands, or the user issues the command again, then the issued command is carried out.

LogMode
Specifies a VTAM logon mode (LOGMODE) to be used when opening a session with an application, instead of the LOGMODE chosen by NetView Access Services automatically. Previously, the only way to override the LOGMODE chosen by NetView Access Services was via the NetView Access Services Session Establishment Exit (EMSESEEX). The LogMode defined in this field will be used by NetView Access Services to open all the server sessions with this application both in pass-mode and in relay-mode, when the user requesting the session is logged on this group.

The logmode to be used is chosen according to the following priority:

1. Session Establishment Exit (EMSESEEX)
2. New LogMode field
The field is eight characters long and can contain any string that is a valid VTAM logmode.

Displaying the Attributes of a Group Application
Fill in the Group and Application fields. Enter the DISPLAY (D) command. NetView Access Services displays the current data.

Adding an Application for a Group
Fill in all the fields and enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. This application is now defined for this group.

Deleting an Application from a Group
Fill in the Group and the Application fields. Enter the DELETE command. NetView Access Services prompts you to confirm the request. Press ENTER. The application no longer belongs to that group. Neither the group administrator nor the users can gain access to it, or gain any information about it on their administration panels.

Updating an Application for a Group
You can change the access mode of an application for all the users assigned to use applications in the group, or you can make the group-wide application name point to a different application. Display the current data. Change the fields as you require. Enter the UPDATE (U) command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services updates the information.

Listing Applications
**Applications that a Group has Access to:** Fill in the Group field and put a question mark in the Application field. Enter the LIST (L) command. NetView Access Services lists the applications of the group by their group-wide names.

**Applications in the System:** Type a question mark in the Application field and leave the Group field blank. Enter the LIST (L) command. NetView Access Services lists the applications on the system by their system-internal names.

Listing Groups
**Groups in the System:** Type a question mark in the Group field, and leave the Application field blank. Enter the LIST (L) command. NetView Access Services lists the groups in the system.

**Groups with Access to an Application:** Type a question mark in the Group field and fill in the Application field. Enter the LIST (L) command. NetView Access Services lists the groups that have access to this application. This is the group-wide application name. If another group uses the application, but gives it a different name, it is not listed here, even though the system-internal name is the same.
Providing a Free Selection Field

To provide a free selection field for users assigned to use applications in a group, enter eight periods in the Application field and fill in the Access Mode field. See “Assigning the Free Selection Field” on page 75 for further details on this field.

Criteria for Assigning Applications to Groups

When deciding how to assign applications to groups, you should consider the following:

- The applications of one group have the same:
  - Copy keys
  - Account number
  - Number of allowed concurrent sessions per user
  - Multiterminal authorization
  - Shared session authorization.

- The users of a group:
  - Should (optimally) use all of the group applications
  - Must be able to contact their group administrator easily.

This means that the applications of one group should have similar program function (PF) keys. Also, the users in a group should have similar tasks to perform, be assigned to the same group administrator, and have the same level of authorization.

Defining an Administrator

NetView Access Services needs at least one system administrator. PUBUSER is provided by IBM to carry out the initial administration during installation. You can have one or more group administrators for each group. You can also have more than one system administrator. Additionally, you can define a user to be a broadcast administrator allowing that user to broadcast selective broadcast messages. To define and authorize users as administrators, choose option 7, Define an Administrator on the Administration Selection panel. The panel shown in Figure 14 is displayed.
Define an Administrator

User . . . . . . . . . . . . . . . . . . . . . (If group administrator)
Group . . . . . . . . . . . . . . . . . . . . .
Last Update:

Fill in the following:

Type . . . . . . . . . . . (S=System/G=Group/B=Broadcast)

Admin Exit Data . __________________________________________________________

Enter a command: d (display), a (add), u (update), l (list), or delete

COMMAND ==> ________
PF 1=Help  3=End

Figure 14. Define an Administrator Panel

Explanation of Fields

**User**

The user ID of the user you are defining as an administrator. It can contain up to 8 alphanumeric characters.

**Group**

The name of the group when you define a group administrator. It can contain up to 8 alphanumeric characters.

**Last Update**

When both the User and Group fields are filled in and the DISPLAY (D) command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update.

**Type**

The type of administrator you are defining. This is mandatory when defining an administrator.

- **S** System administrator. This includes all administration tasks.
- **G** Group administrator. This includes all group administration tasks for the group specified. If you want to authorize a group administrator to broadcast selective broadcast messages system wide, you must, in a second step, add this user as a broadcast-only administrator by leaving the Group field blank and specifying type B.
- **B** Broadcast-only administrator. The user whose ID is specified is authorized to broadcast selective messages system wide.

**Admin Exit Data**

This is a 60-character field in which you can enter data. The data entered in this field is only valid for external groups. It is passed directly to the adminis-
Displaying Whether a User Is an Administrator

**System or Broadcast-Only Administrator:** Fill in the User field and leave the Group field blank. Enter the DISPLAY (D) command. NetView Access Services responds by displaying S (system) or B (broadcast) in the Type field, the date and time when this user became a system or broadcast-only administrator, and the user ID of the administrator who performed the update.

**Group Administrator:** Fill in the User field and Group field, type G in the Type field and enter the DISPLAY (D) command. NetView Access Services responds by displaying the date and time when this user became an administrator for this group, and the user ID of the administrator who performed the update.

Defining Administrators

**A New System Administrator:** Fill in the User field with the user ID of the user that you want to authorize as a system administrator, and enter S in the Type field. Leave the Group field blank. Enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services adds this user to the system administrators.

**A New Group Administrator:** Fill in the User field with the user ID of the user you want to authorize as a group administrator, fill in the Group field and enter G in the Type field. Enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services adds this user to the administrators for this group.

**A New Broadcast-Only Administrator:** Fill in the User field with the user ID of the user you want to authorize as a broadcast-only administrator, and enter B in the Type field. Leave the Group field blank. Enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services adds this user to the broadcast-only administrators.

Updating the Characteristics of an Administrator

You can only update the Admin Exit Data for an administrator. You cannot change the type of administrator. This can only be done by a DELETE followed by an ADD administrator command.

**System or Broadcast-Only Administrator:** Fill in the User field. Leave the Group field blank. Enter the DISPLAY (D) command. Change the Admin Exit Data as required and enter the UPDATE (U) command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services updates the characteristics for that system or broadcast-only administrator.

**Group Administrator:** Fill in the User and the Group field. Enter the DISPLAY (D) command. Change the Admin Exit Data as required and enter the UPDATE (U) command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services updates the characteristics for that group administrator.
Deleting Administrators

**System or Broadcast-Only Administrators:** Fill in the User field. Leave the Group field blank. Enter the DELETE command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services deletes this user from the list of system or broadcast-only administrators.

**Group Administrators:** Fill in the User and the Group field. The group is the one for which you no longer want this user to be an administrator. Enter the DELETE command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services deletes this user from the list of administrators for this group.

Listing Administrators

**System Administrators:** Type a question mark in the User field and leave the Group field blank. Enter the LIST (L) command. NetView Access Services lists all the system administrators.

**Broadcast-Only Administrators:** Type a question mark in the User field, leave the Group field blank, and type B in the Type field. Enter the LIST (L) command. NetView Access Services lists all broadcast-only administrators.

**Administrators of a Group:** Type a question mark in the User field and fill in the Group field. Enter the LIST (L) command. NetView Access Services lists the administrators of this group.

**All Group Administrators:** Type a question mark in the User field, leave the Group field blank, and type G in the Type field. Enter the LIST (L) command. NetView Access Services lists all group administrators defined to the system.

Listing Groups

**Groups in the System:** Leave the User field blank and put a question mark in the Group field. Enter the LIST (L) command. NetView Access Services lists the groups in the system.

**Groups for a Specific Administrator:** Fill in the User field, and put a question mark in the Group field. Enter the LIST (L) command. NetView Access Services lists the groups that this user is authorized to administer.

Sending a General Broadcast Message

Occasionally you might want to inform every user, or those users using a particular language, of an event or a situation. You can do this by using NetView Access Services’s General Broadcast function. A general broadcast message has a maximum length of 75 characters. The message is displayed on the Application Selection panel in the message area at the top of the panel. To enter a general broadcast message, choose option 8, Broadcast a Message, on the Administration Selection panel. The panel shown in Figure 15 is displayed.

You can enter a broadcast message for each language on the Broadcast a Message panel. This message is then displayed on terminals of users who have selected that language (using the Language Selection panel or a user exit).
Note: General broadcast messages are only active until NetView Access Services is terminated.

<table>
<thead>
<tr>
<th>Language</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>1</td>
</tr>
<tr>
<td>German</td>
<td>2</td>
</tr>
<tr>
<td>Japanese</td>
<td>3</td>
</tr>
<tr>
<td>Uppercase</td>
<td>4</td>
</tr>
<tr>
<td>French</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7</td>
</tr>
</tbody>
</table>

Select language _ (* for all languages)

Type in, change, or delete message:

__________________________________________________________________________

Enter a command: d (display), a (add), u (update), or delete.

COMMAND ==> ________
PF 1=Help  3=End

Figure 15. An Example of the Broadcast a Message Panel

Explanation of Fields

Language Fields
The eight fields on the panel contain the names of the languages. An asterisk (*) is displayed to the left of the field when an active broadcast message exists for the language.

Select Language
You can enter the number of the language for which you want to process a message. You can enter an asterisk to add, update, or delete a broadcast message for all languages.

Entering a General Broadcast Message
To send a general broadcast message, fill in the Select Language and message text fields, and use the ADD (A) command. The message can be up to 75 characters long. For example, if you want to tell all users that the system will be unattended over the Easter weekend, you fill in the panel as shown in Figure 16. Enter an asterisk in the Select language field, if you want to add the message to all languages for which a broadcast message has not already been defined.
Displaying a General Broadcast Message

To display a general broadcast message, select the language and use the DISPLAY (D) command. Pressing the ENTER key with nothing entered in the command line has the same effect as using the DISPLAY (D) command.
Updating a General Broadcast Message
To update an existing general broadcast message, select the language, change the message text as required, and use the UPDATE (U) command. Enter an asterisk in the Select language field, if you want to update all defined messages.

Deleting a General Broadcast Message
To delete the message, select the language and use the DELETE command. Enter an asterisk in the Select language field, if you want to delete all defined messages.

When the users refresh their screens, the broadcast message no longer appears on the Application Selection panel.

Sending Selective Broadcast Messages
When you want to selectively broadcast messages, you can use the selective broadcast function instead of the general broadcast function. The advantage of this function is that you can send one or several broadcast messages of arbitrary length to an individual user, all users, or to a group of users.

To process a selective broadcast message, choose option 9, Broadcast Selectively, on the Administration Selection panel. You can also enter the BMSG command in the command line on the Application Selection panel. In both cases, the Broadcast Selectively panel is displayed.

If you have authorized a user to be Broadcast Administrator as described in “Defining an Administrator” on page 48, the Broadcast Selectively panel is displayed when the user enters the BMSG command on the Application Selection panel. A broadcast administrator does not see the Administration Selection panel. For information on sending selective broadcast messages, refer to Chapter 6, “Broadcast Administration Tasks” on page 77.

Defining BIND User Data for Applications
When an application is selected from the Application Selection panel, NetView Access Services can send BIND user data to the application with the request for the session. The application interprets this data as part of the session request. For example, TSO can accept a user ID. For a detailed description of BIND user data, see “Defining BIND User Data” on page 97.

To define this data, select option 10, Define BIND User Data for Applications, on the Administration Selection panel. The panel shown in Figure 18 is displayed. This panel sets up data for the NetView Access Services system, regardless of the group. Therefore it uses the system-wide name for a system or application, rather than the group-wide name for an application.
**Explanation of Fields**

**System-Internal Name**
This field contains up to 8 alphanumeric characters. This is the system-wide name for the system or application. It must be the same as the one on the Define an Application for the System panel.

**Last Update**
When the System-Internal Name field is filled in and the DISPLAY (D) command is used, the Last Update field displays the user ID of the system administrator who last updated the data, and the date and time of the update. When you add or update the data, the field displays your user ID and the date and time of the update.

**Passed Data**
There are four lines of unlabeled area for you to enter data. This data is defined for every user that uses this application, regardless of the group. You can use variables in this area. For example, &UID enables NetView Access Services to get the user ID from the user’s Maintain User Parameters panel for this application. See “Using Variables in NetView Access Services” on page 83 for information on setting values for these variables.

**Displaying BIND Data**
Fill in the system-internal name and enter the DISPLAY (D) command. NetView Access Services displays the current BIND user data for this application.

If you have no data defined, you get a message to this effect.

When you add, delete, or update BIND data, you must notify the users because this could affect their logon processes.
Adding BIND Data
Fill in the system-internal name for this application and the BIND user data. Enter the ADD (A) command. NetView Access Services prompts you to confirm the request. Press ENTER. The new BIND user data is now active for this application.

Deleting BIND Data
Display the current data, to make sure that you want to delete it. Enter the DELETE command. NetView Access Services prompts you to confirm the request. Press ENTER. There is now no BIND user data defined for this application.

Updating BIND Data
Display the current data. Change this data as you require. Enter the UPDATE (U) command. NetView Access Services prompts you to confirm the request. Press ENTER. The updated data is now defined for this application.

Listing the Applications for Which BIND User Data Has Been Defined
Enter the LIST (L) command. NetView Access Services responds with a list of the applications, by their system-internal names, that have BIND user data defined for them.

Refreshing Profiles from VSAM Data Sets
The refresh option allows you to refresh the profiles with the latest updates from VSAM. This may be necessary if the VSAM data sets are shared by more than one NetView Access Services (including the Batch Load Facility). The profiles EMSSRTS, EMSSRTG, EMSSRPF, EMSPLDT, and EMSSBROD are refreshed. This includes adding new profiles, modifying existing profiles, and deleting profiles that have been removed from the VSAM data sets.

To refresh these profiles, select option 11, Refresh Profiles from VSAM Data Sets on the Administration Selection panel. When the refresh is completed, you are notified by a message. The refresh function can also be invoked using an operator command.

Notes:
1. When you share your data sets with several NetView Access Services, the VSAM locking function should be enabled to prevent other administrators updating data sets at the same time. Refer to NetView Access Services Version 2 Customization for further information on the VSAM locking and refresh functions.
2. When the refresh function is used, the status of all applications on the Application Selection panel is set to offline until the next inquiry.

Providing a Bulletin Board
The Bulletin Board function allows you to provide any information that users can view online. For example, you can provide information such as company announcements, private sales, and club offers.
Bulletin Board Information

The Bulletin Board information is contained in partitioned data sets and members stored on a disk. These are defined by the DD name EMSBULL in the NetView Access Services startup job. All the functions of editors such as ISPF and XEDIT can be used to produce and update the information.

The partitioned data sets can contain two types of information:

- An index data member containing items of information that can be selected. Each item in the index member refers to another data member in which the information is located. This data member can also contain a sub-index. The number of nested indexes is unlimited.

- The information contained in an index item.

The index data members are formatted as follows:

- An index data member must have the &INDEX; keyword in line 1, starting at position 1, so that NetView Access Services can identify the member as an index data member. This line is not presented to the user and can contain additional information to identify the data member.

- The data member of the top-level index must be EMSBULL1.

- The lines that follow can contain the title of the Bulletin Board item to be selected for more information. Each line must contain a data member name that contains the associated information or another index of items.

- The information in a data member can consist of uppercase and lowercase characters.

Figure 19 shows an example of a top-level index member with the name EMSBULL1:

```
&INDEX; This is the primary INDEX member
Company Announcements member01
For Sale member02
Shares News member03
Cafeteria News member04
Sailing Club News member05
```

Figure 19. Example of a Top-Level Index Member, EMSBULL1

Columns 1 to 60 contain the title, and columns 61 to 72 contain the data member name starting at any position in that area.

The text can be highlighted when the data member name is preceded by the character ampersand (&) starting after column 60. One or more blanks are allowed between & and the data member name.

The information type data members are unformatted. Only the text within the columns 1 through 72 are presented to the user.

Figure 20 on page 58 shows an example of information contained in a data member selected from an index data member.
Important:

The cafeteria will be closed next Friday, July 8th
Full service will be available on Monday, July 11th
and so on...

Figure 20. Example of Information in a Data Member

Examples of Bulletin Board Information

When users request the Bulletin Board only the titles of the items are displayed, as shown in Figure 21.

<table>
<thead>
<tr>
<th>Company Announcements</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Sale</td>
</tr>
<tr>
<td>Shares News</td>
</tr>
<tr>
<td>Cafeteria News</td>
</tr>
<tr>
<td>Sailing Club News</td>
</tr>
</tbody>
</table>

Figure 21. The Bulletin Board Panel Showing Items in an Index

When the user selects an item from the list of items on the Bulletin Board, the Bulletin Board panel is shown as in Figure 22.
Gaining Access to a Single Application Several Times

NetView Access Services does not permit a single user to establish several concurrent sessions with the same application in relay mode. For example, if CICS is defined to NetView Access Services using the name CICS, a user cannot have two concurrent relay mode sessions with that application using the same name (without using the free selection field). However, the system administrator can assign the same application to a group several times, using a different group-wide application name each time.

Using this technique, access can be gained to the same application several times. For example, the system administrator can assign the same CICS application to a group using the application names CICS1 and CICS2. In this case, the system administrator uses the system-internal name of CICS each time and changes the Application name specification of CICS1 and CICS2. The name CICS is a NetView Access Services system-internal name and is not necessarily the same as the VTAM network application name. These values are specified when the system administrator defines the application. The two different application names can then be assigned to any user in that group. A user can therefore establish two concurrent sessions with the same CICS application. In this case, both of the NetView Access Services application names direct the sessions to the same application.

Gaining Concurrent Access to Applications in Different Groups

A NetView Access Services user can belong to several groups. To enable the user to gain access to applications in a different group you can define NetView Access Services as another application. The application (NetView Access Services) can be associated with users in a group or groups. Users can initiate a second session with NetView Access Services using a different group identifier. They can then
gain access to a different set of applications associated with a different group, assuming they are assigned to use applications in that group. However, users are not allowed to establish a pass-mode session from a second-level NetView Access Services.

When using this technique, the installer must ensure that the pseudo terminal prefix is defined as the INPLU parameter in the SERVRTN statement in the INPARM data set. Otherwise gaining access to NetView Access Services the second time fails.

When gaining concurrent access to NetView Access Services, a different group ID must be used. Direct or indirect recursive logons under the same group ID are not allowed. The second logon to NetView Access Services can also be automated since it accepts logon user ID, password, and group name as BIND user data. You can define BIND user data as follows:

- Specify the variables &UID and &PWD for the user ID and password. These take the default value for the user.
- Specify one of the variables &UVAR1 to &UVAR4 or &GVAR1 to &GVAR5 for the group name.

To initiate a second-level access to NetView Access Services, a user enters the application ID or name on the first access level Application Selection panel. Some of the user operational characteristics that must be considered when gaining access to NetView Access Services a second time are as follows:

- Escape key and Jump key definition and usage:
  If the same PF, or PA key, or the ATTN key is designated as an escape key or a jump key on both the first and second accesses of NetView Access Services, that PF, or PA key, or the ATTN key always performs the function for the first access level. The second access level of NetView Access Services loses the function of those keys. For example, if PA1 is defined as the escape key on both first and second-level accesses, then it always returns the user to the first access level Application Selection panel. The user can redefine the escape key and jump key using the User Administration functions.

- Jumping between first and second access levels:
  From an application accessed from the second-level access of NetView Access Services, the user can either:
  - Jump to another second-level application using the jump key, provided that key is not defined in the first access level, or
  - Escape to the second access level Application Selection panel using the second access level escape key, again provided that key is not defined in the first access level.

From an application accessed from the second-level or from the second application selection menu, the user can also:

- Jump to a first-level application using the jump key, or
- Escape to the first-level application screen using the first access level escape key.

From a first-level application, a user can return to the second access level of NetView Access Services using the jump key. The user is returned to the second-level panel that was displayed when exiting the second access level of NetView Access Services. That screen can be either the second access level
Application Selection panel or an application screen accessed from the second level.

There is no mechanism for jumping directly from a first-level application screen to a second-level application screen unless the second-level application was the last screen accessed prior to leaving that level.

- **LOGOFF and DISC commands**

  The LOGOFF and DISC commands, when entered from the second-level Application Selection panel, return the user to the second-level NetView Access Services Logon panel. From the second-level Logon panel, a user must enter the LOGOFF command in the User field to return to the first-level Application Selection panel. An alternative to terminating a second-level session is to issue an LF command from the first-level Application Selection panel. The LF command, when issued for a second-level NetView Access Services session, only terminates all active second-level applications. You can modify the logoff user exit routine EMSELGFX so that the Logon panel is skipped when the user returns from a second-level NetView Access Services group to the first level.

  The DISC command, when entered from the first-level Application Selection panel, disconnects the user terminal from NetView Access Services, while keeping all first and second-level application sessions active. The LOGOFF command, when entered from the first-level Application Selection panel, terminates all first and second-level application sessions.

Consider the following before setting up pass-mode recursive calls:

- **NetView Access Services** uses various VTAM routines to accomplish the pass mode recursive call. The user’s terminal displays messages that the user might not recognize before displaying the NetView Access Services Logon panel or the Application Selection panel.

- **You need to ask the installer if there is an application set up as a VTAM LOGAPPL for the terminals that require access to the pass-mode recursive call function.** If a LOGAPPL application exists for a terminal, that application receives control before the NetView Access Services logon is complete.
Chapter 5. Group Administration Tasks

This chapter describes the group administrator tasks which are:

- Maintaining group-wide parameters for each application in the group.
- Assigning users to a group, the applications each user can use, and user-specific parameters for each application. This is necessary for Normal groups, optional for External groups, and not required for Public groups.

You start with the Administration Selection panel, shown in Figure 23. Options 2 and 3 are group administrator options. Option 1 can be used to define parameters for the applications you use. How to do this is described in the *NetView Access Services Version 2 User’s Guide*.

