Book Cover

Distributed Console Access Facility

Installation and Configuration Guide

Version 1.31

Document Number SH19-4068-01

Part Number 34H0762

Program Number
5622-212

NOTICES

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" in topic NOTICES.

ISO 9001 Certification

This product was developed using an ISO 9001 certified quality system.

Certification has been awarded by the Italian quality system certification group, CSQ (Certification No. CISQ/CSQ 9151.IBM1).

CSQ is a member of the mutually recognized organization of European assessors, ITQS, which assesses and certifies quality systems in the field of information technology enterprises.

EDITION Edition Notice

Second Edition (August 1995)

This edition applies to Version 1.31 of the licensed program Distributed Console Access Facility, Program Number 5622-212, which runs on the following operating systems:

- OS/2 workstations run on IBM Operating System/2* Version 2.1 or later.
- The Windows** target runs on Microsoft** Windows** Version 3.1x or Microsoft Windows for Workgroups Version 3.1x.
- The DOS target runs on Disk Operating System (DOS) Version 6.3 or later or Microsoft DOS Version 6.2 or later.

Make sure you are using the correct edition for the level of the product.

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

A form for reader′s comments is provided at the back of this publication. You may also address your comments to:

End-User Technologies
Rome Networking Software Laboratory
IBM SEMEA S.p.A.
P.le G. Pastore, 6
00144 Rome
Italy
FAX: **39+6+5966+2456**
Internet ID: ROMERCF at VNET.IBM.COM

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

Table of Contents

FIGURES Figures

TABLES Tables

NOTICES 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, is 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, U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
P.O. Box 12195
3039 Cornwallis
Research Triangle Park, NC 27709-2195
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

For online versions of this book, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

TRADEMARKS Trademarks

The following terms, denoted by an asterisk (*) at their first occurrence in the DCAF publications, are trademarks of IBM Corporation in the United States or other countries:

Advanced Peer-to-Peer Networking	APPN
AT	BookManager
Extended Services for OS/2	IBM

Library Reader	NetView
Operating System/2	OS/2
Personal Computer AT	Personal System/2
Presentation Manager	PS/2
ThinkPad	VTAM
Workplace Shell	XGA

The following terms, denoted by a double asterisk (**) at their first occurrence in the DCAF publications, are trademarks of other companies in the United States or other countries:

ATI	ATI Technologies, Inc.
FasTalk	Universal Data Systems
Hayes	Hayes Microcomputer Products, Inc.
HP	Hewlett-Packard Company
Intel	Intel Corporation
IPX	Novell, Inc.
Microsoft	Microsoft Corporation
MNP	Microcom Systems, Inc.
Motorola	Motorola, Inc.
MS	Microsoft Corporation
MS-DOS	Microsoft Corporation
NetWare	Novell, Inc.
Novell	Novell, Inc.
NT	Microsoft Corporation
SatisFAXtion	Intel Corporation
SPX	Novell, Inc.
Telebit	Telebit Corp.
Windows	Microsoft Corporation
386	Intel Corporation

PREFACE About This Book

This book explains how to install, personalize, and configure the IBM Distributed Console Access Facility (DCAF). The DCAF enables a user at one programmable workstation to remotely control the keyboard and mouse input and monitor the display output of another programmable workstation.

WHO Who Should Use This Book

This book is intended for the following users:

- System planners and programmers who will define the network for Distributed Console Access Facility. See "Planning for Installation" in topic 1.0.
- System programmers who will install and customize prerequisite products for the Distributed Console Access Facility. See "Planning for Installation" in topic 1.0.
- System programmers who will install and customize Distributed Console Access Facility. See "Installing and Personalizing the DCAF" in topic 2.0.
- System planners and programmers who will define or install and customize DCAF security. See "DCAF Security" in topic 4.0.
- System programmers who will configure the communications for DCAF. See "Configuring" in topic 3.0.

As a system programmer or planner, you should be familiar with the IBM operating system that you are using. Version 1.31 of the Distributed Console Access Facility runs on the following operating systems:

- OS/2 workstations run on IBM Operating System/2* Version 2.1 or later.
- The Windows** target runs on Microsoft** Windows** Version 3.1x or Microsoft Windows for Workgroups Version 3.1x.
- The DOS target runs on Disk Operating System (DOS) Version 6.3 or later or Microsoft DOS Version 6.2 or later.

In addition, you should know how to use a text editor, such as the OS/2 System Editor, to edit text files.

HOW How to Use This Book

This book is structured for users who are planning to install and use the Distributed Console Access Facility product for the first time or who are upgrading to version 1.31 of DCAF. This book has the following parts:

- "Planning for Installation" in topic 1.0, gives a general concept of DCAF and guidelines to plan for installation. It also gives the technical requirements (such as software, hardware, workstation model, communications, and memory) for using DCAF.
- "Installing and Personalizing the DCAF" in topic 2.0, provides information on all the DCAF components and how to choose, install and customize them.
- "Configuring" in topic 3.0, provides examples to configure for DCAF.
- "DCAF Security" in topic 4.0, provides information on DCAF security and how to set it up.