The Administration Selection panel is displayed regardless of which normal or external group you are logged on to. This means that you can administer parameters for the groups for which you are an administrator, even when you are logged on to a group for which you are not an administrator.

```
EMSPA3 Administration Selection
Terminal: I123456B

Select one of the following:

1 - Maintain User Parameters
2 - Maintain Group Parameters
3 - Assign a User to a Group

COMMAND ==> ________
PF 1=Help 3=End
```

*Figure 23. Administration Selection Panel for the Group Administrator*
Maintaining Group Parameters

When you select option 2, Maintain Group Parameters, on the Administration Selection panel, the panel shown in Figure 24 is displayed. On this panel you can display and update the parameters of an application that the group has access to. You can also list applications and groups.

<table>
<thead>
<tr>
<th>EMSPG1 Maintain Group Parameters</th>
<th>Terminal: I123456B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ___________________________</td>
<td></td>
</tr>
<tr>
<td>Application _____________________</td>
<td></td>
</tr>
<tr>
<td>Last Update: ____________________</td>
<td></td>
</tr>
</tbody>
</table>

Fill in or change the following:

- Application Description ______________________________
- Default Selection ID . . On the selection panel
- Jump Key . . . . . . Default for the group
- Msg. Received Indicator (N=Normal/J=Jump/I =Information)
- Logon Profile Type . . (G=Group/S=System)
- Automatic Logon . . (Y=Yes/N=No)
- Application ID Display . . (Y=Yes/N=No)
- Row/Column . . . . . . (Row=-43...43/Column=-132...132)
- Text . . . . . . . . ______________________________

Enter a command: d (display), u (update), or l (list).

COMMAND ==> __________
PF 1=Help 3=End

Figure 24. Maintain Group Parameters Panel

Explanation of Fields

**Group**
The group name given to the group by the system administrator. It can contain up to 8 alphanumeric characters. NetView Access Services uses this name to identify the group. The users assigned to use applications in this group see the group name in the general information area of the Maintain User Parameters panel.

**Application**
The group-wide name of an application, as defined by the system administrator (described in “Assigning an Application to a Group” on page 44). It can contain up to 8 alphanumeric characters. This name appears on the Application Selection panel.

**Last Update**
When the Group and Application fields are filled in and the DISPLAY command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you update the group parameters, the field displays your user ID and the date and time of the update.
Application Description

This description appears on the Application Selection panel, next to the application name. It can contain up to 30 characters of text describing the application. It is a good idea to state in this text whether the application is set up for relay mode, pass mode, or both, so that users are aware of the access mode.

Default Selection ID

This controls the sequence of the applications on the Application Selection panel. You can enter a value between 1 and 99 here to denote the default position of the application on the Application Selection panel for all use assigned to use applications in the group. A blank puts the application at the bottom of the list.

The users assigned to use applications in Normal and External groups can define their own Selection IDs on the Maintain User Parameters panel to override the definition in this field. For Public groups the definition set here applies to all users logging on to the group.

Jump Key

This is a PF or PA key written in the format PFnn or PAnn, or the ATTN key written in the format ATTN. Leave the field blank if you do not want to define a jump key. The jump key is used by users assigned to use applications in the group to jump to this application from others.

The users in Normal and External groups can define their own jump keys, on the Maintain User Parameters panel, to override the definition in this field. For Public groups this definition applies to all users in the group. Changing a jump key for an application must be done before adding the users. Once a user has been added, you cannot change that user’s jump key. The user must change it himself.

The jump key can only be used in relay mode.

If the ATTN key is defined as the jump key, you must be aware of the same important points as those described for defining the ATTN key as the escape key. Refer to defining the ATTN key as the escape key on page 41.

Msg. Received Indicator

This controls the way in which users receive messages from any suspended application. There are three modes:

- **N (Normal)**
  
  The user is notified of a message received from a suspended application by an audible alarm, and a highlighted asterisk is displayed in the M column on the Application Selection panel next to the application that sent the message.

- **J (Interruptive with Jump)**
  
  During an active session, NetView Access Services notifies the user of a message sent from a suspended application by an audible alarm. When the user presses any function key other than the CLEAR key, the present session is interrupted and NetView Access Services automatically jumps to the application that sent the message.
• I (Interruptive with Information)

If the user is working on an application panel, NetView Access Services notifies the user of a message sent from a suspended application by an audible alarm. When the user presses any function key other than the CLEAR key, the session is interrupted and NetView Access Services displays the Application Selection panel with a highlighted asterisk in the M column next to the application that sent the message.

If the user is using the Application Selection panel, NetView Access Services displays an updated panel with a highlighted asterisk in the M column next to the application that sent the message.

If the user is working on a user administration panel, NetView Access Services displays a Message Display panel notifying the user that suspended applications have sent messages. When the user presses any function key other than the CLEAR key, the former panel is displayed and the user can decide on the action to take to view the message.

The users in Normal and External groups can redefine the mode in which messages are received on the Maintain User Parameters panel.

Note: Applications such as monitoring systems that periodically issue messages are not suitable to run under control of NetView Access Services. This is because NetView Access Services does not expect suspended applications to issue more than two messages in this state. This does not apply if Virtual Terminal option Y is specified for the application.

Logon Profile Type

Specifies the default logon profile for this application, for all the users assigned to use applications in this group. G specifies that each user has the group-wide logon profile as default. S specifies that each user has the system-wide logon profile as default. Refer to Chapter 8, “Creating and Controlling Logon and Logoff Profiles” on page 91 for further information. This field is only used for relay mode applications. For Public groups this definition applies to all users in the group.

Automatic Logon

Specifies whether the user assigned to use applications in this group can use automatic logon for this application. Enter Y for Yes or N for No.

This depends on how the system administrator has defined the application. If the system administrator has authorized automatic logon, you can specify Y or N. If not, NetView Access Services assumes N for External groups and for Normal groups. For users logging on to Public groups, see “Automatic Logon for Users of Applications in Public Groups” on page 94. This field is only used for relay mode applications.
Application ID Display

Specifies whether an identifier can be displayed on each panel of an application to help users recognize which application is being used. Enter Y if you want the user to be able to display the identifier, or N to suppress its display. The default is N.

It is recommended to suppress displaying of the application identifier, unless Virtual Terminal option Y has been specified for the application. Unpredictable results can be expected if the identifier is displayed when Virtual Terminal option N is specified for the application.

If you enter Y, you must specify the row and column, and the type of highlighting in which the identifier is to be displayed.

- **Row/Column**

  Specifies the row and column in which the identifier text is to be displayed on each panel of the specified application. You must determine the best place on the panels of each application. You can specify the following:

  - **Row**

    You can enter a value in the range of minus 43 to 43 with the exception of zero. A positive value indicates the actual row on the physical screen counting from the top.

    A negative value indicates a relative row on the physical screen counting from the bottom depending on the number of rows on the physical screen.

  - **Column**

    You can enter a value within the range of minus 132 to 132 with the exception of zero. A positive value specifies a column counting from the left of the physical screen. This is an actual column and specifies the column in which the text of the identifier is to start.

    A negative value specifies a column counting from the right of the physical screen depending on the number of columns on the physical screen. This is a relative column and specifies the column in which the text of the identifier is to start or end. This depends on whether the Virtual Terminal option for the application is set to Y or N. For example, if the option is set to N and you specify -20 and the terminal can display 132 columns, the text ends in column 112 of the row you specify. If the option is set to Y, the text starts in column 113 of the row you specify.

  If you specify row minus 1 and column minus 1, the application identifier is displayed at the bottom right of the screen regardless of whether the terminal screen has 80 or 132 columns. If you specify a position greater than the physical size of the screen, the application identifier is not displayed.
• **Color/Highlight**

  Specifies the color and highlight in which the identifier is to be displayed. The following colors are supported:

  - R Red
  - G Green
  - B Blue
  - W White
  - Y Yellow
  - T Turquoise
  - P Pink.

  The following highlighting is supported:

  - H Highlighted
  - R Reverse video
  - B Blinking
  - U Underlined.

  If the user’s terminal does not support extended color or highlighting, the defaults for the terminal are used.

• **Text**

  The text of the identifier can be up to 30 characters. If no text is entered, the application description on the Application Selection panel is the default.

### Displaying the Parameters of an Application for a Group

Fill in the Group field and the Application field, and enter the DISPLAY command. NetView Access Services responds by filling in the current values in the remaining fields.

### Updating the Parameters of an Application for a Group

Display the current values. Change the values as you require and enter the UPDATE command. NetView Access Services prompts you to confirm the request. Press ENTER. NetView Access Services updates the values as you have specified.

### Listing Applications

**Applications for a Group:** Enter a question mark in the Application field and fill in the Group field. Enter the LIST command. NetView Access Services lists the applications that the specified group has access to.

**Applications for Your Groups:** Enter a question mark in the Application field and leave the Group field blank. Enter the LIST command. NetView Access Services lists all the applications of the groups for which you are an administrator. For system administrators, NetView Access Services lists all the applications on the system (by their group-wide names).
Listing Groups

Your Groups: Enter a question mark in the Group field. Leave the Application field blank. Enter the LIST command. NetView Access Services lists all the groups for which you are an administrator. For system administrators, NetView Access Services lists all the groups on the system for which applications have been defined.

Your Groups That Have Access to a Particular Application: Enter a question mark in the Group field and fill in the Application field. Enter the LIST command. NetView Access Services lists all the groups (for which you are an administrator) that have access to this application. For system administrators, the list shows all the groups on the system that have access to this application.

Assigning a User to a Group

You can use Option 3, Assign a User to a Group, on the Administration Selection panel to define users to a group. How this option is used depends on the type of the group. For Normal NetView Access Services groups, you must define which applications each user can use in the group, certain parameters for each application, and certain authorizations for the user. It is not possible to assign applications to be used by users logging on to Public groups. Therefore, this option need not be used. For External groups, the installation-wide administration exit (EMSEADEX) must be installed to interface with the external security system to use this option. Refer to NetView Access Services Version 2 Customization for further information. When you choose option 3, Assign a User to a Group, on the Administration Selection panel, NetView Access Services displays the panel shown in Figure 25.

<table>
<thead>
<tr>
<th>User</th>
<th>Group</th>
<th>Application</th>
<th>Last update:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fill in or change the following:

- Default Group: _ (Y=Yes/N=No)
- Access Mode: _ (R=Relay/P=Pass/B=Both)
- Terminal Assume: _ (Y=Yes/N=No/C=Conditional)
- Record Authorization: _ (Y=Yes/N=No)
- Shareable: _ (Y=Yes/N=No)
- Pseudo Terminal Name: _ Used by VTAM

Logon variables

&GVAR1 2 3 4 5

Admin Exit Data

Enter a command: d (display), a (add), u (update), l (list), or delete.

COMMAND ==> ________

PF 1=Help 3=End

Figure 25. Assign a User to a Group Panel
Explanation of Fields

The following explanation of the fields applies to Normal and External groups. This panel cannot be used for Public groups.

User
The user ID with which the user logs on to NetView Access Services. It can contain up to 8 alphanumeric characters.

Group
The group name as defined by the system administrator. It can contain up to 8 alphanumeric characters.

Application
The group-wide name for the application. It can contain up to 8 alphanumeric characters.

This is the name of the application that you are assigning to, or deleting from, a user. A user becomes associated with a group when the first application is assigned. This association no longer exists when the user’s last application is deleted. You can decide, on a user-by-user basis, which application name is to be used to associate an application with a user.

Enter eight periods in this field if you want this user to have a Free selection field on the Application Selection panel. See “Assigning the Free Selection Field” on page 75 for further information. Adding one application for a user in an External group automatically adds all the others. Individual applications can then be deleted.

Last Update
When the User, Group, and Application fields are filled in and the DISPLAY command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you assign a user to a group, the field displays your user ID and the date and time of the update.

Default Group
This indicates whether this group is the default group of the user. Enter Y for Yes or N for No. The default value is N for Normal groups, and Y for External groups. The user is assigned to this group if another group is not specified on the Logon panel. If this field contains Y for any application, it will automatically be Y for all applications. You can only have one default group for each user.

Users can see whether the group they logged on to is their default group on their Maintain User Parameters panel. How to define an external group as a default group is explained in NetView Access Services Version 2 Customization.

Access Mode
Specifies the mode of access authorized for individual users of the application. This can be R (relay), P (pass), or B (both). The default is R. The effect of what you specify depends on what mode of access the system administrator has specified for the application. For example, if the system administrator specifies B, you can specify access mode R, P, or B. However, if the system administrator specifies R, then specifying P or B is ignored. If you and the system administrator specify access mode B, the individual users of the application can specify the mode in which they want to gain access to the application.
Terminal Assume
This indicates whether this user can transfer a session with this application from one terminal to another. This is only possible if the system administrator has specified multiterminal access Y for the group. Enter Y for Yes, N for No, or C for conditional. The default is N. If you specify C, assuming a session for an application for this user can no longer be performed with the jump key.

If the system administrator has specified multiterminal access S (secure terminal) for the group, the users assigned to use applications in the group cannot assume sessions with single applications regardless of what you specify. When a user logs on at another terminal, the complete terminal session is taken over and the NetView Access Services Logon panel is displayed on the original terminal.

Record Authorization
This indicates whether or not a user can record a logon profile for this application. This profile can only be used for relay mode, and if the application has been authorized for automatic logon. Enter Y for Yes or N for No. The default is N.

Shareable
This indicates whether or not a user can share a session with this application with another user. This is only possible if the system administrator has specified that this application can be shared and has specified that users assigned to use applications in the group can respond to a request to share a session. The default is N.

Pseudo Terminal Name
Use this field when an application requires a specific logical terminal name for a user. You can enter the name of the pseudo terminal authorized to be used by this user for this application (up to 8 alphanumeric characters). NetView Access Services then uses this name to establish a relay mode session for that application. The default is blank. The use of this field is optional.

The same pseudo terminal names can be specified for the same user for several applications. The specified pseudo terminal can be used for concurrent access to more than one application (one per VTAM application) by the same user.

See “Pseudo Terminal Names” on page 11 for information on pseudo terminals.

This name should not be the same as any name from a pool of names set up by the system administrator using the pseudo terminal prefix, nor should it be assigned to more than one user.

Logon Variables (&GVAR1...&GVAR5)
These fields can contain data to be inserted in logon profiles for relay mode applications or in BIND user data. The variables can be specified when logon sequences are recorded for an application. When, during automatic logon, a variable is requested, the appropriate value set in these fields is used. It can be any data that can be interpreted by the application, for example, printer ID or billing number. Each field can contain up to 8 alphanumeric characters. The default is blank.

Any update you make does not affect users already logged on. The update takes effect after the next logon.
Admin Exit Data

This is a 60-character field in which you can enter data of your choice. The data entered in this field is only valid for external groups. The data is passed to the administration exit, EMSEADEX. For example, you could enter the user’s name in this field. For further details, refer to NetView Access Services Version 2 Customization.

Displaying User and Application Data

Fill in the Application, User, and Group fields, and enter the DISPLAY command. NetView Access Services fills in all the current values.

Adding a User to a Group or an Application for a User

It is not necessary to add every application for every user in External groups.

To add a user to a group or an application for a user:

1. Fill in the Application, User, and Group fields. To add a new user who can use all the applications in the group, put an asterisk in the Application field. To add a new application for all users, put an asterisk in the User field.

   All the other fields have default values, as described in the explanation of the fields. If you require values different from the default values, fill in those fields as required.

   To add all applications accessible by a group to a new user, using the asterisk in the Application field, you must leave the Access Mode and the Pseudo Terminal Name blank, because they can be different for each application. When adding an application for all users, you must leave the Pseudo Terminal Name and the Default Group fields blank, because they may be different for each user.

2. Enter the ADD command. NetView Access Services prompts you to confirm the request.

3. Press ENTER. NetView Access Services adds the user or users with this application or applications to the group definitions.

Deleting One or All Applications of a User

To delete one or all applications of a User:

1. Fill in the Application, User, and Group fields. Leave the remaining fields blank. To delete all the applications for a particular user, put an asterisk in the Application field.

2. Enter the DELETE command. NetView Access Services prompts you to confirm the request.

3. Press ENTER.

This user is no longer authorized to use this application or applications. If you delete all applications for a user, then this user is no longer defined in this group. To delete one application from all users, you must request that the system administrator does it, using option 6, Assign an Application to a Group, on the Administration Selection panel.
Updating User and Application Data

To update user and application data:

1. Display the current data. Change the information as required.

To update the data of a particular application for all users in a normal group, enter an asterisk in the User field. You must leave the Default Group and Pseudo Terminal Name fields blank, because they can be different for each user.

2. Enter the UPDATE command. NetView Access Services prompts you to confirm the request.

3. Press ENTER. The new data becomes the current data.

Any changes you make do not affect users already logged on in the group. The changes take effect at the next logon.

Listing Applications

The LIST commands described in the following do not list Public group applications. For External groups, you can list only the applications that a particular user can use in a specific group by providing both the user ID and the group ID. Listing user information usually requires the complete user database to be scanned. Depending on the size of the database, this can take some time. Therefore, NetView Access Services has a progress indicator that displays the actual status of the List request.

EMS1071D List request in progress. Records read: nnnnnnnnn

All Applications: Enter a question mark in the Application field and leave all other fields blank. Enter the LIST command. NetView Access Services lists all the applications that are assigned to any user in all the groups for which you are an administrator. For system administrators, it lists all the applications in the system that are assigned to a user.

Applications of a Particular User: Enter a question mark in the Application field and fill in the User field. Leave the other fields blank. Enter the LIST command. NetView Access Services lists the applications that this user can use in the groups for which you are an administrator. For system administrators, NetView Access Services lists all the applications that this user can use.

Applications of a Group: Enter a question mark in the Application field and fill in the Group field. Leave the other fields blank. Enter the LIST command. NetView Access Services lists the applications of this group that are assigned to a user.

Applications That a Particular User Can Use in a Particular Group: Fill in the User and the Group fields, and put a question mark in the Application field. Enter the LIST command. If you are an administrator of the group or a system administrator, NetView Access Services lists the applications of the user in this group.

Listing Users

The LIST commands described here only list the users in Normal groups. Listing user information usually requires the complete user database to be scanned. Depending on the size of the database, this can take some time. Therefore, NetView Access Services has a progress indicator that displays the actual status of the List request.

EMS1071D List request in progress. Records read: nnnnnnnnn
**Users in Your Groups:** Enter a question mark in the User field and leave the other fields blank. Enter the LIST command. NetView Access Services lists all the users in the groups you administer. For system administrators, NetView Access Services lists all the users on the system.

**Users with Access to a Particular Application:** Enter a question mark in the User field and fill in the Application field. Leave the other fields blank. Enter the LIST command. NetView Access Services lists the users, in the groups that you administer, who have access to this application. For system administrators, NetView Access Services lists all the users on the system who have access to this application (assuming all the groups use the same name for the application).

**Users Assigned to use Applications in a Particular Group:** Fill in the Group field and enter a question mark in the User field. Leave the other fields blank. Enter the LIST command. NetView Access Services lists the users of this group, provided you are an administrator of this group or a system administrator.

**Users That Can Use a Particular Application in a Group:** Fill in the Group and Application fields, and put a question mark in the User field. Enter the LIST command. NetView Access Services lists the users, provided you are an administrator of this group or a system administrator.

### Listing Groups

**Your Groups:** Enter a question mark in the Group field and leave the other fields blank. Enter the LIST command. NetView Access Services lists the groups you are authorized to administer. For system administrators, NetView Access Services lists all the groups.

**Groups to which a Particular Application Is Assigned:** This applies to Normal groups only. Enter a question mark in the Group field and fill in the Application field. Leave the other fields blank. Enter the LIST command. NetView Access Services lists your groups to which the application is assigned. For system administrators, NetView Access Services lists all groups to which this application is assigned. At least one user must be assigned to use the application in the group.

**Groups of Which a User Is Assigned to Use Applications:** This applies to Normal groups only. Enter a question mark in the Group field and fill in the User field. Leave the other fields blank. Enter the LIST command. NetView Access Services lists the groups (for which you are an administrator) to which this user is assigned to use applications. For system administrators, NetView Access Services lists all the groups to which this user is assigned to use applications.

**Groups in Which a User Can Use a Particular Application:** This applies to Normal groups only. Fill in the User and Application fields and put a question mark in the Group field. Enter the LIST command. NetView Access Services lists your groups in which this user can use this application.
Assigning the Free Selection Field

You can assign the free selection field to a user by specifying eight periods (........) in the Application field on the Assign a User to a Group panel, and adding the application for the user (for a Normal group).

This field must also be authorized by the system administrator who must specify eight periods (........) in the Application field of the Assign an Application to a Group panel. If the group administrator authorizes a user to use all applications in the group by specifying an asterisk (*) in the Application field, then the free selection field is also assigned to the user.

If a group administrator assigns this facility to a user, then that user can access all applications in the group, even if the user was originally authorized to access only a subset of the group applications.

For Public and External groups the free selection field is made available to all users when it is assigned to the group by the system administrator. You can delete it for individual users in External groups.

The Free Selection application mechanism cannot be used together with the external application authorization feature. When using external application authorization, all the applications that the user is allowed to access are already displayed on the Application Selection panel. Any application that a user is not allowed to access, is not displayed on the panel, and cannot be accessed.
Chapter 6. Broadcast Administration Tasks

If you are authorized as a broadcast administrator, you can send selective broadcast messages. To do this, enter the BMSG command on the Application Selection panel. The panel shown in Figure 26 is displayed.

The panel is divided as follows:

- An area where you can define the message ID and language ID, and a member name of a partitioned data set that contains the message text.

- An area where you can specify to which user or users the message is to be sent to by defining various criteria. You can mix this criteria for a dedicated selection. You must, however, specify the language ID.

**Note:** The specified criteria are not parsed or checked for validity. For example, you are not informed of a misspelled user ID and your message will not be received by the user.

- A field to specify whether the message is to be sent as an interruptive message.

- An area to specify whether the message is to be time-controlled. Messages that are time-controlled are sent within a predefined time period. Therefore, you must specify a start and a stop time for your message. You can also specify whether the message is to be purged at the stop time.