- Appendix A, "Optimizing DCAF" in topic APPENDIX1.1, provides suggestions to get the best out of DCAF.

- Appendix B, "Startup Files" in topic APPENDIX1.2, summarizes the changes to the startup files that occur during installation and shows a sample DCAFDOS.BAT file that is used by the DOS target workstation at startup time.

- Appendix C, "Response Files" in topic APPENDIX1.3, provides sample response files and personalization parameters for CID installation.

- Appendix D, "DOS Target Technical Information" in topic APPENDIX1.4, discusses technical information for DOS workstations using DCAF, including command line parameters, specifying NetBIOS resources, use of terminate and stay resident programs and code page changes.

- Appendix E, "Windows Target Technical Information" in topic APPENDIX1.5, discusses technical information for Windows targets using DCAF.

- Appendix F, "Common Modem Device Initialization Strings" in topic APPENDIX1.6, provides the initialization strings for the most common modems that you can use with the DCAF.

- "Glossary of Terms and Abbreviations" in topic GLOSSARY explains the product-specific terms you will encounter while reading this book.

- The "Index" in topic INDEX helps you find the information that you need quickly.

TERMINOLOGY Terminology

This section explains some of the terms that are used in this book.

Term **Definition**

Cancel Close a drop-down menu, dialog box, or current selection.

Check Turn on a toggle command in a drop-down menu or select a check box option in a dialog box.

Choose Choose a menu command or command button.

Select Any of the following:

- Mark data in the window for further action. Selected text or objects appear highlighted or outlined.
- Open a drop-down menu.
- Click a drop-down arrow to open a list box.
- Turn on an option button or check box in a dialog box.

Because DCAF components run in OS/2, DOS, and Windows environments, instructions include mixed terminology. Table 1 gives OS/2 terms with their Windows equivalents.

Table 1. Comparison of OS/2 and Windows Terminology

OS/2 Term	**Windows Term**
push button	command button
radio button	option button
check box	same

list box	same
field	text box
spin button	spin box
pull-down menu	drop-down menu
pop-up menu	same
cascading menu	same

WHERE Where to Find More Information

The following list contains the names and order numbers of books in the DCAF library.

Hardcopy	
Distributed Console Access Facility Installation and Configuration Guide	SH19-4068
Distributed Console Access Facility Messages and Codes	SH19-4070
Distributed Console Access Facility Target User's Guide	SH19-6839
Distributed Console Access Facility User's Guide	SH19-4069
Softcopy CD-ROM	
IBM Networking Systems Softcopy Collection Kit	SK2T-6012
OS/2 Collection Kit	SK2T-2176

In addition, the DCAF library is available for IBM BookManager* READ/2 and Library Reader* on a diskette included in the DCAF package.

RELATED_PUBLICATIONS Related Publications

Refer to the following publications for information about the software related to DCAF.

IBM Operating System/2 APPC Programming Reference, S01F-0295

IBM Operating System/2 ACDI Programming Reference, S01F-0294

IBM Extended Services for OS/2 Network Administration Guide, S04G-1001

IBM Extended Services for OS/2 Communications Manager Configuration Guide, S04G-1002

IBM Extended Services for OS/2 Programmable Configuration Reference, S04G-1003

IBM Extended Services for OS/2 Communications Manager Host Connection Reference, S04G-1004

IBM Extended Services for OS/2 Programming Services and Advanced Problem Determination for Communications, S04G-1007

IBM Communications Manager/2 Workstation Installation and Configuration Guide, SC31-7169

IBM Communications Manager/2 User's Guide, SC31-6108

IBM TCP/IP for OS/2: User's Guide, SC31-6076

Workstation Security Services Installation and Operating Guide, SA34-2141

Product documentation for IPX/SPX**

Product documentation for LAN Support Program

Product documentation for Windows**

CHANGES Summary of Changes

The following is a list of changes to the DCAF for this release:

- APPN* connection support was added
- Book reorganized into three books:
  - Distributed Console Access Facility Installation and Configuration Guide
  - Distributed Console Access Facility Messages and Codes
  - Distributed Console Access Facility User's Guide
- Configuration/Installation/Distribution (CID) enablement was added
- Display driver independence was added
- Installation from a CD-ROM enablement was added
- IPX and TCP/IP connections for OS/2 and Windows targets was added
- New configuration scenarios
- Support for direct NetBIOS connections between controller and target was added
- Workstation directory on the controller was added

These changes are documented in this book.

1.0 Planning for Installation

1.1 DCAF Fundamentals

The IBM Distributed Console Access Facility (DCAF) provides a remote console function that allows one workstation, the controller, to control the keyboard and mouse input and monitor the display output of another workstation, the target.