Messages that are not time-controlled are sent immediately.

![Figure 26. The Broadcast Selectively Panel](image-url)
Explanation of Fields

**Message ID**
This field can contain up to four decimal digits that specify the identification number of the message. If a new message is to be added, you can leave this field blank because an identification number is automatically filled in by NetView Access Services. For a message to be displayed, updated, or deleted you must specify its identification number in the range of 1 to 9999.

**Language ID**
This field contains one number that specifies the language in which the message is to be sent. Those users that have selected that language receive the message. If you want to send a message with no language criterion, you can enter an asterisk in this field. A message for which a language ID has been specified supersedes a message specified with an asterisk when a user receives messages. The system language default is the default value.

**Last Update**
When the Message ID and Language ID fields are filled in and the DISPLAY (D) command is used, the Last Update field displays the user ID of the system administrator who last updated the parameters, and the date and time of the update. When you add or update a message, the field displays your user ID and the date and time of the update.

**Member Name**
This field contains up to eight characters. You can fill in this field with the name of a member in a partitioned data set where the message text is stored. If you specify a member name that does not exist, an error message is generated. The partitioned data set name must be defined during NetView Access Services startup.

**User**
This field contains up to eight characters that specify the user ID to which the message is to be sent. This field is ignored if it is left blank.

**Group**
This field contains up to eight characters that specify the name of the group to which the message is to be sent. This field is ignored if it is left blank.

**Terminal**
This field contains up to eight characters that specify the VTAM network name of a user terminal to which the message is to be sent. You can use a generic terminal ID to select a group of terminals. This field is ignored if it is left blank.

If the user is logged on at more than one terminal, the message is displayed at the terminal where the user first presses a PF key, PA key, or the ENTER key.

**System Application Name**
This field contains up to eight characters that specify the system-wide name of an application to which the message is to be sent. This is ignored if it is left blank.

**Group Application Name**
This field contains up to eight characters that specify the group-wide name of an application to which the message is to be sent. This field is ignored if it is left blank.
Interruptive Message
This field can contain Y for Yes or N for No to specify whether the message is to be sent in interruptive or normal mode.

Time Controlled Message
This field can contain Y for Yes, N for No, or D for Daily. This specifies whether the message is to be handled as a time-controlled message or a nontime-controlled message. If you specify Y or D, fill in the Start of broadcasting, End of broadcasting, and Purge message fields. If you specify Y, the message is active from the time you define in the Start of broadcasting field until the time you specify in the End of broadcasting field. If you specify D, the message is resent (updated) every 24 hours from the time you specify for Start of broadcasting until the time you specify for End of broadcasting. If you specify N in the Time Controlled Message field, default values are used.

- **Start of broadcasting**
  These two fields contain ten and five characters, respectively, that specify the date and time that the message is to become active. At the specified time, all addressed users are notified that there is a message pending.
  The defaults are:
  
  Date: System date  
  Time: 00.00
  
  If you specified D in the Time Controlled Message field, the message is resent at the same time every 24 hours.

- **End of broadcasting**
  These two fields contain ten and five characters, respectively, that specify the date and time when the message is to be suspended. At the date and time you specify, the message will no longer be seen by the users. However, if N is specified for Purge message, the message will still be available in the system. The defaults are:

  Date: 9999-12-31
  Time: 23.59

- **Purge message**
  This field can contain Y for Yes or N for No to specify whether the message is to be purged after it is suspended.

Notes:
1. The date, time, and purge message fields must be specified for time-controlled messages.
2. The content of the time fields must be in chronological order, otherwise an error message is generated.
3. The International Organization for Standardization (ISO) standard format for date and time is used. This format is displayed on the panel.
Displaying a Selective Broadcast Message

To display the current values of a message, enter the Message ID and Language ID in the appropriate fields on the Broadcast Selectively panel, and use the DISPLAY (D) command. To display the message text for the appropriate language ID, press the ENTER key. The Generate or Modify a Broadcast Message panel is displayed, as shown in Figure 27. You can edit the message text on this panel. If there is more than one page of messages, you can scroll through them using the Forw and Backw PF keys.

```plaintext
EMSPS8 Generate or Modify a Broadcast Message
Terminal: I123456B

Message text
--------------------------------------------------------------------------
OFFICE is not available today___________________________________________
Tel. 129799284________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

Press CLEAR to reset message text; press End PF key to return.

COMMAND ==>________
PF 1=Help  3=End  7=Backw  8=Forw
```

Figure 27. Generate or Modify a Broadcast Message Panel

Adding a Selective Broadcast Message

To add a new message you can:

- Modify the text of an existing message.
- Enter the message text of a new message.
- Specify the member name of the partitioned data set to be read in as follows:
  - Enter the member name of the partitioned data set in the appropriate field on the Broadcast Selectively panel.
  - Fill in all other fields and press ENTER.
  - Edit the message text on the Generate or Modify a Broadcast Message panel.
  - Press the End PF key to return to the Broadcast Selectively panel.
  - Enter the ADD (A) command and press ENTER.
  - Press ENTER to confirm the add request. If the message data set is shared and an ADD is already in process, you receive a message telling you that the profile database is in use and that you must try again later.
Updating a Selective Broadcast Message

To update a message, enter the Message ID and Language ID and the new values in the appropriate fields on the Broadcast Selectively panel, and use the UPDATE (U) command. If you want to modify the message text, you can use the DISPLAY (D) command to display the actual stored values for the message.

When you enter the UPDATE (U) command, NetView Access Services fills in any blank fields with the actual values for the specified message, and displays a message asking you to confirm the update request.

**Important:** The UPDATE (U) command, unlike the DISPLAY (D) command, does not automatically read the message text of the specified message. Therefore, ensure that the message text is correct before updating the message.

If the message data set is shared and an UPDATE is already in process, you receive a message telling you that the profile database is in use and that you must try again later.

**Rules for Updating Selective Broadcast Messages:** You must follow certain rules when updating a message. Noncompliance with these rules causes NetView Access Services to generate an error message:

1. A message cannot change its Message ID or Language ID by an UPDATE command. The Message ID together with the Language ID is the unique access key for a stored message and must not be changed.

2. All input data must be valid for the UPDATE (U) command to be processed. Blank fields are filled in with the appropriate values of the old message when NetView Access Services asks you to confirm the update request.

3. You cannot use the member name. You can only update message text by modifying it in the text field on the Generate or Modify a Broadcast Message panel.

Deleting a Selective Broadcast Message

To delete a message, enter the Message ID and Language ID in the appropriate fields on the Broadcast Selectively panel, and use the DELETE command. A message is only deleted if the Message ID and Language ID match. When you press ENTER, a message is displayed asking you to confirm the delete request. Pressing ENTER again deletes the message.

If the message data set is shared and a DELETE is already in process, you receive a message telling you that the profile database is in use and that you must try again later.
Listing Selective Broadcast Messages

You can list the selective broadcast messages by entering the LIST (L) command in the command line on the Broadcast Selectively panel. The List Messages panel is displayed as shown in Figure 28.

<table>
<thead>
<tr>
<th>ST</th>
<th>MID</th>
<th>Language ID</th>
<th>Message Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0015</td>
<td>1</td>
<td>OFFICE is not available today.</td>
</tr>
<tr>
<td>A</td>
<td>0011</td>
<td>*</td>
<td>The following rules apply to all NetView Access Services users:</td>
</tr>
<tr>
<td></td>
<td>0001</td>
<td>*</td>
<td>Please log off. Shutdown in 5 minutes!</td>
</tr>
<tr>
<td></td>
<td>0002</td>
<td>*</td>
<td>Please log off. Shutdown in 1 minute!</td>
</tr>
</tbody>
</table>

Figure 28. List Messages Panel

Explanation of Columns

**ST**  Status indicator. An A for a message that is active in the system and a blank for an inactive message.

**MID** Message ID.

**L**  Language ID of the message, or an asterisk for no specific language.

**Message Text**  The text of the messages.

**Notes:**

1. Several messages may exist with the same Message ID, but with different language IDs.

2. If all the messages do not fit on one panel, you can scroll forward and backward using the PF keys.
Chapter 7. Security Aspects of NetView Access Services

This chapter describes the NetView Access Services security aspects for the following:

- Using variables
- Automatic logons
- Control of user access
- Access modes that a user can use
- Timing out
- Multiterminal authorization
- Terminal-assume authorization.

For information on the interfaces to external security systems, refer to NetView Access Services Customization.

Using Variables in NetView Access Services

When establishing a session with an application, ampersand (&) variables can be used instead of hard-coded values. Each time NetView Access Services encounters an ampersand variable while establishing a session, it is replaced by the value specified for the variable. However, for additional security, do not use a hard coded password in any logon profile because it is stored in a VSAM data set. The following ampersand variables can be used:

**&UID**
User ID. NetView Access Services uses this value for BIND user data or during an automatic logon to an application when it encounters the variable &UID in the logon profile. If no value is specified, NetView Access Services assumes the NetView Access Services user ID by default.

**&ACCNO**
Account number. NetView Access Services uses this value for BIND user data or during an automatic logon when it encounters the variable &ACCNO in the logon profile. If no value is specified, NetView Access Services uses information that has been specified for the group by the system administrator as the default.

**&PWD**
Password. NetView Access Services uses this value for BIND user data or during an automatic logon when it encounters the variable &PWD in the logon profile. If no value is specified, NetView Access Services uses the NetView Access Services password as the default. If a password is changed during logon to NetView Access Services, the variable &PWD takes the value of the NetView Access Services New field (from the NetView Access Services Logon panel), which becomes the current password when logon processing has been completed.
&NPW
New password. NetView Access Services uses this value for BIND user data or during an automatic logon when it finds &NPW in a logon profile or in the BIND user data. If no value is specified, no default is used by NetView Access Services. The variable is left blank.

&OPW
Old password. NetView Access Services uses this value for BIND user data or during an automatic logon when it finds &OPW in a logon profile or in the BIND user data. If no value is specified, and the password is changed during a logon to NetView Access Services, then this variable takes the current NetView Access Services password as default. The current NetView Access Services password will be the old password when the logon processing has been completed. If a user disconnects from NetView Access Services and the password is changed during a reconnect to NetView Access Services, the variable &OPW takes no default password.

&SPW
Sensitive password. During the recording of a logon profile, you can use the sensitive password &SPW variable. When NetView Access Services is running the logon profile, it stops at this variable and prompts you to enter your password or other sensitive data. When the application recognizes the correct input, the logon continues.

&UVAR1 through &UVAR4
Users can assign values for these variables for each of their applications. The variables can be used for BIND user data or during an automatic logon.

If no values are specified, no default is assumed by NetView Access Services.

&GVAR1 through &GVAR5
A group administrator can assign values for these variables for users assigned to use applications in groups. The variables can be used for BIND user data or during an automatic logon.

&1 through &3
A user can assign temporary values to variables &1 through &3. The values assigned to these variables can be used by a user when selecting an application from the Application Selection panel. For example, CICS users can pass user ID, transaction ID, and account directly to the CICS application instead of waiting for an appropriate panel and then entering the data. Users must be told for what they are expected to use these variables.

Variables to which values cannot explicitly be assigned, but can be used in BIND user data or in automatic logon profiles, are:

&T卢
This contains the LU name of the user’s terminal. Each terminal has a different value for TLU.

&LCD
This contains the language identifier for the language currently in use at the terminal, as specified in the language name exit (EMSELNEX). See the NetView Access Services Version 2 Customization for details of this exit.
&OWNLU
This contains the LU name of the NetView Access Services that owns the corresponding terminal. Every user on the same NetView Access Services system has the same value for OWNLU.

&GRP
This contains the group ID under which the user is logged onto NetView Access Services.

The variables are described in detail in *NetView Access Services Version 2 User’s Guide*. Refer to Chapter 9, “Using BIND User Data to an Application” on page 97 for information on ampersand variables.

## Automatic Logons

If relay mode is used to access an application, an automatic logon profile can be invoked to assist the user’s logon. Authorization to use this function is controlled by the NetView Access Services administrators. The system administrator must authorize the use of the automatic logon facility when defining the application to the system.

If you are a system administrator, you add each application to the NetView Access Services system and decide whether to authorize automatic logon for this application. If automatic logon is allowed, you can set up a system-wide logon profile using variables.

If you are a group administrator, you can decide whether your group can use automatic logon for an application. You are restricted by the way the system administrator has set up the application for the system. You can set up group-wide logon profiles.

You can also authorize individual users assigned to use applications in your group to record logon sequences. If a user is not authorized to record logon sequences, only the group logon profile or the system logon profile can be used for automatic logon.

## Control of User Access

NetView Access Services allows the administrators to set up access parameters at the group and user level.

Group administrators have access to parameters for their own groups only. They control the access that users have to applications. The installer can limit the terminals that can be used at startup with the INPLU parameter. With the Language Verification exit the terminals can be further restricted.

By using the external application authorization feature, you can ensure that users only have access to the applications that they are authorized to use by RACF.
Access Modes That a User Can Use

As a group administrator you can use the Define a User to a Group panel (option 3 on the Administration Selection panel), to determine whether users can use an application in relay mode, pass mode, or both. If users are allowed to use both modes, they can decide which mode to use, by using the select pass (SP) and select relay (SR) commands. Relay mode is the default.

On the same panel you can also define whether they can use the terminal-assume feature of NetView Access Services. For this feature, your group must have been authorized for multiterminal access by the system administrator using option 5, Define a Group.

Users assigned to use applications in the group can then log on to NetView Access Services at more than one terminal at a time. To safeguard information, they can assume sessions from one terminal to another, so that no one can see the information on the first terminal. It also saves users from having to return to the first terminal to log off or disconnect from an application before using it at the current terminal.

Timing Out

To be timed out means that a user is logged off without requesting it. This prevents information from being displayed for long periods of time when the user is called away from the terminal. There are a number of ways a user can be timed out from an application or from NetView Access Services. Timing out can happen in any of the following ways:

- The installer of NetView Access Services can set a “no-keystroke time-out”. This is the maximum amount of time that the user can remain logged on to NetView Access Services without pressing any key. As soon as that time is reached, NetView Access Services disconnects the user and displays the Logon panel at the terminal.

- The system administrator can set a NetView Access Services time-out for each application. When the user is timed out from an application, NetView Access Services logs the user off from the application and displays the Application Selection panel.

- In addition to the NetView Access Services time-outs, each application can also have a time-out of its own. These time-outs are independent of NetView Access Services, but have the same effect as a NetView Access Services time-out for an application. The application logs the user off and NetView Access Services displays the Application Selection panel.
Multiterminal Access Authorization

Multiterminal access authorization is given by the system administrator for the group. With this authorization, the user can log on to NetView Access Services with the same user ID and password at more than one terminal. The terminals are linked in a multiterminal session. The same Application Selection panel is shown on each terminal, with the same applications active (highlighted).

A user can only use each application from one terminal at a time in a multiterminal session.

However, if the system administrator specifies S for multiterminal access authorization, users of applications in the group can log on at another terminal, but the complete terminal session is taken over and the NetView Access Services Logon panel is displayed on the original terminal.

Terminal-Assume Authorization

There is another type of authorization that is related to multiterminal access authorization. It is referred to as terminal-assume authorization, and can be given by the group administrator for each group application assigned to be used by a user.

When users are logged on to two or more terminals, with the same user ID and group ID, and want to use an application at one terminal that is currently being used at another terminal, then they can “assume” the session from that terminal. The group to which the user is assigned to use applications must have multiterminal access authorization for this function to be used.

When a user selects an application that is in use at another terminal, NetView Access Services disconnects that terminal and displays the Logon panel, provided that the terminal types are compatible. The user takes over the application at the terminal at the point at which it was disconnected. If the terminal types are not compatible, a message is displayed and the application cannot be taken over.

Note: Terminal compatibility is based on the session and terminal characteristics. Figure 29 shows how NetView Access Services determines the compatibility. The comparison is performed dynamically, the actual session characteristics are compared to the terminal characteristics.
Figure 29. Terminal-Assume Compatibility Handling
Figure 30. Terminal-Assume Compatibility Handling Continued
Chapter 8. Creating and Controlling Logon and Logoff Profiles

This chapter describes how you create and control profiles for automatic logon and logoff. It describes:

- Automatic logon and logoff
- Recording logon and logoff sequences
- Recording commands
- Tracing logon and logoff sequences
- Activating a logon profile as a group-wide or system-wide profile.


NetView Access Services functions such as terminal assume and selective broadcast are suspended during automatic logon and logoff.

If a REXX exec has been defined to perform automatic logon or logoff, then the descriptions in this chapter do not apply.

Automatic Logon and Logoff

When the user selects an application in relay mode, NetView Access Services looks for a logon profile that has been previously recorded. There are three levels of profile for logging on and off:

- Users can create their own individual logon profiles (user profiles).
- A group administrator can create a logon profile that can be used by all users assigned to use a particular application in the group (groupwide profiles).
- A system administrator can create a logon profile that can be used by every user of the system (system-wide profiles).

If there is no logon profile for this application, NetView Access Services displays the first panel of the application. For example, this might be a logon panel, in which case the user can log on manually.

If NetView Access Services finds a logon profile, it logs on to the application for the user. The commands and data in the profile are transmitted to the application as required. The user does not have to perform the logon manually, but can use the application as soon as the automatic logon is complete.

When the user logs off from an application using the NetView Access Services LF, LOGOFF, or EXIT command, NetView Access Services looks for a logoff sequence. If there is one, NetView Access Services uses it to perform the logoff. If there is no logoff sequence, NetView Access Services terminates the session immediately. In this case the application reacts as if the power to the terminal had been switched off.
Authorizing Automatic Logon

The system administrator must authorize the use of automatic logon when defining the application to the system on the Define an Application for the System panel. The group administrator can in turn authorize its use at group level on an application basis on the Maintain Group Parameters panel. When automatic logon is authorized for an application, the following parameters can be given values:

- Alternative sequences
- Record authorization
- Logon profile type
- Active profile

Alternative Sequences
Using option 4, Define an Application for This System, on the Administration Selection panel, the system administrator defines how many alternative sequences each application handles in each logon profile. This value dictates how many alternative sequences you can record for each logon profile for that application.

Authorization to Record the Profile
Before users can record any sequences, the group administrator must give them record authorization, using option 3, Define a User to a Group, on the Administration Selection panel. Each user that can record a logon sequence must be defined as a user of that application.

Logon Profile Type
For each group, the group administrator decides, using option 2, Maintain Group Parameters, on the Administration Selection panel, whether the group-wide logon profile or the system-wide logon profile should be the default (assuming that both exist). At the user level, the user (if not a user of applications in a Public group) can select which profile to use: system, group, or (if authorized to record one for a particular application) user profile. The user can dynamically update the profile used from one logon to another.
Active Profile
The user specifies which of two profiles should be the active one. An overview of the automatic logon selection is shown in Figure 31.

![Figure 31. How the Logon Profile is Selected](image)

Recording the Logon and Logoff Sequences
To create a logon profile, you record a sequence of steps for logging on and logging off. You give NetView Access Services the command to begin the recording for a particular application. NetView Access Services responds by displaying the first panel of that application. You log on manually, entering data, which can include variables. You can continue recording up to the point at which you usually start your work. For example, if you are recording a logon sequence for VM, you could select OFFICE after the VM logon is completed. To end the recording, you use the escape key to return to the Application Selection panel, and file the recording. You use a similar method for recording a logoff sequence. The *NetView Access Services Version 2 User’s Guide* describes in further detail how to record sequences.
As an administrator, you can create a system-wide or group-wide logon profile by recording a logon or logoff sequence and filing it in your own user logon profile. To do this you must also be authorized as a user of the application. You must then activate the profile so that it can be used by your group or by all users.

If you are a group administrator, you specify whether each individual user has the authorization to record logon sequences. If a group-wide and system-wide logon profiles exist, each authorized user can choose whether to use the system-wide profile, the group-wide profile, or one of their own. The group administrator decides whether the default profile for the users assigned to use applications in the group is the group-wide or system-wide logon profile.

If a system-wide or group-wide logon profile is recorded, the user ID and password ampersand variables should be used, otherwise your user ID and password will be stored in the profile in clear text.

**Automatic Logon for Users of Applications in Public Groups**

Users of applications in Public groups can only use a group-wide or system-wide logon profile. They cannot record their own logon sequences. This also means that administrators cannot record system-wide or group-wide sequences while working in a Public group. For group administrators to be able to record a group-wide logon sequence, it is necessary to temporarily change the group type to Normal. Group administrators can then log on and, assuming they have record authorization, create and activate their group-wide logon profile. The group type should then be changed back to Public (by the system administrator). The logon profile to be used (group-wide or system-wide) is specified by the group administrator for the whole group on the Maintain Group Parameters panel.

**Tracing Logon and Logoff Sequences**

You can trace the steps of a logon sequence for an application using the TR command. NetView Access Services responds by displaying the first panel of the logon sequence and then generates an audible alarm. Pressing ENTER displays the next panel of the sequence. In this way, you can trace the sequence and see what was recorded for each step of the sequence. Pressing any key other than ENTER ends the trace. A logoff sequence is traced using a similar procedure. For further information on tracing logon and logoff sequences, refer to NetView Access Services Version 2 User’s Guide.

**Description of the Recording Commands**

The following recording commands can be used on the Application Selection panel:

- **BR** Begins recording a sequence
- **BRA** Begins recording an alternative sequence for an existing profile
- **QR** Quits recording
- **FR** Files a sequence in the active logon profile or as an alternative into an active profile
FRI  Files a sequence either in an inactive profile or as an alternative sequence into an inactive profile (depending on whether you used BR or BRA to begin the recording)

FRM  Files a sequence that you began with BRA as a main logon sequence (instead of an alternative sequence)

AG  Activates a profile that you have recorded and filed already, as a group profile

AS  Activates a profile that you have recorded and filed already, as a system profile

TR  Traces, step by step, a profile for automatic logon or logoff.