This chapter explains, in addition to the fundamentals of the DCAF, the DCAF environment with its various components. You need to know this information before you can begin to install the product. Think of DCAF as a system that works on top of your system and communications environment.

When the DCAF session is in the monitoring state, the controller sees a screen image of the target workstation's display. The target workstation user has complete control of the operations of the target workstation.

When the DCAF session is in the active state, the controller operates and controls the target workstation. The keystrokes typed by the controller are relayed to the target workstation and acted upon as if they were typed by the target workstation user. The keystroke input and the resulting screen image of the target workstation's display are seen on both the controller and target workstations. During the active state, keystroke input from the target workstation user is not accepted. However, if the hot key combination is enabled for the target workstation, then the target workstation user can press the hot key combination and regain control of the target workstation. Then the target user can choose to change the session state (for example, from active state to monitoring state).

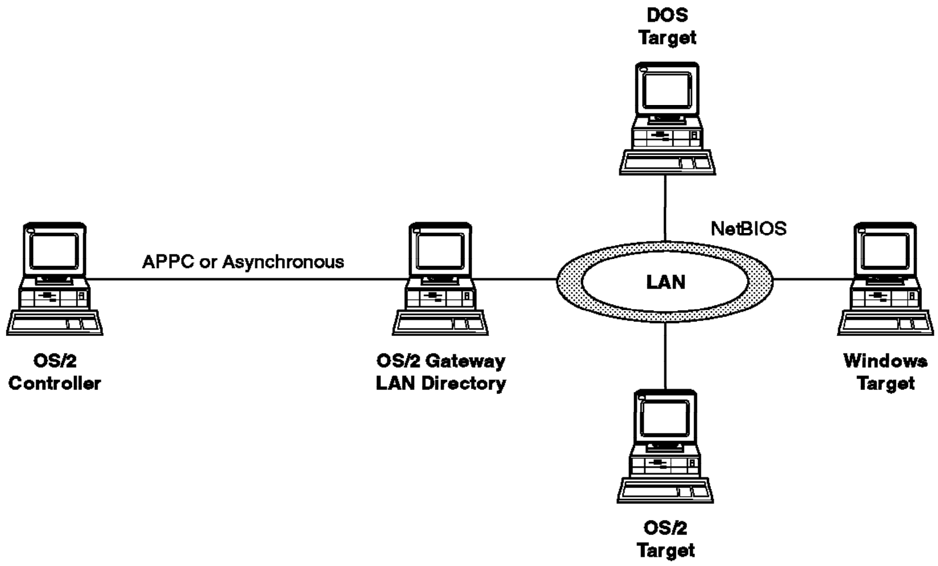
The controller can establish sessions with multiple target workstations at the same time and access them by switching to different windows. Although multiple controllers can be defined within the network, only one of them at a time can have a session with any single target workstation.

DCAF workstations can connect directly (as in Figure 1) or through a gateway (as in Figure 2).

PICTURE 1

Figure 1. Example of Direct Connection

Connections through the DCAF gateway can be established from a DCAF controller workstation to any kind of DCAF target (OS/2*, DOS, or Windows**).



PICTURE 2

Figure 2. Example of Connection through a DCAF Gateway

1.1.1 Benefits of Using the DCAF

DCAF is a tool for network management, network administration, network security, problem determination and diagnosis, and application assistance in the form of Help Desk functions. Its remote control capability can save time, money, and increase the productivity of your administrative and support personnel. You can centralize technical expertise at the controller sites and reduce the need for highly skilled personnel at remote locations. In addition, you can control unattended workstations remotely. Reduced operational requirements that can result from using the DCAF reduce costs and allow for faster growth for distributed applications within the distributed workstation environment.

DCAF′s centralized security administrator streamlines system management of a secure-session environment. DCAF helps protect your software assets by logging connections during secure-sessions. This keeps an auditing trail.

Here is a typical scenario of DCAF′s Help Desk function: Someone is having trouble starting the company′s new accounting program and contacts the help desk. The help desk person takes control of the workstation (target) and types the correct keystrokes to run the accounting program. The target user observes the controller′s input and learns how to start the new accounting program. The controller gives back control of the workstation, monitors the screen to be sure that the target user can work independently, and ends the session.

1.1.1.1 Some Examples of Using the DCAF

You can use Distributed Console Access Facility to:

- Control unattended PCs remotely
- Diagnose and solve problems on another PC by modem or over a LAN
- Manage Personal System/2* (PS/2)* workstations remotely and have access to data and programs stored on a PS/2 (for example, in the home or in the office)

- Run DOS, Windows**, and OS/2* on an unattended PC by modem or over a LAN
- Support customers and provide help remotely
- Transfer text and data between PCs
- View and control another PC

1.1.2 Understanding the DCAF Environment

DCAF offers two main levels of security, which limit users′ ability to take over your target workstations. These levels, basic DCAF (or nonsecure) and secure DCAF, offer protection for your workstations to varying degrees. For typical nonsecure environments that deal with non-confidential information, basic DCAF provides adequate protection. Secure DCAF is more complex and caters to environments, such as banks and insurance companies, that work with confidential material and require greater protection.

In order to be part of the DCAF environment, the workstations must have DCAF components installed. The role assigned to each workstation determines which components you install on the workstation.

1.1.2.1 The DCAF Components

Before you start with installation, you should be familiar with the DCAF components. The roles that each workstation has in your network determine the component that you install on it. All components, except targets, run on OS/2 workstations only.

You can install one or more components on the same workstation, but it is recommended that you install only the necessary components on each workstation. For example, on one workstation install a controller, on another, the gateway and LAN directory, and on a third, a target.

1.1.2.1.1 The Controller

The controller enables you to control the keyboard and mouse input and monitor the display output of a target workstation. It enables you to transfer files between the controller and target.

1.1.2.1.2 The Target

The target runs on three kinds of operating systems:

The OS/2 target enables an OS/2 workstation to be monitored and controlled by the controller. The controller connects to it directly if it is a basic DCAF target and through a gateway if it is secure.

The Windows target enables a Windows workstation to be monitored and controlled by the controller. The controller connects to it, whether it is operating in the DOS full-screen or in a Windows graphic environment. The controller connects to it directly if it is a basic DCAF target and through a gateway if it is secure.

The DOS target enables a DOS workstation to be monitored and controlled by the controller. To install the DOS target, either create an installation package or use the CID method. Use the packager on an OS/2 workstation to create a DOS target installation package and then, install the target on the DOS workstation. The controller connects to the DOS target directly if it is a basic DCAF target and through a gateway if it is secure.

1.1.2.1.3 The Gateway

The gateway links a controller with secure targets or with targets connected through a SNA backbone. The gateway always requires that you install a LAN directory on a workstation, any workstation, on the same LAN.

The gateway connects to all targets using the NetBIOS communication protocol. Therefore, install the gateway only in those parts of your network that use NetBIOS.

The gateway supports more than one session at a time so you probably need one gateway per logical LAN. To connect to secure targets, the gateway must be secure too.

1.1.2.1.4 The LAN Directory

The LAN directory provides a list of the targets on a LAN that are available to the controller. When the controller connects directly with the targets via IPX/SPX**, NetBIOS, or TCP/IP, the LAN directory is optional. When the controller connects with the targets through a gateway, the LAN directory is required.

Install one LAN directory per logical LAN. If you install more than one LAN directory on a logical LAN, give it a unique name.

The LAN directory also keeps a list that associates the workstation's physical address on the LAN with a nickname that make the target name easy to remember. It also enables the controller to find targets quickly. You can install the LAN directory on the target, gateway, if present, or any workstation on the same LAN as the target.

1.1.2.1.5 The Security Administrator

The security administrator is necessary for secure DCAF only. It provides centralized maintenance of the databases for controllers, target access tables, secure target workstations, and security authenticators. Install one security administrator, typically on a controller, for your whole network if you are using secure DCAF. Safeguard this workstation from unauthorized access.

The security administrator keeps an encrypted database of authorized users and an audit log file, EQNADMN.LOG. To be able to transfer security database files to the security authenticator, you must install either the security authenticator or a controller on the same workstation as the security administrator.

1.1.2.1.6 The Security Authenticator

The security authenticator is necessary for secure DCAF only. It authenticates sessions with secure targets. Gives access to secure targets, based on security profiles for authorized controllers that it receives from the security administrator.

Install the security authenticator on an OS/2 target on the same LAN. Install it either on the security administrator workstation or the secure OS/2 target workstation so that it can receive security information from the security administrator.