---

Activating a Recording as a Group-Wide or System-Wide Profile

After you have recorded a sequence and filed it, NetView Access Services stores it as one of your own two user logon profiles. Make it your active user logon profile, using the Maintain User Parameters panel. Refer to NetView Access Services Version 2 User's Guide to see how to do this.

When you have tested the profile to make sure it functions correctly, make it into the group-wide or system-wide profile for that application, using the activate group (AGn) or activate system (ASn) command, as appropriate.

The AG command can only be used by a group administrator (or a system administrator acting as a group administrator), for the group in which he is currently logged on.

The AS command can only be used by a system administrator.

If you record group-wide or system-wide for an application, users can decide whether or not to use them or to use profiles recorded by themselves. If users are not authorized to record their own profiles, they can use only the group-wide or system-wide profile. To use the AG or AS command, enter it on the Command line on the Application Selection panel. An example of using the AG command is shown in Figure 32.

```
1 VM1 07:30 PF15 VM Pass mode
2 VM2 07:30 PF16 VM2 Relay mode
3 IMS 07:30 PF17 IMS Relay unique
4 OFFICE 07:00 PF18 OfficeVision/MVS Relay mode
5 TSO 07:30 PF19 TSO
6 DWCICS 07:00 PF20 DW/370 CICS DW111 Relay mode
7 NETVIEW 08:00 PF21 NETVIEW 2.0 Pass mode
F ........ PF22 Free selection
```

COMMAND ==> ag vm1

Figure 32. Using the AG Command

If a logon profile contains variables, each user’s default values are called during automatic logon with this logon profile.
Chapter 9. Using BIND User Data to an Application

This chapter explains what BIND user data is and describes the types that exist.

What BIND User Data Is

BIND user data is data that is sent to an application automatically when a session is requested. Some applications can interpret this data as logon information for the application, in which case the data works like an automatic logon. You can include variables in BIND user data. You can also use this facility to help the user in automating the logon process in pass mode.

Defining BIND User Data

The system administrator defines one set of BIND data for each application for all NetView Access Services users using option 10, Define BIND User Data for Applications, on the Administration Selection panel. System variables (for example, &UID, &PWD, &ACCNO), group variables (for example, &GVAR1 through &GVAR5), user variables (for example, &UVAR1 through &UVAR4) and selection panel variables (for example, &1 through &3) can be used to define the BIND data. If variables are used, the system, group, or user variable values are substituted into the BIND user data before it is sent to the application. The group administrator can establish the values for the group variables, but the user can define the values for the system and user variables for each application using the user administration facility. For a detailed explanation of these variables, see the NetView Access Services Version 2 User's Guide.

Since the user can define the value of these variables on an application basis using the Maintain User Parameters panel, different values can be assigned to the same variables for different applications. For example, the user can define the variable &UID to be one value for a CICS application and another value for access to TSO. If the &UID variable is defined by the system administrator to be included in the user BIND data, then a different user ID can be passed to each of the applications.

However, for this facility to be used effectively to assist the user in the logon process, the application must be able to interpret this BIND user data. Some applications can interpret the data as logon information, while other applications ignore or discard the information. For example, TSO/E accepts the user ID or logon ID, but not the password, as part of the BIND user data. If the password is included in the BIND to TSO/E, it is flagged as an invalid parameter for the user logon. CICS/MVS can accept user ID and password, provided that a user program is written to intercept the data, decipher the parameters, and carry out the appropriate logon transactions.
There are two types of BIND user data, structured and unstructured:

**Structured** This data uses unique identifiers (keywords) to format information in the BIND, for example, UID=TUID, and is indicated by X’00’ in the first byte of the transmitted data. This data can be sent to another NetView Access Services to log on to that one. Each field of user data in the BIND is in the form of a length field, a unique identifier, and data.

**Unstructured** This format defines user data in the BIND as positional data. This data is sent to the selected application as it is defined to NetView Access Services. For further information, refer to “Unstructured BIND User Data” on page 100.

When defined as an application, NetView Access Services supports both structured and unstructured BIND user data.

**Structured BIND User Data**

You should check that the application can accept and interpret structured BIND user data. Also consider the security. Using structured BIND user data may result in a password appearing on a screen. You can enter the BIND user data in structured form on the Define BIND User Data for Applications panel. Use the following keywords:

- **UID=** User ID
- **OPW=** Password
- **NPW=** New password
- **GRP=** Group ID
- **OLU=** Originating LU
- **ILU=** Intermediate (initiating) LU
- **ALU=** Target application or LU
- **TRN=** Transaction name
- **EMP=** Employee serial number
- **ACC=** Account code
- **LCD=** Language code
- **RCT=** Routing count
- **XLU=** Associated LU (printer)
- **FDF=** Free data form.

The general form of all structured BIND user data is:

```
keyword=keyword-value,...
```

The following describes the rules for writing the parameter statements:

1. The keywords may be specified in any order.
2. No blanks may be included in a keyword specification. For example,

   ```
   UID=AAAAA
   ```

   is correct, but

   ```
   UID = AAAAA
   ```

   results in an error and NetView Access Services cannot process such a keyword.
3. The statements are separated only by commas. Except for the last parameter, a comma must immediately follow the parameter value. For example,

```
UID=AAAAA ,OPW=BBBBB
```

is correct, but

```
UID=AAAAA ,OPW=BBBBB
```

results in an error, because the blank immediately following a keyword value signals the end of the input. So, in the second example, OPW=BBBBB is ignored. The four lines on the panel are regarded as a single 256-character input field. You must complete one line before continuing on to the next.

4. Free format data must be inserted within single quotation marks ('). For example, FDF='Free data form'.

NetView Access Services translates structured BIND user data before transmitting it to the applications. A stream of BIND user data consists of subfields, each having the following format:

```
<LL><ID><DATA>
```

where:

- **LL** Length Field (1 byte) of the parameter not including this byte itself
- **ID** Identifier (1 byte) of the parameter
- **DATA** Value of the parameter.

There is an identifier (ID) for each keyword parameter. The following IDs have been defined:

- X'81' User ID
- X'82' Password
- X'83' New Password
- X'84' Group ID
- X'85' Originating LU
- X'86' Intermediate (initiating) LU
- X'87' Target Application or LU
- X'88' Transaction Name
- X'89' Employee Serial Number
- X'8A' Account Code
- X'8B' Language Code
- X'8C' Routing Count
- X'8D' Associated LU (Printer)
- X'FF' Free Data Form.

If you enter the location on the Logon panel, and the user ID and password in the user ID and Password fields, the data is taken as structured, and is translated before being transmitted to the NetView Access Services at the other location.

The following is an example of how to enter structured BIND user data:

```
UID=UID,OPW=BRWN,GRP=SYSGRP,FDF='FREE DATA FORM'
```
NetView Access Services interprets this input into the format:

```
008EECC08CDEED0FCDC4CCEC4CDDD (Hex representation)
```

You read the hex representation vertically. So the characters along the top (labeled: Character representation) are represented in hexadecimal format by the two hexadecimal digits vertically beneath them.

- The first 00 indicates that this is structured BIND user data
- X'05' is the length field of the first parameter (TUID)
- X'81' indicates that the first parameter is a user ID
- TUID is the value of the first parameter
- X'06' is the length field of the second parameter (BRWWN)
- X'82' indicates that the second parameter is a password
- BRWWN is the value of the second parameter
- X'0F' is the length field of the third parameter (Free Data Form)
- X'FF' indicates that the third parameter is a piece of Free Data Form
- FREE DATA FORM is the value of the third parameter.

The lowercase “a” (that appears before TUID) is the character represented by X'81', but it is irrelevant to the BIND user data. Similarly the lowercase “b” that appears before BRWWN is not part of the data but it appears here because it is the character represented by X'82'.

**Unstructured BIND User Data**

You must ensure that the application can accept and interpret unstructured BIND user data. Also consider the security aspects. For example, using unstructured BIND user data may result in a password appearing on a panel. You can enter the BIND user data in unstructured form on the Define BIND User Data for Applications panel.

When NetView Access Services receives unstructured data, it interprets it as positional data with the following format:

```
User ID/Password/New Password/Application ID/Group ID/Location ID/Language
```

The slash character (/) is used as a delimiting character. If you leave out one of the variables, you must type two slash characters to denote a blank field of data. The values between the slash characters can contain up to 8 characters (leading blanks are not permitted).

Language should be given as a 3-character abbreviation. This is explained in the Language Name exit EMSELNEX in NetView Access Services Version 2 Customization.
Entering BIND User Data

The length of the BIND user data must not exceed 255 characters. Remember that the variable might have a different number of characters from the actual value. The total length of the data cannot exceed 255 characters after the variables have been replaced by actual values. Refer to Chapter 4, “System Administration Tasks” on page 31 for more information about how to define BIND user data for the applications of your NetView Access Services system.

Variables for BIND User Data

You may find it useful to use variables in the BIND user data. You put the variable name where you would otherwise put an actual value. You can update the actual values without changing the BIND user data. Refer to “Using Variables in NetView Access Services” on page 83 for a description of the variables.

Important Security Consideration: If you specify values for the variables &PWD, &NPW, and &OPW for BIND user data, you run the risk of passwords being visible on panels of applications, because each application responds differently to BIND user data.

The following variables can be used:

Maintain User Parameters panel
&UID, &ACCNO, &PWD, &NPW, &OPW, and &UVAR1 through &UVAR4.

Assign a User to a Group panel
&GVAR1 through &GVAR5.

Application Selection panel
&1 through &3.

Variables to which you do not assign values, but can use in BIND user data are &TLU, &LCD, &OWNLU, and &GRP.
Part 3. Batch Load and Reporting Utility

This part provides information on the Batch Load and Reporting Facility.
Chapter 10. Using the Batch Load and Reporting Utility

The Batch Load and Reporting Utility (abbreviated to Batch Load) enables the NetView Access Services profile data sets to be updated in batch.

Batch Load can be used to update profile information when mass updates are necessary. Such situations occur in the installation phase or when user departments reorganize. Batch Load runs as a separate job and can perform the updates directly on the NetView Access Services profile database.

The main functions provided by Batch Load are:

- Command statements used to formulate all the necessary updates on the NetView Access Services profile database.
  - The command statements are in a free format and use, where possible, the same keywords used on the respective NetView Access Services panels.
  - The command input file can be created automatically, for example, by a TSO CLIST from already existing user or application definitions of an installation.
- A list command enables you to generate list reports showing the current characteristics of the different profiles in the NetView Access Services profile database.
- Different operating modes enable you to specify the execution types such as:
  - **VERIFY** The Batch Load commands are verified, but not executed.
  - **EXECUTE** The correct Batch Load commands are executed immediately.
  - **CONDITIONAL** All the Batch Load commands are verified in a first step. Only if all the commands are correct can they be carried out in a second step.

Functional Summary

Batch Load carries out the following (see Figure 33 on page 106):

- Parses the options from the PARM field of the EXEC statement and sets the operational mode of the Batch Load.
- Reads the Command Input Data Set and validates the command syntax and semantic.
- Writes a copy of the commands and error messages to the Report Output Data Set.
- Reads the existing profiles and verifies their consistency.
- Carries out the commands to:
  - Add new profiles
  - Update existing profiles
  - Delete profiles
  - List profile information on the list output data set.
Running the Batch Load and Reporting Utility

To run Batch Load in the MVS/ESA environment, use the Job Control Language (JCL) statements that are described in the following text. A sample job stream is shown in Figure 34. To identify the JCL statements, the numbers used in the following JCL description are the same as those used in the figure.

1. JOB statement. This statement has no special meaning as far as Batch Load is concerned. Any job name that is adequate for the installation is permitted.

2. EXEC statement. The provided program name EMSBXPMC of Batch Load must be specified.

3. PARM parameter of the EXEC statement. The Batch Load execution options are defined in the PARM parameter. This is a set of general parameters that control the execution of the program.

4. The STEPLIB DD statement specifies the load library containing the Batch Load modules. If using the supplied exits for Batch Load, this library must be APF authorized.

5. The data set that contains the NetView Access Services system profile.

6. The data set that contains the NetView Access Services Group applications profile.

7. The data set that contains the NetView Access Services user profile.

8. The data set that contains the NetView Access Services BIND user data.

9. The data set that contains the NetView Access Services group profile.
The data set that contains the NetView Access Services Automatic logon data. This data set is used only by Batch Load for the consistency check and the downward delete.

The data set that contains the NetView Access Services group access list.

The data set for the listing of messages is the SYSPRINT data set. The attributes of the SYSPRINT data set defined in the system are:

- LRECL=133
- RECFM=FBA

A block size (BLKSIZE) of 133 is used if no other block size, or a block size that is not a multiple of 133, is given.

The report data set for the commands and error messages is the EMSBREPO data set.

The attributes of the EMSBREPO data set are the same as for the SYSPRINT data set.

The output data set for the list function is the EMSBLIST data set.

The attributes of the EMSBLIST data set are the same as for the SYSPRINT data set.

The job stream must end with a SYSUDUMP DD statement to allow for a dump to be taken when error conditions exist.

Command statements for Batch Load are provided in the command input data set.

The sample job as shown in Figure 34 can be found in member EMSBLOAD in the ems.v2r1m1.CUSTJOBS data set.
//EMSBLOAD JOB (account_no),'startup_jcl',
//   CLASS=a,MSGLEVEL=(1,1),MSGCLASS=x,
//   USER=user_id,NOTIFY=userid
/**
  ***********************************************************/
/**
  MODULE-NAME: EMSBLOAD
/**
  DESCRIPTIVE NAME: NVAS BASE Product Customization Job
/**
  COPYRIGHT: 5695-036 (C) COPYRIGHT IBM CORP. 1997
/**
  LICENSED MATERIALS - PROPERTY OF IBM
/**
  SEE COPYRIGHT INSTRUCTIONS, G120 - 2083
/**
  STATUS: NVAS/MVS Version 2, Release 1.1
/**
  FUNCTION: Performs the NVAS Batch Load and Reporting Utility
/**
  NOTES:
/**
  THIS FILE IS TAILORED AT NVAS CUSTOMIZATION TIME.
/**
  MODULE-TYPE: Customization JCL
/**
  CHANGE ACTIVITY:
/**
  ***********************************************************/
/**
  BATCHLO EXEC PGM=EMSBXPMC,REGION=2M,
  PARM='EXEC,UID=PUBUSER,UNLOCK'
/**
  NVAS load module library...:
/**
  STEPLIB DD DSN=ems.v2r1m1.SEMLMD,DISP=SHR
/**
  NVAS VSAM clusters...:
/**
  EMSBSRTS DD DSN=ems.v2r1m1.EMSSRTS,DISP=SHR
  EMSBSRTG DD DSN=ems.v2r1m1.EMSSRTG,DISP=SHR
  EMSBSRTU DD DSN=ems.v2r1m1.EMSSRTU,DISP=SHR
  EMSBPLDT DD DSN=ems.v2r1m1.EMSPLDT,DISP=SHR
  EMSBGRPF DD DSN=ems.v2r1m1.EMSGPRF,DISP=SHR
  EMSBALLT DD DSN=ems.v2r1m1.EMSALLT,DISP=SHR
  EMSBGAL DD DSN=ems.v2r1m1.EMSGAL,DISP=SHR
/**
  PRINT output data sets...:
/**
  SYSPRINT DD SYSOUT=/c5197,DCB=(LRECL=133,RECFM=FBA)
  EMSBRPO DD SYSOUT=*/,DCB=(LRECL=133,RECFM=FBA)
  EMSBLIST DD SYSOUT=*/,DCB=(LRECL=133,RECFM=FBA)
  SYSUDUMP DD SYSOUT=*/
/**
  Sample Command Input for NVAS Batch Load program...:
/**
  EMSBCOMM DD DSN=ems.v2r1m1.CUSTJOBS(EMSBLINP),DISP=SHR
/**

Figure 34. Sample Job Control Statements
Input Parameter Data Set

Before running Batch Load in the MVS/ESA environment, you must define the command input data set. A sample command input stream can be found in member EMSBLINP in the ems.v2r1m1.CUSTJOBS data set.

Starting Batch Load

To start Batch Load in MVS/ESA, a set of job control language (JCL) statements must be read into the MVS/ESA input stream. Figure 34 on page 108 shows an example of this.

After successful completion the Batch Load terminates with a return code of zero.

Batch Load Return Codes

Batch Load returns a code in register 15 to indicate the results of program execution. The return codes and their meanings are as follows:

00    Successful completion.
12    Error in input command file detected. Verify the output listing. Correct the error according to the information given in the associated messages. Correct the error and run the job again.
20    A severe error has been detected. Investigate the system console and the job output for the cause of the error. Perform the appropriate actions as suggested in the message descriptions. Correct the error and run the job again.

Batch Load Restrictions

When using the Batch Load you must consider the following:

- Batch Load does not provide functions to maintain the automatic logon data set EMSALLT. However, entries can be deleted as part of the downward delete processing.
- The Batch Load downward delete function deletes all lower-level profile records related to the deleted profile record. If, for example, a system application is deleted, all definitions for this application on group and user level including automatic logon records are deleted.
- You can run Batch Load concurrently with NetView Access Services on the same profiles. However, never run Batch Load and NetView Access Services concurrently unless you have prepared the system to share VSAM data sets. The results on your VSAM data sets are unpredictable. Refer to NetView Access Services Version 2 Customization for information on sharing VSAM data sets. While Batch Load is running, VSAM access is suppressed for NetView Access Services and no administration work is possible. However, users can continue working with their applications.
- To activate profile changes performed by the Batch Load while NetView Access Services is running, the system administrator must invoke the refresh function using Option 11, Refresh Profiles from VSAM Data Sets.
- You must be aware that Batch Load is profile-oriented unlike NetView Access Services administration, which is panel-oriented. This means that a group
Batch Load Options

The Batch Load options define a set of general parameters needed to control a certain Batch Load execution. The Batch Load options are specified in the PARM parameter of the JCL statement.

For the Batch Load options you can use either the explicit long form or the short form. The short form appears in the following enclosed in parentheses (…).

The options are:

**VERIFY (VERI)**

The Batch Load commands are verified, all errors are reported, but no execution of the commands takes place.

**EXECUTE (EXEC)**

Each Batch Load command is verified. If the command contains an error, then the error is reported and the next command is processed. Each correct command is immediately carried out.

If the option is not specified, then the default is EXECUTE.

**CONDITIONAL (COND)**

The Batch Load commands are verified in a first step and the errors are reported. If all the commands in the command input data set are correct, then the execution of all the commands takes place in a second step.

The only errors that may appear during the execution step are errors detected by the execution of the administration exit routine EMSEADEX.

**Note:** Only one of the previous three parameters can be used at one time.

**UID=**

Mandatory option specifying the user ID of an administrator already defined in the NetView Access Services database. If the NetView Access Services database is empty, then Batch Load accepts any name.

The user ID is inserted in the “last update information” field of each added or updated profile record.

**MAXLINE=**

Specifies the maximum number of lines listed on a page in the report output data set and in the list output data set. Header lines are included in this number.

The value of the number must be between 24 and 99. If this option is not specified, then the default number of lines per page is 60.

**SHORT**

Specifies that all LIST commands should select their short list format.

The SHORT list format contains only a subset of information for each profile.

**LIST=REPORT**

Specifies that the list output data set should be the same as the reporting output data set.
UNLOCK
Specifies that the Batch Load proceeds even if the NetView Access Services database is locked. Batch Load ignores a possible lock of the database and also suppresses its own locking activities. The option can be used if a Batch Load job is to perform only read operations on the database, for example, Batch Load LIST commands.

NOSRTU
Specifies that the installation only provides for external groups. Access parameters for user profiles are held on external media (for example RACF). You do not have to define data set EMSBSRTU, and the DD statement for this data set can be omitted from the Batch Load startup JCL.

Command Statements

The Batch Load command specifies:

- The action to be carried out
  - Add a new record to the data set
  - Update an existing record in the data set
  - Delete a record from the data set
  - Replace a record of a data set with a new record with changed characteristics
  - List profile information.
- The data set on which the action is to be carried out
  - Application profiles data set
  - Group profiles data set
  - Application routing data set
  - User profiles data set
  - Administrator authorization data set
  - BIND user data set.
- Parameters
  Defining the profile on which the command must be carried out and the values that are to be inserted or updated in the respective profile data sets.

Reading the Syntax Diagram

Read the diagram from left to right, top to bottom, adding elements as you go.

Each diagram begins with a double right arrow and ends with a right and left arrow pair. Lines ending with a single right arrow indicate that the syntax diagram continues. Lines beginning with single right arrows are continuation lines. In these diagrams, all spaces and other characters are significant.

Required items appear on the main path.

\[ KEYWORD \rightarrow \text{required item} \]
Optional items appear below the main path.

\[
\text{\texttt{\textasciitilde\textasciitilde KEYWORD\textasciitilde\textasciitilde}}\quad \text{\texttt{[optional_item]}}\quad \text{\texttt{\textasciitilde\textasciitilde}}
\]

Variable values that you provide are shown in lowercase.

\[
\text{\texttt{\textasciitilde\textasciitilde variable_value\textasciitilde\textasciitilde}}
\]

If you can choose from two or more items, they appear vertically in a stack.

\[
\text{\texttt{\textasciitilde\textasciitilde KEYWORD\textasciitilde\textasciitilde}}\quad \text{\texttt{[required_choice1\textasciitilde\textasciitilde required_choice2\textasciitilde\textasciitilde required_choice3\textasciitilde\textasciitilde]}}
\]

If choosing one of the items is optional, the entire stack appears below the main path.

\[
\text{\texttt{\textasciitilde\textasciitilde KEYWORD\textasciitilde\textasciitilde}}\quad \text{\texttt{[optional_choice1\textasciitilde\textasciitilde optional_choice2\textasciitilde\textasciitilde]}}
\]

If one of the optional items is the default (that is, if you do not code anything, the default is used), it is shown above the main path.

\[
\text{\texttt{\textasciitilde\textasciitilde KEYWORD\textasciitilde\textasciitilde}}\quad \text{\texttt{[default_choice\textasciitilde\textasciitilde optional_choice1\textasciitilde\textasciitilde optional_choice2\textasciitilde\textasciitilde]}}
\]

A repeatable operand is shown like so:

\[
\text{\texttt{\textasciitilde\textasciitilde KEYWORD\textasciitilde\textasciitilde}}\quad \text{\texttt{[\texttt{variable_value}]}}
\]

Syntax diagrams may be broken into fragments. A fragment is indicated by vertical bars with the name of the fragment between the bars. The fragment is shown following the main diagram, like so:

\[
\text{\texttt{\textasciitilde\textasciitilde \texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde A Fragment\textasciitilde\textasciitilde}}\quad \text{\texttt{\textasciitilde\textasciitilde}}
\]

\[
\text{\texttt{\textasciitilde\textasciitilde \texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde \texttt{A Fragment:}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}
\]

\[
\text{\texttt{\textasciitilde\textasciitilde \texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde \text{\texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}}\quad \text{\texttt{\textasciitilde\textasciitilde}}
\]

The general format of all Batch Load commands is:
Syntax of Batch Load Commands

- command—data set, parameter=value,...—comment

Figure 35. General Format of Batch Load Commands

Command
Specifies the name of the action to be carried out. Short forms are accepted and are specified in the following list in parentheses (...). Lowercase letters are accepted in the command name.

**ADD**
Adds a new record to the data set.

**UPDATE (UPD)**
Updates an existing record in the data set.

**DELETE (DEL)**
Deletes a record from the data set.

**REPLACE (REP)**
Deletes a certain record from the data set (if it exists), and adds a new record to the data set.

**LIST (LIS)**
Lists information from the profile data set.

Data set
Positional parameter specifying the name of the data set. Lowercase letters are accepted in the data set specification.

**SYSTEM_APPLICATION**
Application profiles data set EMSSRTS.

**GROUP**
Group profiles data set EMSGPRF.

**GROUP_APPLICATION**
Application routing data set EMSSRTG.

**USER**
User profiles data set EMSSRTU.

**ADMINISTRATOR**
Administrator authorization data set EMSGAL.

**BIND_USER_DATA**
BIND user data set EMSPLDT.

Parameter
Specifies the parameter keyword. Lowercase letters are accepted in the parameter keyword.
Value
Specifies the value of the keyword parameter. This can be:

- An empty string.
- An asterisk (*) character with the meaning of “all”.
- A keyword.

Some of the keyword values can be specified in a short form.
In the following command description such short forms are specified in parenthesis (...). Lowercase letters are accepted in the keyword.

- A name consisting of maximal eight alphanumeric characters; the first character being a letter. The characters at sign (@), number sign (#), and dollar sign ($) are accepted to extend the letter character set.
  Lowercase letters are accepted in the name and are converted to uppercase.
- Decimal number consisting of a string of digits.
- String of up to eight characters that must not contain blanks and commas.
  Lowercase letters are accepted in the string but are not converted to uppercase.
- Text enclosed in quotes.
  Lowercase letters are accepted in the string but are not converted to uppercase.
- A function key PF01 through PF24, PA01 through PA03, or ENTER.
  The number of the PF or PA key can be specified with one or two digits (PF3 or PF03).
  Lowercase letters are accepted in the function key.

Comment
Optional user comment.

Rules for Writing Batch Load Commands
The following describes the rules for writing Batch Load commands:

- The commands may be specified in any order if you take the following restriction into consideration.
  If you add new profiles to the data sets and you make a reference to another profile, this profile must either be already defined in the respective profile data set, or its definition must precede, in the current input command file, the command that makes the reference to its name.
- Each command begins with the command name and may begin in any column.
- Any number of blanks may follow the command name before the positional parameter specifying the name of the data set.
- The positional parameter specifying the name of the data set must appear on the same line as the command name.
- Each line different from a comment line must contain at least one parameter specification.
- Blank lines are not accepted in the command input data set.
• No blanks may be included in the parameter value, except in parameter values
  specified as quoted texts.

• The quoted text parameter value begins and ends with a quote character that is
  ignored before inserting the text into the respective profile data set. You may
  insert quotes inside of the specified text, writing two quote characters for each
  intended quote.

• A parameter value followed by a blank indicates the end of the command.

• The parameters of a statement are separated by commas. Except for the last
  parameter, a comma must immediately follow the parameter value.

• A comma followed by a blank signals the end of the line, and that another
  parameter is expected on the next line that is not a comment line.

• A parameter may not span more than one line. This means that a parameter
  keyword and the associated parameter value must be written on the same line.

• The keyword parameters of the statements may be written in any order after
  the positional parameter specifying the name of the profile data set.

If a quoted text parameter value does not fit into the command input line, the
quoted text cannot be interrupted and continued on the next command input
line. In this case the command syntax provides a set of consecutive param-
ters like BIND_1, BIND_2, ..., BIND_5, each defining a substring of the
intended quoted text. Such parameters must appear in this order. That means
that if BIND_3 is specified, it must be preceded in the command by BIND_1
and BIND_2, in that order.

The order of the parameters EXIT_1 and EXIT_2 is restricted by the same rule.
If EXIT_2 is specified, then it must be preceded in the command by EXIT_1.

In accordance with the conventions of sample exit EMSEADEX, the format of
the concatenated substrings of EXIT_1 and EXIT_2 for user and administrator
oriented commands is:

USER NAME | INSTALLATION DATA

The split vertical bar (X‘6A’) is used to separate two values, which are
assigned to the PGMRNAME and INSTDATA fields of the RACF user profiles.
These are synonymous with the NAME and DATA parameters of the TSO
ADDUSER command. The NAME field can consist of up to 20 characters.

The format of the concatenated substrings of EXIT_1 and EXIT_2 for group
oriented commands is:

INSTALLATION DATA

The value of the concatenated substring is assigned to the INSTDATA field of
the RACF group profile. This is synonymous with the DATA parameter of the
TSO ADDGROUP command.

The total length of EXIT_1 and EXIT_2 must not exceed 60 characters,
including the separator symbol.

• Comment lines may be specified by coding an asterisk (*) in column 1. A
  remark may also be written in a line following a parameter and at least one
  blank.

• Every parameter can be specified only once. An error results if the same
  parameter is repeated in the same statement.
• Lowercase letters are accepted in all command components. For "name" parameter values, lowercase letters are converted to uppercase before being inserted into the NetView Access Services database.

**Commands for the System Application Profile Data Set EMSSRTS**

The format of the command is:

```
EMSSRTS
  ADD SYSTEM_APPLICATION=,SYSTEM_INTERNAL_NAME=name
  UPDATE(UPD) AUTOMATIC_LOGON=keyword
  DELETE(DEL)
  REPLACE(REP)
  LIST(LIS)
  PRIMARY_LU_NAME=name AUTOMATIC_LOGON=keyword
  TPN_OF_ASR=name ACB_TYPE=keyword ACCESS_TYPE=keyword
  ALTERNATE_SEQUENCES=number IDLE_TIME_VALUE=number
  PSEUDO_TERMINAL_PREFIX=name MAXIMUM_SESSIONS=number
  SHAREABLE=keyword APPLSTAT_TIME_VALUE=time_value
  BACKUP_APPLICATION_NAME=name
```

**Figure 36. Commands for System Application Profile Data Set EMSSRTS**

**Command**

Specifies the action to be carried out:

**ADD**

Adds a new system application.

**UPDATE (UPD)**

Updates the characteristics of an existing system application.

**DELETE (DEL)**

Deletes a system application.

This command must be specified only with the keyword parameter SYSTEM_INTERNAL_NAME. If you specify any of the other keyword parameters, the command is rejected with an error message.

**REPLACE (REP)**

Deletes the system application (if it exists), and adds the system application again to the profile data set with changed characteristics.

**LIST (LIS)**

Lists information about the system application.

This command must be specified only with the keyword parameter SYSTEM_INTERNAL_NAME. If you specify any of the other keyword parameters, the command is rejected with an error message.

For the listing you can select:

- A particular system application
• All system applications.

Command variables
Specify the parameters to be added, updated, deleted, replaced, or listed:

SYSTEM_APPLICATION
Is a positional parameter specifying that the object of the command is the application profiles data set.

SYSTEM_INTERNAL_NAME=name
Specifies the system-wide nickname for each subsystem, transaction, or application. An asterisk (*), instead of the name, can be used in a LIST command to select all system applications for the listing.

PRIMARY_LU_NAME=name
Specifies the VTAM ACB name of the application in the host or in another system. The parameter is mandatory for ADD and REPLACE commands. The parameter is not allowed if ACB_TYPE=NO is specified.

AUTOMATIC_LOGON=keyword
Specifies whether:

YES (Y) Automatic logon to that system is allowed.

NO (N) Automatic logon is not allowed.

If the parameter is not specified in the ADD command, the default is YES.

TPN_OF_ASR=name
Specifies the transaction program name for an ASR. This parameter is required in ADD and REPLACE commands if ACB_TYPE=NO is specified. Otherwise it is not allowed.

ACB_TYPE=keyword
Specifies whether:

UNIQUE (U) A unique ACB is used

SHARED (S) A shared ACB is used

INDIVIDUAL (I) An individual ACB is used

NO ACB (N) No ACB is used for an ASR-ASR session.

The parameter is mandatory in ADD and REPLACE commands.

ACCESS_TYPE=keyword
Specifies the mode in which the application can be accessed:

RELAY (R) Relay mode

PASS (P) Pass mode

BOTH (B) Relay or pass mode.

If the parameter is not specified in the ADD command, the default is RELAY. ACCESS_TYPE=RELAY is required if ACB_TYPE=No is specified.

ALTERNATE_SEQUENCES=number
Specifies the maximum number of alternate automatic logon records for each user who has access to that application. The number must be between 0 and 10.

If the parameter is not specified in the ADD command, the default is 5.
**IDLE_TIME_VALUE**=number

To help protect against unauthorized access to a terminal that is not in use, NetView Access Services can disconnect relay-mode sessions for which there is no user activity after a predefined period has elapsed. You can specify any integer between 0 and 999 minutes.

For example, if you specify a value of 20, the session is disconnected after 20 minutes, if no data is sent from an application to NetView Access Services during this time period.

The default is 60. A value of zero means that NetView Access Services will not disconnect the session, and inactivity with this application is allowed indefinitely. This is not used for pass-mode applications.

The idle-time value specified has nothing to do with the idle-time values for the NetView Access Services physical terminal sessions, which are set during installation in the startup parameters.

**PSEUDO_TERMINAL_PREFIX**=name

Specifies the prefix for the pseudo terminal names used to access the application in relay mode.

The name can contain one or more asterisks (*) to specify a generic pseudo terminal prefix. Generic pseudo terminal prefixes must have a length of 8 bytes.

This parameter is mandatory for ADD and REPLACE commands when the ACCESS_TYPE is not PASS.

The parameter is not allowed if ACB_TYPE=NO is specified.

**MAXIMUM_SESSIONS**=number

Specifies the maximum number of sessions for the application. The number must be between 0 and 65534. If the parameter is not specified in the ADD command, the default is 99.

You can specify any number between 0 and 65534 if ACB_TYPE=SHARED is specified. If you specify ACB_TYPE=UNIQUE or ACB_TYPE=INDIVIDUAL, the maximum number of sessions is limited by the possible size of the pool.

For example: For PSEUDO_TERMINAL_PREFIX=IMSAB, the number of maximum sessions can be any number between 1 and 999.

**SHAREABLE**=keyword

Specifies whether this application can be shared by two users or not:

YES (Y) This application can be shared.

NO (N) This application cannot be shared. Definitions made at the lower level are ignored. N is the default.

**APPLSTAT_TIME_VALUE**=time_value

Specifies the time interval between invocations of the process used to determine the status of an application.

This must be a numeric string of 1 to 4 characters. Values between 0 and 1440 minutes can be specified. A value of 0 must be specified for ACB_TYPE=NO. 0 is the default.

**BACKUP_APPLICATION_NAME**=name

Specifies the system-internal name of the backup application. It can consist of up to 8 alphanumeric characters including &-, #, and $. However, the first char-
acter must not be a digit. It can be specified for both pass mode or relay mode applications, but cannot be specified for applications with ACB_TYPE=NO.

Commands for the Group Profile Data Set EMSGPRF

The format of the command is:

```
EMSGPRF

<table>
<thead>
<tr>
<th>Command</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD</td>
<td>Adds a new group. You can customize the sample exit EMSEADEX provided by NetView Access Services so that it rejects the definition of external group profiles when, for instance, these profiles are defined directly using RACF TSO commands. In this situation, the ADD command only completes successfully when the corresponding group profile is already defined.</td>
</tr>
<tr>
<td>UPDATE (UPD)</td>
<td>Updates the characteristics of an existing group. The GROUP_TYPE cannot be changed because databases are used to store the group profile information.</td>
</tr>
<tr>
<td>DELETE (DEL)</td>
<td>Deletes a group. This command must be specified only with the keyword parameter GROUP_NAME. If you specify any of the other keyword parameters, the command is rejected with an error message. The sample administration exit EMSEADEX provided by NetView Access Services rejects deletion of external groups to which user profiles are still connected. Therefore, you must delete all user profiles connected to the external group before deleting the group profile.</td>
</tr>
</tbody>
</table>
```

Figure 37. Commands for Group Profile Data Set EMSGPRF
You can customize the sample exit EMSEADEX so that it rejects the definition of external group profiles when, for instance, these profiles are defined directly using RACF TSO commands. In this situation, the DELETE command only completes successfully when the corresponding group profile is already defined.

If the external group was defined by another administrator, the sample exit EMSEADEX returns error code X'34'. Batch Load issues an error message, but the delete completes successfully.

**REPLACE (REP)**
If the group profile is already defined, the REPLACE command performs an update of the corresponding group profile with all the specified parameters. Parameters not specified take the default values. The group type cannot be changed.

If the group profile is not already defined, then the REPLACE command functions as an add operation.

You can customize the sample exit EMSEADEX so that it rejects the definition of external group profiles when, for instance, these profiles are defined directly using RACF TSO commands. In this situation, the REPLACE command only completes successfully when the corresponding group profile is already defined.

**LIST (LIS)**
Lists information about the group.

This command must be specified only with the keyword parameter GROUP_NAME. If you specify any of the other keyword parameters, the command is rejected with an error message.

For the listing, you can select:

- A particular group
- All groups.

**Command variables**
Specify the parameters to be added, updated, deleted, replaced, or listed:

**GROUP**
Is a positional operand specifying that the object of the command is the group profiles data set.

**GROUP_NAME=**name
Specifies the name of the group.

An asterisk (*), instead of the name, can be used in a LIST command to select all groups for the listing.

**GROUP_TYPE=**keyword
Specifies whether the group is:

- NORMAL (N) A normal group
- PUBLIC (P) A public group
- EXTERNAL (E) An external group.

If the parameter is not specified in the ADD or REP command, the default is NORMAL.
You cannot change the group type for update or replace operations. Normal groups are not allowed if you specify the NOSRTU option.

**ACCOUNT_NUMBER**
Specifies the account number that can be used by your installation to charge for all activities of the group.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

**NUMBER_OF_SESSIONS**=number
Specifies the number of relay application sessions that each user can use simultaneously.

The number must be between 1 and 99.

If the parameter is not specified in the ADD command, the default is 10.

**MULTI_TERMINAL**=keyword
Specifies whether:

- **YES (Y)** Each user assigned to use applications in the group can log on to more than one terminal at a time.
- **NO (N)** Each user assigned to use applications in the group can log on to only one terminal at a time.
- **S** Secure terminal. Each user assigned to use applications in the group can log on at another terminal, but the complete terminal session is taken over and the NetView Access Services Logon panel is displayed on the original terminal.

If the parameter is not specified in the ADD command, the default is NO.

**ESCAPE_KEY**=function_key
Specifies the PF or PA function key, or the ATTN key assigned as the Escape key. All users assigned to use applications in the group use this key to escape from any relay mode application.

If the parameter is not specified in the ADD command, the default is PA02. If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

**COMMAND_KEY**=function_key
Specifies the PF key or ENTER key used after the user has typed a NetView Access Services command in a panel of the application.

If the parameter is not specified in the ADD command, the default is PF10.

**COPYFROM_BEGIN**=function_key
Specifies the PF key assigned to start the copy-from area.

If the parameter is not specified in the ADD command, the default is PF02.

**COPYFROM_END**=function_key
Specifies the PF function key assigned to end the copy-from area.

If the parameter is not specified in the ADD command, the default is PF02.

**COPYTO**=function_key
Specifies the PF function key assigned to start the copy-to area.

If the parameter is not specified in the ADD command, the default is PF02.
COMMAND_PREFIX=text
   Specifies the prefix that the users of this group must type before a NetView Access Services command from one of the panels of a relayed application.
   
   If the parameter is not specified in the ADD command, then $$ is the default.
   
   The prefix cannot be longer than 8 characters. Blanks are not allowed in the prefix.

PRINTER=string
   Specifies the default printer name. One of the following can be specified:
   
   • A printer LU name. This can be a string of 1 to 8 characters.
   • SYSTEMPR (system printer).

ASP_FORMAT=keyword
   Specifies the Application Selection panel format:
   
   Normal (N)   The standard NetView Access Services panel format
   Compact (C)  The format used allows up to 42 applications to be displayed on a single page. The previous limit of a maximum of 99 applications has been removed.

   If the parameter is not specified in the ADD command, the default is Normal.

SHARED_SESSION_RESPONSE=keyword
   Specifies authorization to accept a request to share a session:
   
   Systemwide (S)   The users assigned to use applications in the defined group are authorized to accept a request to share a session with all other users of the NetView Access Services system.
   
   Groupwide (G)    The users assigned to use applications in the defined group are authorized to accept a request to share a session with all other users assigned to use applications in that group.
   
   None (N)         The users assigned to use applications in the defined group are not authorized to accept a request to share a session. This is the default.

EXIT_1 and EXIT_2=text
   The two text strings specified in these parameters are concatenated, representing the user data character string to be conveyed to the administration exit routine EMSEADEX.
   
   The parameters must not be specified for groups other than external.
   
   The whole concatenated string must not contain more than 60 characters. Refer to “Rules for Writing Batch Load Commands” on page 114 for further information on these parameters.

PRINT_KEY=function_key
   Specifies the PF or PA key assigned as the Print key.
   
   The default is PF24, if no value is specified in the ADD command.
   
   If you want to delete the value for this parameter in the profile, you can specify an empty string in the UPDATE command.
LOGON_REXX_EXEC=name
Specifies the name of the REXX exec to be executed when a user logs on to the specified group. The name must be the same as the name of the member in which the REXX instructions are located.

If you want to delete the value for this parameter in the profile, you can specify an empty string in the UPDATE command.

LOGOFF_REXX_EXEC=name
Specifies the name of the REXX exec to be executed when a user enters the LOGOFF, EXIT, or DISC command within the specified group, and when the time-out value for the terminal session is reached. The name must be the same as the name of the member in which the REXX instructions are located.

If you want to delete the value specified for this parameter, you can specify an empty string in the UPDATE command.

Commands for the Group Application Profile Data Set EMSSRTG
The format of the command is:

```
EMSSRTG
```

- **ADD**
  - GROUP_APPLICATION, GROUP_NAME=name

- **UPDATE(UPD)**
  - GROUP_NAME=name

- **DELETE(DEL)**
  - GROUP_NAME=name

- **REPLACE(REP)**
  - GROUP_NAME=name

- **LIST(LIS)**
  - GROUP_NAME=name

```
```

```
```

Figure 38. Commands for Group Application Data Set EMSSRTG

Command
Specifies the action to be performed:

**ADD**
- Adds a new application to the group.
UPDATE (UPD)
Updates the characteristics of an existing application in the group.

DELETE (DEL)
Deletes an application from the group.

This command must be specified only with the keyword parameters
GROUP_NAME and APPLICATION. If you specify any of the other keyword
parameters, the command is rejected with an error message.

REPLACE (REP)
Deletes an application (if it exists) from the group, and adds the application
again to the group with changed characteristics.

LIST (LIS)
Lists information about the applications in this group.

This command must be specified only with the keyword parameter
GROUP_NAME and APPLICATION, and optionally with
SYSTEM_INTERNAL_NAME.

One of the keyword parameters APPLICATION and
SYSTEM_INTERNAL_NAME must be specified, but not both.

If you specify any of the other keyword parameters, the command is rejected
with an error message.

For the listing, you can select:
- A particular application or all applications
- A particular group or all groups
- A particular system internal name or all system internal names
- Any combination of these criteria.

Command Variables
Specify the parameters to be added, updated, deleted, replaced, or listed:

GROUP_APPLICATION
Is a positional operand specifying that the object of the command is the appli-
cation routing data set.

GROUP_NAME=name
Specifies the name of the group.

An asterisk (*) instead of the name may be used in a LIST command to select
all groups for the listing.

APPLICATION=name
Specifies the group-wide name of the application.

To specify a free selection application for the user assigned to use applications
in the group, the name must consist of eight point characters.

An asterisk (*), instead of the name, can be used in a LIST command to select
all applications for the listing.

SYSTEM_INTERNAL_NAME=name
Specifies the system-wide name of the application.

An asterisk (*) instead of the name may be used in a LIST command to select
all system applications for the listing.
This parameter is mandatory for ADD and REPLACE commands when the application is not the free selection application. For the free selection application this parameter is not allowed.

**ACCESS_TYPE=keyword**
Specifies the mode in which the application can be accessed:

- **RELAY (R)** Relay mode
- **PASS (P)** Pass mode
- **BOTH (B)** Relay or pass mode.

When the parameter is not specified for the ADD or REPLACE commands, then the value defaults to the value found in the corresponding system application profile.

**LOGON_PROFILE=keyword**
Specifies whether:

- **GROUP (G)** The default logon profile for this application is the group-wide logon profile.
- **SYSTEM (S)** The default logon profile for this application is the system-wide logon profile.

If the parameter is not specified in the ADD command, the default is GROUP.

**AUTOMATIC_LOGON=keyword**
Specifies whether:

- **YES (Y)** Automatic logon to that system is allowed.
- **NO (N)** Automatic logon is not allowed.