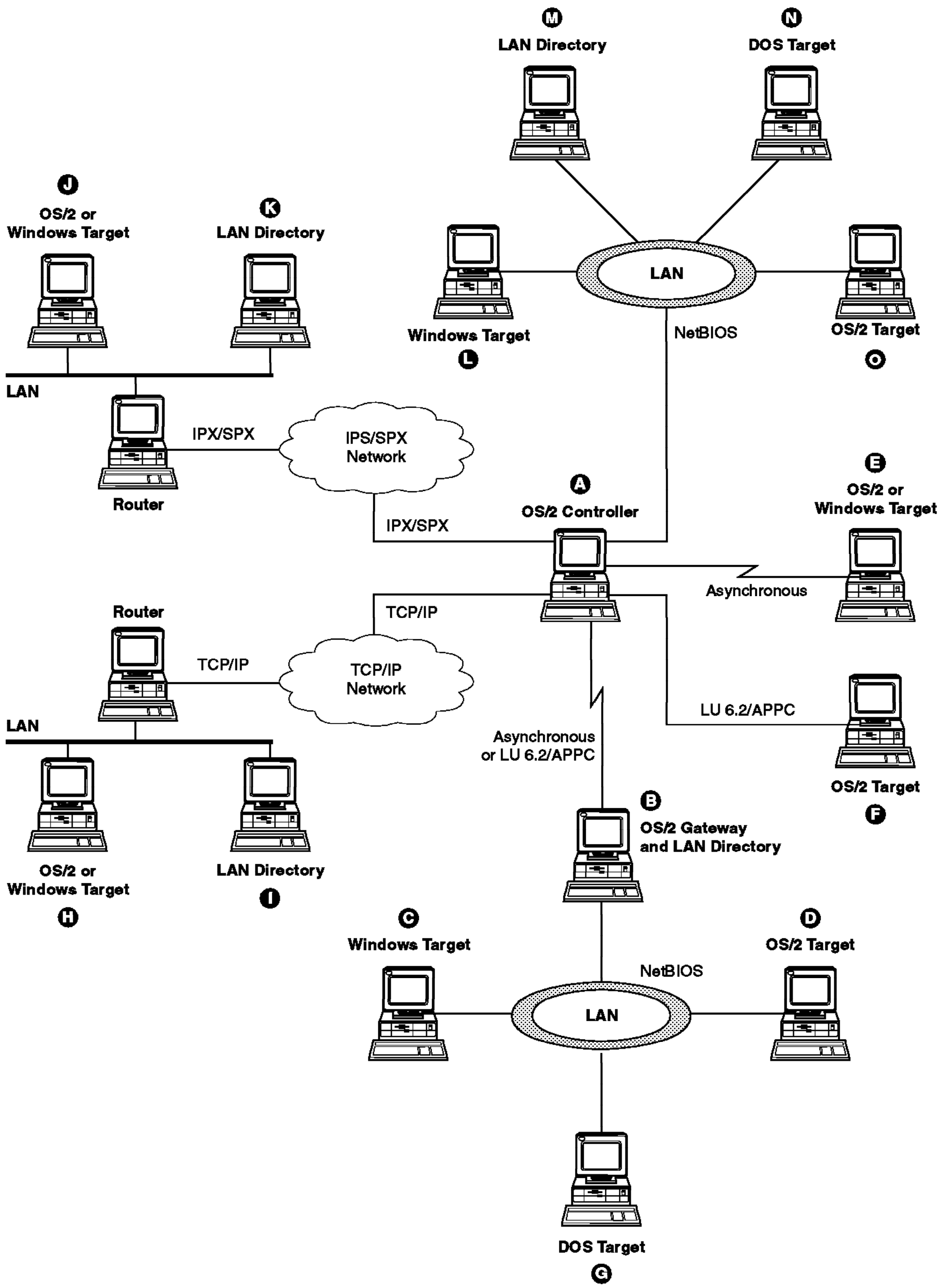
If you install the security administrator on the LAN, you can install the security authenticator on the same workstation. Install at least one security authenticator for each logical LAN in your network.

1.1.2.1.7 The Packager

The packager is an installation aid only. It creates installation packages of DCAF components that you can install on other workstations. In addition, it enables you to prepare a component with the same personalization features to be installed in large numbers all over your network. Always install DOS targets using the packager.

1.1.2.2 The DCAF Network

The DCAF network includes the workstations that have DCAF installed and the communications that link them together. Figure 3 is one example of a basic DCAF environment.



PICTURE 3

Figure 3. Example of a Distributed Console Access Facility Environment

The DCAF workstations communicate with the following communication protocols:

- Advanced Peer-to-Peer Networking* (APPN*)
- Advanced Program-to-Program Communication (APPC), more specifically

Logical Unit Type 6.2 (LU 6.2)

- Asynchronous (also called Asynchronous Communications Device Interface or ACDI)
- IPX/SPX (except for DOS targets)
- NetBIOS
- TCP/IP (except for DOS targets)

Controller **A** communicates directly with target **E** and with gateway **B** using switched asynchronous communications.

Controller **A** communicates also via LU 6.2 over a Systems Network Architecture (SNA) network or backbone through gateway **B** to the targets on the LAN. The SNA backbone represents the part of the network that connects (via switched lines, leased lines, or satellite communications) host computers, communication controllers, and other computer hardware. Any connections over a SNA backbone must go through a gateway.

Controller **A** communicates directly with target **F** via LU 6.2. For LU 6.2 communications, the physical unit type for the controller, target workstation, and DCAF gateway workstation must be configured as a type 2.1 (PU2.1).

Controller **A** communicates via TCP/IP through a router with LAN directory **I** and with target **H**.

Controller **A** communicates via IPX/SPX through a router with LAN directory **K** and with target **J**.

Controller **A** communicates via NetBIOS directly with LAN directory **M** and with targets **L, N,** and **O** on the LAN.

OS/2 target workstations on the LAN require that OS/2 Communications Manager, LAN adapter and protocol support (LAPS) from NTS/2, or the LAN Server 2.0 be installed to provide the NetBIOS device drivers. In order to run the DCAF with other applications that require NetBIOS services, you may need to increase the NetBIOS resources via the OS/2 Communications Manager or LAN Services.