If the parameter is not specified in the ADD command, the default is YES.

**JUMP_KEY=function_key**
Specifies the PF or PA function key, or the ATTN key used by the users assigned to use applications in the group to jump to this application from others.

If the parameter is not specified in the ADD command, the default is PA02.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the update command.

**SELECTION_ID=number**
Specifies the sequence number at which position this application appears on the Application Selection panel.

The number must be between 0 and 99, or empty.

For the free selection application, the number is ignored and is always set to zero by Batch Load.

Empty means that the parameter is specified, but with no value. In this case a space is loaded into the profile database for this parameter and causes the application to be displayed at the bottom of the list.

**APPLICATION_DESCRIPTION=text**
Specifies up to 30 characters of text enclosed in quotes describing the application. This description appears on the Application Selection panel, next to the application name.
MSG_RECEIVED_INDIC=keyword
Specifies how messages are to be received:

NORMAL (N)  Normal message received indication.
JUMP (J)    Jump message received indication.
INFORMATION (I)
            Information message received indication.

If the parameter is not specified for the ADD command, the default is NORMAL.

DATA_COMPRESSION=keyword
Specifies whether NetView Access Services is to compress data before sending it.

YES (Y)    Outbound-only data compression required.
NO (N)     No data compression required.
F          Full. Outbound and inbound data compression. Option Y must be specified for Virtual Terminal, if outbound and inbound data compression is required.

If the parameter is not specified in the ADD command, the default is NO.

Note: Do not specify full compression if DBCS (Double Byte Character Set) is to be used. Unpredictable results can be expected.

SHAREABLE=keyword
Specifies whether this application can be shared by the users assigned to use this application in the group or not.

YES (Y)    Users assigned to use this application in this group can share this application.
NO (N)     Users assigned to use this application in this group cannot share this application. Definitions made at the lowest level are ignored. This is the default.

APPLICATION_ID_DISPLAY=keyword
Specifies whether an application identifier can be displayed on an application panel or is to be suppressed:

YES (Y)    The application identifier can be displayed for this application.
NO (N)     The application identifier is to be suppressed for this application. The default is NO.

It is recommended to suppress displaying of the application identifier, unless Virtual Terminal option Y is specified for the application. Unpredictable results can be expected if the identifier is displayed when Virtual Terminal option N is specified for the application.

ROW=number
Specifies the row in which the application identifier is to be displayed on an application panel. This can be a value in the range of -43 to 43 (with the exception of zero). A positive value specifies a row counting from the top of the physical screen. A negative value specifies a row counting from the bottom of the physical screen.

The default is row 1.
COLUMN=number
   Specifies the column in which the application identifier is to be displayed on an application panel. This can be a value within the range of -132 to 132 (with the exception of zero). A positive value specifies the starting position of the identifier text. A negative value specifies the ending position of the identifier text.
   The default is column -1 (right-most position).

COLOR=keyword
   Specifies the color in which the text of the application identifier is displayed. Valid colors are:
   R Red
   B Blue
   T Turquoise
   G Green
   Y Yellow
   W White
   P Pink.
   The default is blank, which specifies the system default.
   The color refers to the foreground color.
   Note: If the terminal on which the application identifier is to be displayed does not support extended color attributes, the identifier is displayed in the terminal default color.

HIGHLIGHT=keyword
   Specifies the type of highlight in which the application identifier is to be displayed. Valid values are:
   H Highlighted
   R Reverse video
   U Underscored
   B Blinking.
   The default is H.
   Note: If the terminal on which the application identifier is to be displayed does not support extended field attributes, the identifier is displayed highlighted.

TEXT=text
   Specifies the text of the identifier. The text can be up to 30 characters enclosed in quotes, and no underscores can be used. If no text is specified, the application description on the Application Selection panel is the default.

LOGON_REXX_EXEC=name
   Specifies the name of the REXX exec to be executed when a user logs on to the specified application within the group specified. The name must be the same as the name of the member in which the REXX instructions are located.
   If you want to delete the value specified for this parameter, you can specify blanks for this parameter in the UPDATE command.

LOGOFF_REXX_EXEC=name
   Specifies the name of the REXX exec to be executed when a user logs off from the specified application within the group specified, or when the time-out value for the application session is reached. The name must be the same as the name of the member in which the REXX instructions are located.
If you want to delete the value specified for this parameter, you can specify blanks for this parameter in the UPDATE command.

**VIRTUAL_TERMINAL=keyword**

Specifies whether the Virtual Terminal for the specified application is to be enabled.

**YES (Y)**  
The Virtual Terminal is to be enabled for this application.

**NO (N)**  
The Virtual Terminal is not to be enabled for this application.

The default is Y. Virtual Terminal option Y is a prerequisite if Data Compression option F for outbound and inbound data compression is specified.

**LOGMODE=name**

Specifies any string that is valid as a VTAM LOGMODE. The name can be up to eight characters. If you want to delete the value specified for this parameter, you can specify blanks for this parameter in the update command.

### Commands for the User Profile Data Set EMSSRTU

The format of the command is:
**Figure 39. Commands for User Profiles Data Set EMSSRTU**

**Command**

Specifies the action to be performed:

**ADD**

Adds a certain application to a particular user of the group, adds all applications of the group to a particular user, or adds a certain application to all users of the group.

User profiles connected to external groups are stored only in the RACF database. Batch Load calls administration exit EMSEADEX only for user profiles connected to external groups. The only calls to the administration exit EMSEADEX for users in normal groups are calls to get or verify user exit data.

You can customize the sample exit EMSEADEX provided by NetView Access Services so that it rejects the definition of user profiles connected to external group profiles when, for instance, these profiles are defined directly using...
RACF TSO commands. In this situation, the ADD command only completes successfully when the corresponding user profile is already defined.

**UPDATE (UPD)**

Updates the characteristics of a certain application assigned to a particular user of the group, or updates the characteristics of a certain application for all users of the group.

**DELETE (DEL)**

Deletes a certain application from the user of the group, or deletes all the applications of the group for a particular user.

This command must be specified only with the keyword parameters USER_ID, GROUP_NAME, and APPLICATION. If you specify any of the other keyword parameters, the command is rejected with an error message.

You can customize the sample exit EMSEADEX so that it rejects the definition of user profiles connected to external groups when, for instance, these profiles are defined directly using RACF TSO commands. In this situation, the DELETE command only completes successfully when the corresponding user profile is already defined.

If the user in the external group was defined by another administrator, the sample exit EMSEADEX returns error code X'34'. Batch Load issues an error message, but the delete completes successfully.

**REPLACE (REP)**

Replaces the characteristics of a certain application for a particular user of the group, or replaces the characteristics of all applications for a particular user of the group, or replaces the characteristics of a certain application for all users of the group.

If the user profile is already defined, the REPLACE command performs an update of the corresponding user profile with all the specified parameters. Parameters not specified take the default values.

If the user profile is not already defined, then the REPLACE command functions as an add operation.

You can customize the sample exit EMSEADEX so that it rejects the definition of user profiles connected to external groups when, for instance, these profiles are defined directly using RACF TSO commands. In this situation, the REPLACE command only completes successfully when the corresponding user profile is already defined.

**LIST (LIS)**

Lists information about the user profile. This command must be specified only with the keyword parameter USER_ID, GROUP_NAME, and APPLICATION. If you specify any of the other keyword parameters, the command is rejected with an error message. For the listing, you may select:

- A particular user or all users
- A particular group or all groups
- A particular application or all applications
- Any combination of these criteria.

If you process multiple user profiles with the ADD and REPLACE commands, then not all keyword parameters are allowed, and you receive an error message.

Restrictions for the ADD and REPLACE commands are shown in Figure 40 on page 131.
**Note:** The performance can be improved during the run if you:

- Specify the user IDs in descending order in the input file
- Vary the first character of the user IDs.

---

<table>
<thead>
<tr>
<th>Keyword parameter</th>
<th>ADD / REPLACE / UPDATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All applications to a certain user of the group</td>
</tr>
<tr>
<td>USER_ID</td>
<td>M</td>
</tr>
<tr>
<td>GROUP_NAME</td>
<td>M</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>M</td>
</tr>
<tr>
<td>DEFAULT_GROUP</td>
<td>O</td>
</tr>
<tr>
<td>PSEUDO TERMINAL_NAME</td>
<td>O</td>
</tr>
<tr>
<td>ACCESS_TYPE</td>
<td>X</td>
</tr>
<tr>
<td>RECORD_AUTHORITY</td>
<td>O</td>
</tr>
<tr>
<td>TERMINAL_ASSUME</td>
<td>O</td>
</tr>
<tr>
<td>GVAR1</td>
<td>O</td>
</tr>
<tr>
<td>GVAR2</td>
<td>O</td>
</tr>
<tr>
<td>GVAR3</td>
<td>O</td>
</tr>
<tr>
<td>GVAR4</td>
<td>O</td>
</tr>
<tr>
<td>GVAR5</td>
<td>O</td>
</tr>
<tr>
<td>JUMP KEY</td>
<td>X</td>
</tr>
<tr>
<td>SELECTION_ID</td>
<td>X</td>
</tr>
<tr>
<td>DEFAULT_APPLICATION</td>
<td>X</td>
</tr>
<tr>
<td>LOGON_PROFILE</td>
<td>X</td>
</tr>
<tr>
<td>ACTIVE_PROFILE</td>
<td>X</td>
</tr>
<tr>
<td>PROFILE_1_COMMENT</td>
<td>X</td>
</tr>
<tr>
<td>PROFILE_2_COMMENT</td>
<td>X</td>
</tr>
<tr>
<td>MSG_RECEIVED_INDIC</td>
<td>O</td>
</tr>
<tr>
<td>ESCAPE_KEY</td>
<td>O</td>
</tr>
<tr>
<td>COMMAND_KEY</td>
<td>O</td>
</tr>
<tr>
<td>COMMAND_PREFIX</td>
<td>O</td>
</tr>
<tr>
<td>UID</td>
<td>0</td>
</tr>
<tr>
<td>ACCNO</td>
<td>0</td>
</tr>
<tr>
<td>UVAR_1</td>
<td>X</td>
</tr>
<tr>
<td>UVAR_2</td>
<td>X</td>
</tr>
<tr>
<td>UVAR_3</td>
<td>X</td>
</tr>
<tr>
<td>UVAR_4</td>
<td>X</td>
</tr>
<tr>
<td>PRINTER</td>
<td>X</td>
</tr>
<tr>
<td>PRINT KEY</td>
<td>O</td>
</tr>
<tr>
<td>SHAREABLE</td>
<td>X</td>
</tr>
<tr>
<td>APPLICATION_ID_DISPLAY</td>
<td>X</td>
</tr>
<tr>
<td>EXIT_1</td>
<td>0</td>
</tr>
<tr>
<td>EXIT_2</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 40. Restrictions for the ADD and REPLACE Commands**

Where:

- **M** Mandatory
- **O** Optional
- **X** Not allowed.

**Note:** The restrictions only apply for the UPDATE command when applicable.

**Command Variables**

Specify the parameters to be added, updated, deleted, replaced, or listed:

**USER**

- Is a positional operand specifying that the object of the command is the user profiles data set.

**USER_ID=** name

- Specifies the user identifier.

  An asterisk (*), instead of the name, may be used for normal groups to:
• Add an application to all users of the group.
• Update a specific application for all users of the group.
• Select all users for the LIST command.

GROUP_NAME=name
Specifications the name of the group.

An asterisk (*), instead of the name, may be used in a LIST command to select all groups for the listing.

If the group is a Public group, Batch Load rejects the ADD operation for user profiles. So the other operations REPLACE, UPDATE, DELETE, and LIST are also rejected as meaningless.

APPLICATION=name
Specifications the group-wide name of the application.

To specify a free selection application for the user of the group the name must consist of 8 point characters.

An asterisk (*) instead of the name may be used to:
• Add all applications of the group to a particular user. If an application already exists for the user, it is replaced by this operation.
• Delete all the applications of the group for a particular user.
• Select all applications for the LIST command.

DEFAULT_GROUP=keyword
Specifications whether:

YES (Y) This group is the default group of the user.
NO (N) The group is not the default group.

If the parameter is not specified in the ADD command, the default is NO.

PSEUDO TERMINAL NAME=name
When the application requires a specific logical terminal name, this parameter specifies the logical name of the terminal authorized for this application.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the update command.

ACCESS_TYPE=keyword
Specifications the mode in which the application can be accessed:

RELAY (R) Relay mode
PASS (P) Pass mode
BOTH (B) Relay or pass mode.

If this parameter is not specified in an ADD or REPLACE command, then the value of this parameter in the corresponding application routing profile is used as the default.

RECORD AUTHORITY=keyword
Specifications whether:

YES (Y) The user can record a logon profile for this application.
NO (N) The user cannot record a logon profile for this application.

If the parameter is not specified in the ADD command, the default is NO.

TERMINAL_ASSUME=keyword
Specifications whether:
YES (Y)  The user can assume a session from one terminal to another.
NO (N)   The user cannot assume a session from one terminal to another.
C        Conditional. The user cannot assume a session using the jump key.

If this parameter is not specified in the ADD or DELETE command, the value in the corresponding group application profile is used as the default.

GVAR1 through GVARS=string
Define the global variables used in logon profiles for relay mode applications or BIND user data.

If you want to delete the value of a global variable in the profile, you can specify an empty string in the UPDATE command.

JUMP_KEY=function_key
Specifies the PF or PA function key, or ATTN key used by the user to jump to this application from another.

If this parameter is not specified during an ADD or REPLACE command, then the value is taken from the corresponding application routing profile.

If you want to delete the value of the parameter in the profile, you can specify an empty string in the UPDATE command.

SELECTION_ID=number
Specifies the sequence number at which position this application appears on the Application Selection panel. The number must be between 1 and 99, or empty. Empty means that the parameter is specified, but with no value.

DEFAULT_APPLICATION=keyword
Specifies whether:

YES (Y)  This application is the default application.
NO (N)   This application is not the default application.

When the parameter is not specified in the ADD command, then the default is NO.

The value YES is not allowed for the Free Selection application.

LOGON_PROFILE=keyword
Specifies whether NetView Access Services is to use as logon or logoff profiles:

USER (U)  The user’s own recordings for this application.
GROUP (G)  The group-wide default for this application.
SYSTEM (S)  The system-wide default for this application.

If the parameter is not specified in the ADD command, the default is GROUP.

ACTIVE_PROFILE=number
Specifies the number 1 or 2 of the active profile.

If the parameter is not specified in the ADD command, the default is 1.

PROFILE_1_COMMENT=text
Specifies up to 15 characters of text enclosed in quotes describing the user’s private profile 1.
PROFILE_2_COMMENT=text
Specifies up to 15 characters of text enclosed in quotes describing the user’s private profile 2.

MSG_RECEIVED_INDIC=keyword
Specifies the mode in which selective broadcast messages are received:

NORMAL (N) Normal mode message received indication logon profile.
JUMP (J) Jump mode message received indication.
INFORMATION (I) Information mode message received indication.

If the parameter is not specified, no default is generated in the user profile.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

ESCAPE_KEY=function_key
Specifies the PF or PA function key, or the ATTN key assigned as the Escape key. The Escape key is used by the user to escape from any relay mode application.

The key specified in this parameter is valid for all applications that a user has access to, not only the application specified in the current command.

If the parameter is not specified in an ADD or REPLACE command, no default is generated in the user profile.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

COMMAND_KEY=function_key
Specifies the PF key or ENTER key used to issue a NetView Access Services command from the panel of an application.

The Command key specified in this parameter is valid for all applications a user has access to, not only the application specified in the current command.

If the parameter is not specified in an ADD or REPLACE command, no default is generated in the user profile.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

COMMAND_PREFIX=text
Specifies the prefix that a user must type before a NetView Access Services command on a panel of a relay mode application. The prefix must not be longer than 8 characters. Blanks are not allowed in the prefix. The prefix is valid for all applications that a user has access to, not only the application specified in the current command.

If a value is not specified for the parameter in an ADD or REPLACE command, no default value is generated in the user profile.

If you want to delete the value in the profile, you can specify an empty string in the UPDATE command.

UID=string
Specifies up to 8 characters for the User ID field for this application.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.
**ACCNO=string**
Specifies up to 8 characters for the account number for this application.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

**UVAR1 through UVAR4=string**
Defines the user variables used in logon profiles for relay mode applications or BIND user data.

If you want to delete the value of a user variable specified in the profile, you can specify an empty string in the UPDATE command.

**PRINTER=keyword**
Specifies the default printer name. One of the following can be specified:

- A printer LU name. This can be a string of 1 to 8 characters.
- SYSTEMPR (system printer).

**PRINT_KEY=function_key**
Specifies the PF or PA key assigned as the Print key. All users assigned to use applications in the specified group can use this key to print a panel of an application. The key specified is valid for all applications the user has access to.

If a value for the parameter is not specified in the ADD or REPLACE command, no default is generated in the user profile.

If you want to delete the value specified for the parameter in the profile, you can specify an empty string in the UPDATE command.

**SHAREABLE=keyword**
Specifies at user level whether this application can be shared or not:

- YES (Y) The specified user can share this application with other users.
- NO (N) The specified user cannot share this application with other users. This is the default.

**APPLICATION_ID_DISPLAY=keyword**
Specifies whether an application identifier is to be displayed or suppressed.

- YES (Y) The application ID can be displayed.
- NO (N) The application ID cannot be displayed.

If this parameter is not specified in an ADD or REPLACE command, the value of the parameter found in the corresponding group application profile is used as the default.

**EXIT_1 and EXIT_2=text**
The two text strings specified in these parameters are concatenated, representing the user data character string to be conveyed to the administration exit routine EMSEADEX.

The entire concatenated string must not contain more than 60 characters. Refer to “Rules for Writing Batch Load Commands” on page 114 for further information on these parameters.
Commands for the Administrator Authorization Profile Data Set EMSGAL

The format of the command is:

```
EMSGAL
  ADD ADMINISTRATOR─,USER_ID=name─ ──,GROUP_NAME=name─
  UPDATE(UPD)─ ──,EXIT_1=text─ ──,EXIT_2=text─
  DELETE(DEL)─ ──,TYPE=keyword─
  REPLACE(REP)─ ──,EXIT_1=text─ ──,EXIT_2=text─
  LIST(LIS)─ ──,TYPE=keyword─
```

Figure 41. Commands for Administrator Authorization Data Set EMSGAL

Command

Specifies the action to be performed:

ADD
  Defines a user as a system, group, or broadcast-only administrator.

UPDATE (UPD)
  Updates characteristics of an existing administrator. Only EXIT_1 and EXIT_2 data can be changed.

DELETE (DEL)
  Releases the system, group, or broadcast-only administration authorization for this user.

REPLACE (REP)
  Releases the system or group administrator authority (if existing) for this user, and redefines it. Specifying the parameter TYPE for this command is not allowed.

LIST (LIS)
  Lists information about the administrator.
  This command must be specified only with the keyword parameter USER_ID, GROUP_NAME, TYPE. If you specify any of the other keyword parameters, the command is rejected with an error message.
  For the listing, you can select:
  * A particular user or all users
  * A particular group or all groups
  * Any combination of these criteria
  * A particular broadcast administrator, or all broadcast-only administrators.

Command Variables

Specify the parameters to be added, updated, deleted, replaced, or listed:

ADMINISTRATOR
  Is a positional operand specifying that the object of the command is the administrator authorization data set.
USER_ID=name
Specifies the user identifier.

An asterisk (*), instead of the name, may be used in a LIST command to select all users for the listing.

GROUP_NAME=name
Specifies the name of the group.

If neither this parameter nor the TYPE parameter is specified, then the user gets the system administrator authorization.

If this parameter is not specified and the TYPE parameter is specified, then the user gets the broadcast-only administrator authorization.

The GROUP_NAME parameter is not allowed in combination with the TYPE parameter. An asterisk (*), instead of the name, may be used in a LIST command to select all groups for the listing.

EXIT_1 and EXIT_2=text
The two text strings specified in these parameters are concatenated, representing the user data character string to be conveyed to the administration exit routine EMSEADEX.

The whole concatenated string must not contain more than 60 characters. Refer to “Rules for Writing Batch Load Commands” on page 114, for further information on these parameters.

TYPE=keyword
Specifies the type of administrator and the scope of authorization. This is mandatory when defining an administrator.

S System administrator. This includes all administration tasks.

G Group administrator. This includes all group administration tasks for the group specified. If you want to additionally authorize a group administrator to broadcast selective broadcast messages system-wide, you must in a second step specify this user as a broadcast-only administrator by specifying B for the TYPE parameter and an empty string for the GROUP_NAME parameter.

B Broadcast-only administrator. The user whose ID is specified is authorized to broadcast selective messages system-wide.

The TYPE parameter is allowed only with ADD, DEL, and LIST commands. It is used only to add, delete, or list broadcast-only administrators.

The TYPE parameter is not allowed in combination with the GROUP_NAME parameter.

Notes:

1. Users defined as system administrators cannot simultaneously be defined as broadcast-only administrators. System administrators automatically have this authorization.

2. Users defined as broadcast-only administrators cannot be defined as system administrators.
Commands for the BIND User Data Profile Data Set EMSPLDT

The format of the command is:

```
EMSPLDT
  ADD BIND_USER_DATA, SYSTEM_INTERNAL_NAME=name
  UPDATE(UPD) BIND_USER_DATA, SYSTEM_INTERNAL_NAME=name
  DELETE(DEL) BIND_USER_DATA
  REPLACE(REP) BIND_USER_DATA
  LIST(LIS)

,BIND_1=text 
,BIND_2=text 
,BIND_3=text 
,BIND_4=text 
,BIND_5=text
```

Figure 42. Commands for BIND User Data Profiles Data Set EMSPLDT

Command
Specifications the action to be performed:

ADD
  Defines BIND user data for an application.

UPDATE (UPD)
  Updates the BIND user data for an application.

DELETE (DEL)
  Deletes the BIND user data for an application.
  This command must be specified only with the keyword parameter
  SYSTEM_INTERNAL_NAME. If you specify any of the other keyword parame-
  ters, the command is rejected with an error message.

REPLACE (REP)
  Deletes the BIND user data (if it exists) for an application, and adds it again to
  the profile data set possibly with changed content.

LIST (LIS)
  Lists information about BIND user data of a system application.
  This command must be specified only with the keyword parameter
  SYSTEM_INTERNAL_NAME.
  If you specify any of the other keyword parameters, the command is rejected
  with an error message. You may select a particular system application or all
  system applications for the listing.

Command Variables
Specify the parameters to be added, updated, deleted, replaced, or listed:

BIND_USER_DATA
  Is a positional operand specifying that the object of the command is the BIND
  user data profiles data set.

SYSTEM_INTERNAL_NAME=name
  Specifies the system-wide nickname for each subsystem, transaction, or other
  application.
  An asterisk (*), instead of the name, may be used in a LIST command to select
  all system applications for the listing.
**BIND 1 through BIND 5=text**

The text strings are concatenated to represent the BIND user data character string.

The BIND user data string that results after the concatenation of these text strings must contain no more than 255 characters. Refer to “Rules for Writing Batch Load Commands” on page 114 for further information on these parameters.

---

**LIST Output Formats**

The output of the LIST command for a certain profile record consists of one line, or a sequence of lines, where the characteristics of the profile are edited right justified on fixed-column positions. For each profile type, Batch Load provides a set of header lines showing which parameter is edited on which column. The header lines are written each time the profile type changes in the sequence of LIST commands.

Headers are written at the top of each new page. The number of lines included into a page is either 60 (default) or equal to the number specified on the MAXLINE option.

If you specify the option LIST=REPORT, then Batch Load carries out no page control.

If two LIST commands specify the same profile database, then the output of these two commands is separated in the listing by a separator line.

For certain profile types the characteristics cannot be edited on a single line. For such profiles the listing contains additional lines following the first line.

You may disable the printing of additional lines, specifying the option SHORT as the parameter for the JCL EXEC instruction.

The following shows the corresponding list output format for each profile type.

---

**SYSTEM_APPLICATION Profiles EMSSRTS**

The SHORT list has the following format:

```
System Application Profiles 28/02/94 15:55:08 Page 3
-------------------------------------------------------------------------------------------------------------------
System  Internal  Primary   Aut.   ACB   Access  Alt.   Idle  Terminal    Max.   TPN   Share
Name    Name     Log.   Type   Type   Seq.   Time   Prefix  Ses.    ASR   value
-------- -------- ---- ---- ---- ----- ---- ---- ------- ---- ---- -------
CICS1    ACBCICS1 Y U R 5 6/zerodot EMSYAC 2/zerodot Y 15 PUBUSER 28/02/94 17:51:18
CICS2    ACBCICS2 Y U R 5 6/zerodot EMSYAC 5/zerodot Y 10 PUBUSER 28/02/94 17:48:25
IMSP     ACBINS   N U R 5 6/zerodot EMSYAI 2/zerodot N 10 PUBUSER 28/02/94 17:51:57
NETVIEW  ACBNETV Y U R 5 6/zerodot EMSYAF 5/zerodot Y 10 PUBUSER 28/02/94 17:46:39
TSOP     ACBTSO  Y U R 5 6/zerodot EMSYAT 5/zerodot Y 10 PUBUSER 28/02/94 17:47:39
VM1      ACBVMI   Y U R 5 6/zerodot EMSYAT 5/zerodot Y 10 PUBUSER 28/02/94 17:47:39
VM2      ACBVM2  Y U R 5 6/zerodot EMSYAT 5/zerodot Y 10 PUBUSER 28/02/94 17:47:39
-------------------------------------------------------------------------------------------------------------------
```

Figure 43. SHORT List Format for SYSTEM_APPLICATION Profiles EMSSRTS

The LONG list format has the following format:

---

The following shows the corresponding list output format for each profile type.
System Application Profiles

**Figure 44. LONG List Format for SYSTEM_APPLICATION Profiles EMSSRTS**

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT because in this case the new page control is not activated.

**GROUP Profiles EMSGPRF**

The SHORT list has the following format:

**Figure 45. SHORT List Format for GROUP Profiles EMSGPRF**

The LONG list has the following format:
GROUP Profiles

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Logon Type</th>
<th>Logon Number</th>
<th>Sess. Term. Key</th>
<th>Key Beg.</th>
<th>End Key</th>
<th>Prefix</th>
<th>User ID</th>
<th>Date Time</th>
<th>Exit User Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS/P1</td>
<td>N</td>
<td>P123</td>
<td>5</td>
<td>N</td>
<td>PA2</td>
<td>PF2</td>
<td>$</td>
<td>PUBUSER</td>
<td>28/02/94</td>
</tr>
<tr>
<td>SYS/P2</td>
<td>N</td>
<td>U123</td>
<td>5</td>
<td>N</td>
<td>PA2</td>
<td>PF2</td>
<td>$</td>
<td>PUBUSER</td>
<td>28/02/94</td>
</tr>
<tr>
<td>USER1</td>
<td>N</td>
<td>P123</td>
<td>5</td>
<td>N</td>
<td>PA2</td>
<td>PF2</td>
<td>$</td>
<td>PUBUSER</td>
<td>28/02/94</td>
</tr>
<tr>
<td>USER2</td>
<td>N</td>
<td>U123</td>
<td>5</td>
<td>N</td>
<td>PA2</td>
<td>PF2</td>
<td>$</td>
<td>PUBUSER</td>
<td>28/02/94</td>
</tr>
</tbody>
</table>

Figure 46. LONG List Format for GROUP Profiles EMSGPRF

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT because in this case the new page control is not activated.

GROUP_APPLICATION Profiles EMSSRTG

The SHORT list has the following format:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS/P1</td>
<td>CICS</td>
<td>CICS2</td>
<td>B G Y PF24 1 I F Y</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>CICS Test system</td>
</tr>
<tr>
<td>SYS/P1</td>
<td>IMS</td>
<td>IMS3</td>
<td>R G Y PF24 2 I Y N</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>IMS Production system</td>
</tr>
<tr>
<td>SYS/P1</td>
<td>NETVIEW</td>
<td>NETVIEW</td>
<td>B G Y PF24 3 J N Y</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>NETVIEW Production system</td>
</tr>
<tr>
<td>USER1</td>
<td>DM/CICS</td>
<td>CICS1</td>
<td>R G Y PF18 5 J N Y</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>DM/370 CICS Relay mode</td>
</tr>
<tr>
<td>USER1</td>
<td>IMS</td>
<td>IMS3</td>
<td>R G N PF18 6 J Y N</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>IMS Relay mode</td>
</tr>
<tr>
<td>USER1</td>
<td>OFFICE</td>
<td>VM2</td>
<td>R G Y PF18 7 N N Y</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>OFFICE Relay mode</td>
</tr>
<tr>
<td>USER1</td>
<td>TSOP</td>
<td>TSOP</td>
<td>R G Y PF18 9 N N Y</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>TSOP Unique relay</td>
</tr>
<tr>
<td>USER1</td>
<td>VM1</td>
<td>VM1</td>
<td>R G Y PF18 10 J Y Y</td>
<td>PUBUSER</td>
<td>28/02/94</td>
<td>VM Relay mode</td>
</tr>
</tbody>
</table>

Figure 47. SHORT List Format for GROUP_APPLICATION Profiles EMSSRTG

The LONG list has the following format:
<table>
<thead>
<tr>
<th>Group</th>
<th>Appl. ID</th>
<th>Type</th>
<th>Prof.</th>
<th>Log.</th>
<th>Key ID</th>
<th>Ind. Comp.</th>
<th>User ID</th>
<th>Date</th>
<th>Time</th>
<th>Application description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSP1</td>
<td>CICS</td>
<td>CICS</td>
<td>B</td>
<td>G</td>
<td>Y</td>
<td>PF24</td>
<td>1</td>
<td>I</td>
<td>Y</td>
<td>PUBUSER 28/02/94 18:20:36 CICS Test system</td>
</tr>
<tr>
<td>SYSP1</td>
<td>IMS</td>
<td>IMS</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>PF24</td>
<td>2</td>
<td>I</td>
<td>Y</td>
<td>PUBUSER 28/02/94 18:20:11 IMS Production system</td>
</tr>
<tr>
<td>SYSP1</td>
<td>NETVIEW</td>
<td>NETVIEW</td>
<td>B</td>
<td>G</td>
<td>Y</td>
<td>PF24</td>
<td>3</td>
<td>J</td>
<td>N</td>
<td>PUBUSER 28/02/94 18:21:25 NETVIEW Production system</td>
</tr>
<tr>
<td>SYSP1</td>
<td>TSO</td>
<td>TSO</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>PF24</td>
<td>4</td>
<td>I</td>
<td>N</td>
<td>PUBUSER 28/02/94 18:19:46 TSO Production system</td>
</tr>
<tr>
<td>USER1</td>
<td>DWCICS</td>
<td>DWCICS</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>PF18</td>
<td>5</td>
<td>J</td>
<td>N</td>
<td>PUBUSER 28/02/94 18:18:44 DWCICS Relay mode</td>
</tr>
<tr>
<td>USER1</td>
<td>IMS</td>
<td>IMS</td>
<td>R</td>
<td>G</td>
<td>N</td>
<td>PF17</td>
<td>6</td>
<td>J</td>
<td>Y</td>
<td>PUBUSER 28/02/94 18:25:39 IMS Relay mode</td>
</tr>
<tr>
<td>USER1</td>
<td>OFFICE</td>
<td>OFFICE</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>PF18</td>
<td>7</td>
<td>N</td>
<td>N</td>
<td>PUBUSER 28/02/94 18:16:30 OFFICE Relay mode</td>
</tr>
<tr>
<td>USER1</td>
<td>TSO</td>
<td>TSO</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>PF12</td>
<td>9</td>
<td>N</td>
<td>N</td>
<td>PUBUSER 28/02/94 18:25:13 TSO Unique relay</td>
</tr>
<tr>
<td>USER1</td>
<td>VM1</td>
<td>VM1</td>
<td>R</td>
<td>G</td>
<td>Y</td>
<td>PF18</td>
<td>10</td>
<td>J</td>
<td>Y</td>
<td>PUBUSER 28/02/94 18:17:40 VM Relay mode</td>
</tr>
</tbody>
</table>

**Figure 48. LONG List Format for GROUP_APPLICATION Profiles EMSSRTG**

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT because in this case the new page control is not activated.

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT because in this case the new page control is not activated.

**USER Profiles EMSSRTU**

The SHORT list has the following format:
The LONG list has the following format:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EMSUSER</td>
<td>USER1</td>
<td>DWCICS</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>PF18 1</td>
<td>N</td>
<td>G</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>PUBUSER</td>
<td>28/02/94 18:22:36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMSUSER</td>
<td>USER1</td>
<td>IMS</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>PF17 2</td>
<td>N</td>
<td>G</td>
<td>1</td>
<td>Y</td>
<td>N</td>
<td>PUBUSER</td>
<td>28/02/94 18:22:36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMSUSER</td>
<td>USER1</td>
<td>OFFICE</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>PF18 3</td>
<td>N</td>
<td>G</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>PUBUSER</td>
<td>28/02/94 18:22:36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMSUSER</td>
<td>USER1</td>
<td>VM1</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>PF18 6</td>
<td>N</td>
<td>G</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>PUBUSER</td>
<td>28/02/94 18:22:36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 49. SHORT List Format for USER Profiles EMSSRTU

Figure 50. LONG List Format for USER Profiles EMSSRTU

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT because in this case the new page control is not activated.
ADMINISTRATOR Profiles EMSGAL

The list has the following format:

<table>
<thead>
<tr>
<th>Group</th>
<th>User</th>
<th>Type</th>
<th>Name</th>
<th>User ID</th>
<th>Date</th>
<th>Time</th>
<th>Exit user data</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUBUSER</td>
<td>S</td>
<td>ABC</td>
<td>12/02/93</td>
<td>13:56:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PUBUSER</td>
<td>S</td>
<td>ABC</td>
<td>12/02/93</td>
<td>13:56:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USER1</td>
<td>EMSUSER</td>
<td>PUBUSER</td>
<td>12/02/93</td>
<td>18:32:55</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMSUSER</td>
<td>B</td>
<td>PUBUSER</td>
<td>12/02/93</td>
<td>18:32:55</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 51. List Format for ADMINISTRATOR Profile EMSGAL

The short list format for administrators is the same as the long list format.

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT, because in this case the new page control is not activated.

BIND_USER_DATA Profiles EMSPLDT

The list has the following format:

<table>
<thead>
<tr>
<th>System</th>
<th>Last update information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Bind user data</td>
</tr>
<tr>
<td>Name</td>
<td>User ID</td>
</tr>
<tr>
<td>TSOP</td>
<td>PUBUSER</td>
</tr>
</tbody>
</table>

Figure 52. List Format for BIND_USER_DATA Profile EMSPLDT

When you specify the option SHORT, then only the first line for each profile is printed.

The date and time fields in the header and in the last update information for each profile are prepared by the date and time exit routine EMSEDTEX.

The page count is not edited if you specified the option LIST=REPORT because the new page control is not activated.
Chapter 11. Summary of Dependencies

Within NetView Access Services there are several application access parameters that are defined for each user or each application. Some access parameters depend on how others are set up. This chapter summarizes these dependencies.

For more information about each parameter, refer to Chapter 4, "System Administration Tasks" on page 31 and Chapter 5, "Group Administration Tasks" on page 63.

Refer to the following figure for a summary of the dependencies.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>First defined using option:</th>
<th>Modified using option:</th>
<th>Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Mode</td>
<td>4, S</td>
<td>6, S and 3, G</td>
<td>Access Mode = R</td>
</tr>
<tr>
<td>Print key</td>
<td>5, S</td>
<td>*, U</td>
<td>Access Mode = R</td>
</tr>
<tr>
<td>Escape Key</td>
<td>5, S</td>
<td>*, U</td>
<td>Access Mode = R</td>
</tr>
<tr>
<td>Command Key</td>
<td>5, S</td>
<td>*, U</td>
<td></td>
</tr>
<tr>
<td>Command Prefix</td>
<td>5, S</td>
<td>*, U</td>
<td></td>
</tr>
<tr>
<td>Copy Keys</td>
<td>5, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jump Key</td>
<td>2, G</td>
<td>1, U</td>
<td></td>
</tr>
<tr>
<td>Selection ID</td>
<td>2, G</td>
<td>1, U</td>
<td></td>
</tr>
<tr>
<td>Automatic Logon</td>
<td>4, S</td>
<td>2, G</td>
<td>Access Mode = R</td>
</tr>
<tr>
<td>Record Authorization</td>
<td>3, G</td>
<td></td>
<td>Automatic Logon = Y</td>
</tr>
<tr>
<td>Logon Profile Type</td>
<td>2, G</td>
<td>1, U</td>
<td>Automatic Logon = Y</td>
</tr>
<tr>
<td>Alternative Sequences</td>
<td>4, S</td>
<td>1, U</td>
<td>Record Authority = Y</td>
</tr>
<tr>
<td>Active Profile</td>
<td>1, U</td>
<td>1, U</td>
<td>Logon Profile Type = U</td>
</tr>
<tr>
<td>Msg. Received Indication</td>
<td>2, G</td>
<td>1, U</td>
<td></td>
</tr>
<tr>
<td>Number of Sessions</td>
<td>5, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiterminal Access</td>
<td>5, S</td>
<td></td>
<td>Multiterminal = Y</td>
</tr>
<tr>
<td>Terminal Assume</td>
<td>3, G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shareable</td>
<td>4, S</td>
<td>6, S 3, G</td>
<td></td>
</tr>
<tr>
<td>Shared Session Response</td>
<td>5, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application ID Display</td>
<td>2, G</td>
<td>1, U</td>
<td></td>
</tr>
<tr>
<td>Printer</td>
<td>5, S</td>
<td>+, U</td>
<td></td>
</tr>
<tr>
<td>ACB Type</td>
<td>4, S</td>
<td></td>
<td>Access Mode = R</td>
</tr>
<tr>
<td>Pseudo Terminal Prefix</td>
<td>4, S</td>
<td></td>
<td>ACB Type = U or I</td>
</tr>
<tr>
<td>Pseudo Terminal Name</td>
<td>3, G</td>
<td></td>
<td>Overrides a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pseudo Terminal Prefix</td>
</tr>
<tr>
<td>Maximum Sessions</td>
<td>4, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status Update</td>
<td>4, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Application Name</td>
<td>4, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Idle Time Value</td>
<td>4, S</td>
<td></td>
<td>Access Mode = R</td>
</tr>
<tr>
<td>Account Number</td>
<td>5, S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Group</td>
<td>3, G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Application</td>
<td>1, U</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* = Redefine Keys panel
+ = Printer Destination panel

Figure 53. Summary of Dependencies
Appendix. Forms to Help You Plan for Your Installation

This appendix provides forms to help with planning:

- System applications
- Groups
- Applications for each group.

### Planning for Defining a System Application

<table>
<thead>
<tr>
<th>Application</th>
<th>System Internal Name</th>
<th>Primary LU Name</th>
<th>ACB Type</th>
<th>TPN of ASR</th>
<th>Pseudo Terminal Prefix</th>
<th>Access Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Continuation of Planning for Defining a System Application

<table>
<thead>
<tr>
<th>Application</th>
<th>Shareable</th>
<th>Auto Logon</th>
<th>Alternative Sequences</th>
<th>Idle Time Value</th>
<th>Maximum Number of Sessions</th>
<th>Status Update</th>
<th>Backup Application Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Planning for Defining a Group

<table>
<thead>
<tr>
<th>Group</th>
<th>Group Type</th>
<th>Account Number</th>
<th>ASP Format</th>
<th>Number of Sessions</th>
<th>Multi-terminal Access</th>
<th>Shared Session Response</th>
<th>Logon REXX Exec</th>
<th>Logoff REXX Exec</th>
<th>Printer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Continuation of Planning for Defining a Group

<table>
<thead>
<tr>
<th>Group</th>
<th>Print Key</th>
<th>Escape Key</th>
<th>Command Key</th>
<th>Command Prefix</th>
<th>Copy From Begin</th>
<th>Copy From End</th>
<th>Copy to</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Planning for Assigning an Application to a Group

<table>
<thead>
<tr>
<th>Group</th>
<th>Application</th>
<th>System Internal Name</th>
<th>Access Mode</th>
<th>Shareable</th>
<th>Data Compression</th>
<th>Virtual Terminal</th>
<th>Logon REXX Exec</th>
<th>Logoff REXX Exec</th>
<th>LogMode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Glossary

This glossary defines terms as they are used in this book. If you do not find the terms you are looking for, refer to Dictionary of Computing, SC20-1699.

**ACB.** Access Method Control Block. A control block that links an application program to VSAM or VTAM.

**access.** In RACF, the ability to obtain use of a protected resource.

**access mode.** In NetView Access Services, the type of access a user can have to an application. There is relay mode only, pass mode only, or both.

**access parameter.** A variable that is given a value to determine the type of access to a specific application. In NetView Access Services, parameters that define the access a user can have to an application used via NetView Access Services.

**active user logon profile.** The user logon profile that is selected, from two, to be the one NetView Access Services uses to perform automatic logon to an application.

**administration.** The process of designing, controlling, and managing the use of NetView Access Services or a NetView Access Services group.

**administration panel.** A panel designed to aid in the task of administration.

**administrator.** A person who organizes applications and users into groups, and defines certain parameters for the system, groups, users, and applications.

**alternative sequence.** A sequence of data recorded as an alternative to a main sequence. It is used when an application cannot respond to the main sequence in the logon profile.

**application.** In NetView Access Services, an application program, system, or subsystem.

**application session.** In NetView Access Services, a session between NetView Access Services and an application.

**APPL statement.** In VTAM, a statement identifying an application to VTAM.

**ASR.** Application Service Routine. In NetView Access Services, a service routine that communicates with applications through the communication services of NetView Access Services and then VTAM.

**ASR-to-ASR communication.** In NetView Access Services, a function that implements a link between the ASRs of the same NetView Access Services through the communication services of NetView Access Services without traversing VTAM.

**authorized user.** A user who is authorized by an administrator to use certain restricted commands.

**automatic logon.** In NetView Access Services, the process of creating a logon from NetView Access Services to an application.

**automatic logon authorization.** In NetView Access Services, the right to use the automatic logon function.

**BIND.** In SNA products, a request to activate a session between two logical units.

**BIND user data.** In SNA, data, which relates to a user, that is sent with a BIND request.

**broadcast message.** In NetView Access Services, a message that is transmitted to the Application Selection panels of all users on the system.

**CICS/VS.** Customer Information System/Virtual Storage. An IBM licensed program used in a communications network. It is a transaction manager that provides database and data communications support of transaction programs.

**command key.** In NetView Access Services, the key that is used when in an application, to send a command to NetView Access Services.

**command prefix.** A string of characters that is used, when in an application, to denote the beginning of a command that is sent to NetView Access Services.

**copy buffer.** A portion of storage that is used to hold data that has been copied from an application panel until it is copied to another application.

**default application.** When specified, the application that is assumed if none is entered on the Logon panel.

**default group.** The group with which a user is associated when no group name is entered on the Logon panel.

**disconnecting.** The process of breaking the connection with NetView Access Services temporarily, while keeping all current application sessions active.
**escape key.** The key you use when you are in an application panel to display the Application Selection panel on the screen, without logging off or disconnecting from that application.

**field.** A specified area used for a particular type of data.

**filing.** In NetView Access Services, the process of storing a logon or logoff sequence in a file called a profile.

**first-level help.** In NetView Access Services, help that is displayed in a message when the help key or command is entered once.

**free selection field.** In NetView Access Services, an optional field on the Application Selection panel where a user can enter the name of an application, in the current group, for which he is authorized, but which is not displayed on the Application Selection panel.

**group.** A set of applications bound by common criteria. The system administrator decides the criteria used to define groups and the applications to be used within the group. There are three types of groups: Normal, Public, and External.