DOS target workstations on the LAN require that a LAN support program be installed (such as the IBM LAN Support program). The DCAF supports DOS target workstations on the LAN only.

1.1.2.3 Levels of DCAF Security

DCAF offers the two main levels of security: basic (or nonsecure) and secure. Basic DCAF offers two simple levels of security:

- No password
- Password-only

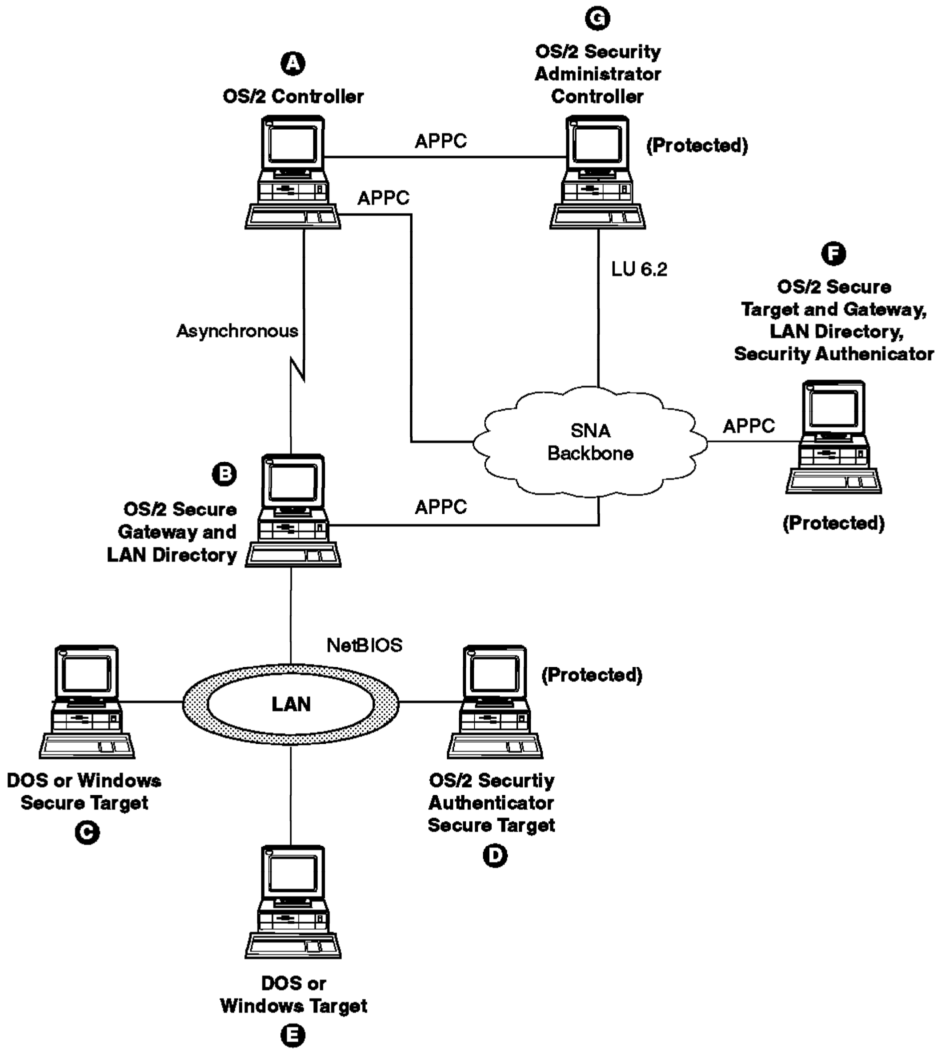
A session with no password is a session between a controller and a gateway or target workstation for which a password is not defined and, therefore, not necessary.

A password-only session is a session between a controller and a gateway or target workstation for which a password is defined. The controller must type the password before the session can be established.

In both cases, the target is installed as a basic or nonsecure target. Basic DCAF provides adequate protection for nonsecure environments that deal with non-confidential information.

Secure DCAF offers a higher and more advanced level of security for environments, such as banks and insurance companies, that work with confidential material. You can make a target almost impregnable to intruders by designating it as a secure target. The controller must access the secure target through a secure gateway. The secure workstations do not have a password. Instead, the controller, authorized for access to a secure controllable workstation, has a personal pass phrase (a compound password) and an access-level profile for a specific secure workstation.

DCAF security works only with the following communication connections: A controller can connect to a secure gateway via APPC/APPN or asynchronous. The secure gateway can connect to a secure target via NetBIOS only.



PICTURE 4

Figure 4. Example of DCAF Environment with Session Security

Figure 4 shows some workstations in a secure DCAF environment. The gateway can use only NetBIOS to communicate with the secure targets. Secure targets must be on a LAN (see targets **C** and **D** in Figure 4).