**group administrator.** The person who administers a group.

**help message.** See first-level help.

**help panel.** See second-level help.

**home location.** The location where you usually work.

**idle time.** The part of operable time during which a program is not used.

**IMS/VS.** Information Management System/Virtual Storage. A general-purpose database system that enhances the capabilities of MVS/ESA for batch processing and telecommunication. It allows users to access a computer-maintained database through remote terminals.

**input field.** A field on a panel where a user can enter data.

**installer.** The person who installs a program.

**installing.** The process of preparing and placing a functional unit in position for use.

**jumping.** In NetView Access Services, going from the current application to another application, without going back to the NetView Access Services Application Selection panel.

**jump key.** The key used to jump from the current application to another application.

**keyword parameter.** A parameter that consists of a keyword, followed by one or more values. See also positional parameter.

**location.** A place where NetView Access Services is installed.

**logging off.** The process of terminating a session with an application or NetView Access Services.

**logging on.** The process of opening a session with an application or NetView Access Services.

**logoff sequence.** A sequence of data recorded during a logoff.

**logon profile.** A file containing a logon sequence, plus any alternative sequences, and a logoff sequence, if one has been recorded. This file is used by NetView Access Services for automatic logon and logoff.

**logon sequence.** A sequence of data recorded during a logon procedure. For example, variables for the user ID and password, and any other information necessary to complete the logon to a particular application that can be used by NetView Access Services to perform the logon automatically for the user.

**LU.** Logical unit. In SNA, a port through which a user gains access to the SNA network to communicate with another user and through which the user gains access to the functions provided by the system. An LU can support at least two sessions, and might be capable of many sessions with other LUs.

**LU name.** In programming, a name used to represent an input/output unit.

**mode.** A method of operation. See pass mode, relay mode.

**multiterminal authorization.** The authorization to be logged on at more than one terminal at a time.

**MVS.** Multiple Virtual Storage. An IBM licensed program whose full name is Operating System/Virtual Storage (OS/VS) with Multiple Virtual Storage/System Product for System/370. It is a software operating system controlling the execution of programs.

**NetView.** An IBM licensed program consisting of a base for command processors that can monitor, control, and improve the operation of a network.

**network.** A configuration of data processing and software connected for information interchange. See also SNA network.
online help. Text displayed when a user requests help with an online function.

operator. A person who operates a device or a system.

operator console. A display console used for communication between the operator and the system, used primarily to specify information concerning application programs, and to monitor the system.

panel. The complete set of information shown in a single display on a screen. Each panel is like a manual page.

pass mode. In NetView Access Services, the mode you use to select an application when NetView Access Services passes control to the application.

PLU. Primary logical unit.

print key. The key used to print a panel of an application.

printer. The printer to which a user can send a copy of a panel of an application. The printer is displayed on the Application Selection panel.

position parameter. A parameter that must appear in a specified location relative to other positional parameters. See also keyword parameter.

primary logical unit. In SNA, the LU that contains the primary half-session for a particular LU-to-LU session. Contrast with secondary logical unit. See LU.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, user-installed programs or equipment, environmental failure such as a power loss, or a user error.

profile. Data that describes the significant characteristics of a user, a group of users, or one or more computer resources.

pseudo terminal name. In NetView Access Services, a name used to represent a terminal in a relay mode session. If the session has ACB type Unique or Individual, this name can be one from a pool of names, each using a common prefix with different numbers affixed. If the session has ACB type Shared, this name is not from a pool, but it could be the same as the prefix, with no numbers suffixed.

pseudo terminal prefix. In NetView Access Services, a string used to define a pool of pseudo terminal names. The names are defined by suffixing numbers to this prefix.

quiescing. The process of bringing a device or a system to a halt by rejection of new requests for work.

RACF. Resource Access Control Facility. An IBM licensed program that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, logging the detected unauthorized attempts to enter the system, and logging the detected accesses to protected resources.

recording. The process of storing a sequence of data for future use in a logon profile.

relay functions. In NetView Access Services, functions that you can perform when all processing of an application goes through NetView Access Services.

relay mode. The mode you use when all processing of an application goes via NetView Access Services.

returning. In NetView Access Services, the process of using a special key or command, when in an application, to display the Application Selection panel on the screen, without logging off or disconnecting from that application.

screen copy. In NetView Access Services, the facility that enables users to copy data from a panel on a terminal screen to a copy buffer, and then to copy it to another panel on the screen.

second-level help. In NetView Access Services, help that is displayed on a panel when the help key or command is entered twice in an input field of a NetView Access Services panel.

secondary logical unit. In SNA, the LU that contains the secondary half-session for a particular LU-to-LU session. Contrast with primary logical unit. See LU.

selective broadcast message. In NetView Access Services, a broadcast message that is sent only to selected users or groups of users by the system administrator.

session. In SNA, a logical connection between two network addressable units that can be activated, tailored to provide various protocols, and deactivated as required. In NetView Access Services, a session between NetView Access Services and an application.

single access control. A facility that provides for programmed control, from a single screen, of a user's authorization to access-protected data.

SLU. Secondary LU.

SNA. System Network Architecture. The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through,
and controlling the configuration and operation of, networks.

**SNA network.** In SNA, the part of a user-application network that conforms to the formats and protocols of System Network Architecture. It enables reliable transfer of data among users, and provides protocols for controlling the resources of various network configurations.

**system.** In data processing, a collection of people, machines, and methods organized to accomplish a set of specific functions.

**system administrator.** In NetView Access Services, an administrator of the system.

**system-internal name.** The name by which an application is identified to the NetView Access Services system. The same application may have a different name within each group.

**terminal assume authorization.** In NetView Access Services, the authorization to assume at one terminal an active session from another terminal.

**timing out.** A feature that logs off a user if an entry is not made within a specified period of time.

**TPN.** transaction program name. In NetView Access Services, the name of the transaction program for ASR-to-ASR communication.

**tracing.** In NetView Access Services, the process of displaying the sequence in which instructions are performed during an automatic logon or logoff.

**TSO.** Time Sharing Option.

**time sharing option.** The option on an MVS operating system providing interactive time sharing from remote terminals.

**user authorization.** The right granted to a user to have complete or restricted access to a function.

**user exit.** A point in an IBM-supplied program at which a user-exit routine may be given control.

**user-exit routine.** A routine written by a user to take control at a user exit of a program supplied by IBM.

**user logon profile.** In NetView Access Services, a logon profile recorded and filed by a user.

**variable.** A name used to represent a data item whose value can be changed while the program is running.

**VTAM.** Virtual Telecommunications Access Method. Its full name is Advanced Telecommunications Function for the Virtual Telecommunications Access Method. A set of programs that maintain the control of the communication between terminals and application programs running under some operating systems.

**VTAM application program.** An application program that has opened an ACB to identify itself to VTAM and can issue VTAM macroinstructions.
Bibliography

The following books belong to the NetView Access Services Version 2 library:

NetView Access Services Version 2 General Information, GH19-4497

NetView Access Services Version 2 Licensed Program Specifications, GH19-4498


NetView Access Services Version 2 Operation, SH19-4501

NetView Access Services Version 2 Customization, SH19-4502


The following are network-related publications:

SNA Application Monitor General Information Manual, GH12-5160

Network Program Products—Planning, SC23-0110

Virtual Machine/System Product Group Control System Command and Macro Reference, SC24-5250

Supervisor Services and Macro Instructions, GC28-1154

3274 Control Unit Description and Programmer’s Guide, GA23-0061

VTAM: Programming, SC23-0115

VTAM: Messages and Codes, SC31-6405

Index

Special Characters
&1 through &3 84
&ACCNO 83
&GRP 85
&GVAR1-5 84
&LCD 84
&NPW 84
&OPW 84
&OWNLU 85
&PWD 83
&SPW 84
&TLU 84
&UID 83
&UVAR1 through &UVAR4 84, 101

A
ACB type 32
ACBs
  individual 14
  selecting the type 14
  shared 12
  unique 13
  with generic pseudo terminal name 34
access mode
  defining 34
  selecting the 86
  using 86
access parameters
  controlling 85
  displaying 68
  maintaining 64
  relay mode 5
accessing
  applications, method of 5
  the same application several times 59
ACCNO 39
account number, defining 39
ACF/VTAM APPL statement 32, 33
activating logon and logoff sequences 95
ADD command 29
adding
  a selective broadcast message 80
  application for a user 72
  application to a group 47
  data sent with a request for a session 56
  new application 38
  new group 42
  user to a group 72
administration
  examples 21
  (continued)
    functions, calling the 28
    group 63
    initial 26
    panels, using commands on the 29
    system 31
administration exit, EMSEADEX 42, 50
administration selection panel 28
  for a group administrator 63
  for a system administrator 31
administrator
  defining 48
    new broadcast only 50
    new group 50
    new system 50
  deleting system 51
  displaying whether user is an 50
  group
    responsibilities 4
    tasks 63
  group, deleting 51
  listing broadcast only 51
  listing groups for which a user is an 51
  of a group, listing 51
  planning 8
  system
    responsibilities 4
    tasks 31
    system, listing 51
  updating characteristics of 50
    broadcast only 50
    group 50
    system 50
  user tasks 29
administrator authorization data set, commands for
  the 136
ADMINISTRATOR profile 144
AG command 95
alternative sequences 35
alternative sequences, defining 35
ampersand variables
&1 through &3 84
&ACCNO 83
&GRP 85
&GVAR1 through &GVAR5 84
&LCD 84
&NPW 84
&OPW 84
&OWNLU 85
&PWD 83
&SPW 84
&TLU 84
commands
 activate group 95
 activate system 95
 administration 29
 administrator authorization data set 136
 application profiles data set 116
 application routing data set 123
 BIND user data profiles data set 138
 group profiles data set 119
 recording 94
 rules for writing batch load 114
 select pass 86
 select relay 86
 syntax of the batch load and reporting 111
 user profiles data set 128
 compression, data
 outbound and inbound 45
 outbound only 45
 controlling access 85
 copyfrom key, defining 42
 copyto key, defining 42
 creating and controlling logon profiles 91

D

data
 defining BIND user for 97
 for an application
 defining BIND user 54
 displaying 38
 updating 38
 passed 55
 sent with a request for a session, displaying 55
 to be sent with a request for a session, adding 56
 to be sent, updating 56
 data compression
 outbound and inbound 45
 outbound only 45
 default
 group 70
 group dependencies 70
 user ID, PUBUSER 26
 define a group panel
 explanation of fields on 39
 define an application for the system panel
 explanation of fields on 32
 define BIND user data for applications panel 98
 defining
 a user to a group 69
 ACB type 32
 access mode 34
 account number 39
 administrator 48, 49
 alternative sequences 35
 application to a system 31
 automatic logon 35
 defining (continued)
 BIND USER data 54, 97
 broadcast-only administrator 50
 command key 41
 command prefix 42
 copyfrom key 42
 copyto key 42
 group 38, 151
 group administrator 50
 group parameters 64
 group type 39
 idle-time value 35
 maximum sessions 35
 multiterminal access authorization 40
 number of sessions 40
 primary LU name 32
 print key 41
 printer 41
 pseudo terminal prefix 33
 REXX exec
 for application logoff 46
 for application logon 46
 for group logoff 40
 for group logon 40
 shareable 35
 shared session response 40
 system administrator 50
 system application 149
 system-internal name 32
 TPN of ASR 33
 defining BIND user data 100
 DELETE command 29
 deleting
 a broadcast message
 general 54
 selective 81
 administrators of a group 51
 all applications of a user 72
 application from a group 47
 application from the system 38
 data sent with a request for a session 56
 group 43
 system administrators 51
 user 72
 user from list of administrators of a group 51
 user from list of system administrators 51
 deleting an application or removing it from the
 LUNT 18
 dependencies, summary 145
 default group 70
 different locations, residing at 43
 disconnect, session idle 35
 disconnecting, leaving sessions active 34
 DISPLAY command 29
 displaying
 access parameters 68
displaying (continued)
attributes of a group application 47
characteristics of a group 42
data for an application 38
data sent with a request for a session 55
information relating to a user 72
information relating to an application 72
selective broadcast messages 80
whether a user is an administrator 50
dynamic modification of LUNT queues 18

E
EMSEADEX, administration exit 42, 50
EMSGPRF group profiles data set, commands for
the 119
EMSSRTG application routing data set, commands for
the 123
EMSSRTS application profiles data set, commands for
the 116
EMSSRTU user profiles data set, commands for
the 128
END command 29
escape key 41
escape key, different levels of NetView Access
Services 60
example of bulletin board information 57
examples of administration 21
exit, session establishment EMSESEEX 33
explanation of fields when
assigning a user to group 70
assigning an application to group 44
defining a group 39
defining an administrator 49
defining an application to the system 32
defining BIND user data for an application 55
maintaining group parameters 64
external group type 39

F
field, assigning the free selection 75
field, key 29
fields, explanation of
assign a user to group panel
access mode 70
application 70
default group 70
group 70
last update 70
logon variables 71
pseudo terminal name 71
record authorization 71
shareable 71
terminal assume 71
user 70
user-exit data 72
fields, explanation of (continued)
assign an application to a group panel
access mode 45
application 44
data compression 45
group 44
last update 45
logoff REXX exec 46
logon REXX exec 46
shareable 45
system-internal name 45
virtual terminal 46
broadcast selectively panel
group 78
group application name 78
interruptive message 79
language ID 78
last update 78
member name 78
message ID 78
system application name 78
terminal ID 78
time controlled message 79
user 78
define a group panel
account number 39
command key 41
command prefix 42
escape key 41
group 39
group type 39
last update 39
logoff REXX exec 40
logon REXX exec 40
multiterminal access 40
number of sessions 40
print key 41
printer 41
screen copy keys 42
shared session response 40
user-exit data 42
define an administrator panel
group 49
last update 49
type 49
user 49
user-exit data 49
define an application for this system panel
ACB type 32
access mode 34
alternative sequences 35
automatic logon 35
backup application name 37
idle-time value 35
last update 32
maximum sessions 35
primary LU name 32
fields, explanation of (continued)
define an application for this system panel (continued)
pseudo terminal prefix 33
shareable 35
status update 36
system-internal name 32
TPN of ASR 33
define BIND user data for an application
last update 55
passed data 55
system-internal name 55
maintain group parameters panel
application 64
application description 65
application ID display 67
automatic logon 66
default selection ID 65
group 64
jump key 65
last update 64
logon profile type 66
msg. received indicator 65
formats, LIST output, batch load 139
forms, planning for installation 149
free selection field, assigning the 75
functional summary, batch load 105

G
general broadcast message
description of 51
sending 52
generic pseudo terminal name 15, 33
generic pseudo terminal name, ACB type 34
geography 43
group
administration  
See group administration
concept 5
default 70
group-wide name of application 44
name 64, 70
name, defining user to group 70
parameters, maintaining 64
group administration
adding
a user 72
an application for a user 72
defining a user to a group 69
listing
all groups 74
all users 73, 74
applications of a group 68
applications of a user 73
applications that a user can use 73
groups in which a user can use an application 74
group administration (continued)
listing (continued)
users assigned to use applications in a 74
users that have access to an application 74
users who can use an application 74
updating
access parameters for applications 68
user and application data 73
group administrator
See also administrator, group
responsibilities 4
tasks 63
updating characteristics of 50
group application, displaying attributes of 47
GROUP profiles 140
group profiles data set, commands for the 119
group selection panel, defining groups on 39
group type
defining 39
external 6
normal 6
public 6
GROUP_APPLICATION profiles 141
grouping criteria, user 43
groups, understanding 5

H
HELP command 29

I
idle time value, defining 35
individual ACB
description of 14
with generic pseudo terminal name 34
initial administration, performing the 26
installing, forms for planning 149
introduction to NetView Access Services 3

J
job control language for batch load 106
jump key 65
jump key dependencies 65
jump key, different levels of NetView Access Services 60

K
key
command 41
escape, different levels of NetView Access Services 60
jump 65
jump, different levels of NetView Access Services 60
key input fields 29

L
language command, batch load 111
limiting access 85
LIST command 29
list of system administrators, deleting a user 51
LIST output formats, batch load 139
listing
administrators of a group 51
all group administrators 51
all groups 47, 73, 74
applications 38, 73
applications for which BIND user data has been defined 56
applications in the system 47
applications of a group 68
applications of a user 73
applications that a user can use 73
broadcast-only administrators 51
groups 69
groups defined to NetView Access Services 42
groups for which user is administrator 51
groups in the system 47, 51
groups in which a user can use an application 74
groups that have access to an application 47
system administrators 51
users assigned to use applications in a 74
users in all groups 74
users that have access to an application 74
users who can use an application 74
which groups have access to an application 69
locations, residing at different 43
logging off
automatically 91
timing out 86
logical unit names table (LUNT) 17
LogMode 46, 128
logoff sequence
activating 95
recording 93
logon
automatic 35, 66
profiles, authorization 91
sequence
activating 95
recording 93
logon variables (&GVAR1...&GVAR5) 71
logon, creating and controlling 91
logons, automatic 85
LU name, primary 32
LUNT
deleting an application or removing it from the 18
queues, dynamic modification of 18
queues, non-shared 17
LUNT (continued)
queues, shared 17

M
maintain group parameters panel
   explanation of input fields 64
maintaining
group parameters 64
maximum number of sessions 33
   sharing a NetView Access Services session 87
maximum sessions
defining 35
   pseudo terminal prefix and 15
message received indication 65
message, broadcasting a 51
modes of access
   pass 5, 34, 45
   relay 5, 34, 45
modification of LUNT queues, dynamic 18
multiterminal access authorization, defining 40

N
name
generic pseudo terminal 15, 33
group
   on maintain group parameters panel 64
   when assigning applications to groups 44
   when defining users to groups 70
primary LU 32
pseudo terminal 11, 71
pseudo terminal, assigning 15
   system-internal
      when assigning application to group 45
      when defining application to system 32
      when defining BIND user data 55
names, sharing the pool of pseudo terminal 13
new group administrator, defining a 50
new group, adding a 42
new system administrator, defining a 50
non-shared LUNT queues 17
normal group type 39
number of sessions, defining 40
number, account 39

O
options, batch load 110
out, timing 86
output formats, LIST, batch load 139
overview, planning 9

P
panels
   using commands on the administration 29
parameters
  displaying the 68
  for an application in your group, updating the 68
  maintaining group 64
  relay mode access 5
pass mode 5, 45
pass mode, defining an application 34
passed data 55
planning
  administrator 8
  for assigning an application to a group 152
  for defining a group 151
  for defining a system application 149
  for installation 149
  overview 9
pool of pseudo terminal names, sharing the 13
pool, size of the 36
prefix
  command 42
  pseudo terminal 33
prefix, pseudo terminal 13
preparing for a new installation 21
primary LU name, defining 32
print key, defining 41
printer, defining 41
profiles
  ADMINISTRATOR 144
  authorization to record the 92
  BIND_USER_DATA 144
  creating and controlling logon 91
  GROUP 140
  GROUP_APPLICATION 141
  recording logon 93
  refreshing from VSAM data sets 56
  SYSTEM_APPLICATION 139
  USER 142
  providing bulletin board information 56
pseudo terminal
  name, generic 15, 33
  name, when defining user to group 71
  names, description of 11
  names, sharing the pool of 13
  names, strategy of assigning 15
  prefix 13
    defining 33
    description of 33
  prefix and maximum sessions 15
public group type 39
PUBUSER supplied user ID 26

Q
queues
  dynamic modification of LUNT 18
  non-shared LUNT 17
  shared LUNT 17

R
record commands, description of the 94
  recording
    authorization 71, 92
    commands 94
    logoff sequences 93
    logon sequences 93
  refreshing profiles from VSAM data sets 56
relay mode 5, 45
  access parameters 5
  considerations 5
  defining an application 34
reporting utility, batch load 105
request for a session, adding data to be sent with a 56
request for a session, displaying data sent with a 55
residing at different locations 43
restricting access 85
REXX exec, defining for
  application logoff 46
  application logon 46
  group logoff 40
  group logon 40

S
second session with the same application 14
security 83, 85
selecting the ACB type 14
selective broadcast message
  adding 80
  deleting 81
  displaying 80
  sending 54, 77
  updating 81
sending
  a broadcast message 52
    general 51
    selective 54, 77
  sent with a request for a session, adding data to be 56
  sequences, alternate 35
  session establishment exit EMSESEEX 33
  session, adding data to be sent with a request for a 56
  sessions
    active when user disconnects 34
    maximum 33
    number of 40
    shareable 71
set, commands for the BIND user data profiles
  data 138
set, commands for the group profiles data 119
shareable application, defining 35
shared ACB
  description of 12
  with generic pseudo terminal name 34
USER profiles 142
user profiles data set, commands for the 128
user-exit data 42, 49
user, adding an application for a 72
users in your groups, listing the 74
using commands on the administration panels 29

V
variables
&1 through &3 84
&ACCNO 83
&GRP 85
&GVAR1 through &GVAR5 84
&LCD 84
&NPW 84
&OPW 84
&OWNLU 85
&PWD 83
&SPW 84
&TLU 84
&UID 83
&UVAR1 through &UVAR4 84
in BIND user data 101
in system-wide logon profile 85
logon 71
VSAM data sets, refreshing profiles from 56

W
writing batch load commands, rules for 114
Communicating Your Comments to IBM

NetView Access Services (MVS/ESA)  
Administration  
Version 2 Release 1  
Publication No. SH19-4500-00

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers’ comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.
- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number: 39+6+5966+2077

Make sure to include the following in your note:
- Title and publication number of this book
- Page number or topic to which your comment applies.
Help Us Help You!


We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?  Satisfied  Dissatisfied

How satisfied are you that the information in this book is:  Satisfied  Dissatisfied

- Accurate
- Complete
- Easy to find
- Easy to understand
- Applicable to your task
- Well organized

Specific Comments or Problems:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Please tell us how we can improve this book:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

Phone No.
Help Us Help You!
SH19-4500-00

NetView Access Services Information Development
Rome Tivoli Laboratory
IBM Italia S.p.A.
Via Sciangai, 53
00144 Rome
Italy