Controller **A** communicates via secure gateway **B** with the secure targets on the LAN. When the controller wants to take over secure target **C**, security authenticator **D** verifies that the controller is authorized to access that workstation.

DOS or Windows target **E** on the LAN is not secure and does not require authentication. It has password-only security. Controller **A** can also establish a session with secure target workstation **F**. Typically, the secure DCAF gateway, LAN directory, and security authenticator reside on target workstation **F**. In this case, controller **A** connects to gateway **F** via APPC, and gateway **F** connects internally to target **F** via NetBIOS.

The security administrator is installed (typically) on a controller workstation. It provides security file maintenance, a message log file, and control access information used by the DCAF security authenticators in a central location. Security files are transferred from the security administrator via a secure session to all of the remote security authenticators. Security administrator workstation **G** transfers new or updated security files to security authenticators **D** and **F**.

When the controller wants to change a pass phrase, the security authenticator verifies the authorization before a session is allowed and keeps a log file of the authentication activity. The verification compares the controller′s input with the security data stored on the security authenticator. The advantage of this mechanism is that there is no way to intercept or discover the pass phrase during transmission, because it sends the ciphered data only.

For auditing purposes, the gateway logs all session connections and the communication errors that it filters.

1.2 DCAF Requirements

This chapter describes all the requirements that you should consider in order to install the DCAF or to upgrade to this release.

1.2.1 Upgrading from Earlier Releases of the DCAF

DCAF 1.31 is compatible with workstations that have DCAF 1.1 with the latest Corrective Service Diskette (CSD) level and with DCAF 1.2 with the latest CSD level. If you install DCAF 1.31 on these workstations, DCAF installs the new version over the earlier version.

Exceptions:

1. Workstations on which DCAF Version 1.0 is already installedTcolon. first deinstall it and then install DCAF 1.31.

2. Windows targets from earlier releases: first deinstall DCAF and then install DCAF 1.31.

In all cases, you must use the controller from DCAF 1.31.

In order to use the DCAF's new features (see "Summary of Changes" in topic CHANGES) and to keep your DCAF environment uniform, it is recommended that you deinstall earlier versions and install DCAF 1.31.

1.2.1.1 Upgrading the Controller Database from Earlier Releases

If you are upgrading the controller to Version 1.31, DCAF provides a way to incorporate your existing database of workstations that are linked by the controller into the DCAF directory for the new controller. Perform the following steps:

1. Back up the EQNCOMM.DIR and EQNCOMM.DAT files on the controller workstation.

2. Upgrade the controller to Version 1.31 and copy the backup files to the same directory.

3. At the command prompt on an OS/2 full-screen, type **eqnutil** in the same directory in which the EQNCOMM files are installed.

DCAF converts the EQNCOMM files into the EQNLR.INI file.

Note: If you run EQNUTIL after having defined new workstations in the DCAF directory, EQNUTIL finds any workstation names that are duplicated in the DCAF directory and logs them in the EQNLR.LOG file. It does not update the duplicated workstations in the DCAF directory.

1.2.1.2 Upgrading DCAF Security to Work with DCAF Version 1.31

If you have any DCAF security databases, the utility EQNUPSDB.EXE reformats the EQNSCATH.MAS file from DCAF 1.1 and DCAF 1.2 for the DCAF 1.31 security administrator. Complete the following steps:

1. Back up the files in Table 2. They are in the directory that you specified (for Security data path) when you installed the DCAF security components. The default is C:\DCAF13.

Table 2. DCAF Security Files to be Copied in Backup Files before

Reinstalling

Component	Filetype	Security File
Security administrator	.MAS	EQNSCUSR EQNSCATH EQNSCTBL
	.TRG	EQNn1*
	.DAT	EQNSCPRM, EQNXFER
Security authenticator	.ATH	EQNSCUSR, EQNSCTRG

*DCAF numbers these files consecutively depending on how many security records you have in the database.

2. Then install DCAF 1.31 on the security administrator workstation.

3. At the command prompt from the security data path on the security administrator, type **EQNUPSDB**. The security database file EQNSCATH.MAS is updated. A message listing the number of successfully updated records appears.

1.2.2 Workstation Requirements for the DCAF 1.31

DCAF runs on hardware and software with the following requirements.

1.2.2.1 Hardware

DCAF 1.31 runs on hardware with the following characteristics:

- Any PC or Personal System/2* model currently supported by the operating systems listed under "Software" in topic 1.2.2.2

- Any communications hardware currently supported by the communications software listed under "Software" in topic 1.2.2.2

- Any modem supporting ACDI protocol for OS/2 workstations or IBM 7855 modem and Hayes-Smart modem for Windows workstations

- Any mouse supported by IBM OS/2 or any PS/2 fully compatible mouse for Windows

- LAN adapter

  - Supported by LAN Support Program
  - Adapter cards supported by Communications Manager

- Other

  - Extended IBM keyboard
  - AT*-compatible keyboard
  - Hayes**-compatible
  - IBM PS/2-compatible mouse
  - IBM 4755 Card Cryptographic Adapter
  - IBM 7855 modem
  - Hayes-Smart modem

1.2.2.2 Software

The DCAF supports the following software:

- Operating systems
  - OS/2 workstations run on IBM Operating System/2* Version 2.1 or later.
  - The Windows** target runs on Microsoft** Windows** Version 3.1x or Microsoft Windows for Workgroups Version 3.1x.
  - The DOS target runs on Disk Operating System (DOS) Version 6.3 or later or Microsoft DOS Version 6.2 or later.
- Communications software
  - For APPC/APPN or ACDI:
    - Communications Manager/2 1.10 or later
    - OS/2 Extended Services* Version 1.0, with refresh level WR06025, or later
  - For IPX/SPX:
    - Novell** NetWare** Requester for OS/2 Version 2.10 or later
    - Novell NetWare Requester for DOS/Windows Version 4.0 or later
    - Novell NetWare Server Version 3.12 or later
  - For NetBIOS:
    - For OS/2 workstations, IBM LAN Adapter and Protocol Support (LAPS) 2.13 or later, or IBM MultiProtocol Transport Services (MPTS) 1.0
    - For DOS and Windows targets, IBM LAN Support Program (LSP) Version 1.3 or later, or MS-LAN Manager 2.2
  - For TCP/IP:
    - IBM TCP/IP for OS/2 Version 2.0, with refresh level UN64092, or later
    - IBM TCP/IP for DOS/Windows Version 2.1.1 or later
    - Microsoft TCP/IP & Data Link Control for Windows for Workgroups 3.1x
    - Novell LAN WorkPlace for DOS Version 4.2 or later

1.2.3 Requirements for the SNA Network Backbone

For DCAF 1.31 to interface with the SNA backbone, the requirements are:

1. DCAF controllers, DCAF gateway workstations, and directly connected OS/2 target workstations must be configured as a physical unit type 2.1 (PU2.1). If the DCAF workstation is downstream from a 3174 control unit, then the 3174 must have either Configuration Support B plus 8Q0800 Programming Request for Price Quotation (PRPQ) or Configuration Support C (APPN* feature).
2. VTAM* 3.2 (or later) and NCP 4.3 (or later) on 3725.
3. VTAM 3.2 (or later) and NCP 5.2 (or later) on 3720 and 3745.

1.2.4 Communication Configuration Requirements for the DCAF 1.31

Some communication configuration requirements for DCAF workstations are:

- Controllers that use an asynchronous connection need a device string profile that is compatible with the OS/2 ACDI services.
- DCAF gateways and direct connections to target workstations use the same adapter/modem configurations as the controllers.
- Targets on the LAN must have the normal LAN adapter that is required to connect to the LAN. All secure targets require a LAN adapter.

1.2.5 Hard Disk Space and RAM Requirements for the DCAF 1.31

Table 3 shows the hard disk space and RAM memory requirements for each DCAF component. These requirements for the OS/2 target vary depending on the communications protocol that it uses. The list includes values for each protocol.

Table 3. Hard Disk Space and RAM Requirements by Component

Component	**Hard Disk Space (KB)**	**RAM (KB)**
Controller	1800	600
DCAF Gateway	1050	450
LAN Directory (IPX/SPX)	1150	380
LAN Directory (NetBIOS)	1150	280
LAN Directory (TCP/IP)	1150	340
Security Authenticator	1300	600
Security Administrator	1500	800
Packager	2200	500
OS/2 Target (APPC/APPN)	1700	680
OS/2 Target (ACDI)	1700	580
OS/2 Target (IPX/SPX)	1700	500
OS/2 Target (NetBIOS)	1700	380
OS/2 Target (TCP/IP)	1700	600
DOS Target	100	40
Windows Target (IPX/SPX)	600	380
Windows Target (NetBIOS)	600	250
Windows Target (TCP/IP)	600	200

1.2.6 How to Order the DCAF

To order the Distributed Console Access Facility 1.31 product in the United States, Asia, and the Pacific:

Table 4. How to Order DCAF 1.31 in IBM United States, Asia, and the Pacific

Order Number	Part Number	Feature number	Language
5871-BBB	79G0466	6683	English Version

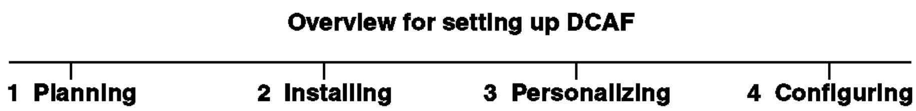
To order the Distributed Console Access Facility 1.31 product in Latin America, Canada, Europe, the Middle East, and Africa:

Table 5. How to Order DCAF 1.31 in IBM Latin America, Canada, Europe, Middle East, and Africa

Order Number	Part Number	Language
5622-212	79G0466	English Version

1.3 Setting Up the DCAF

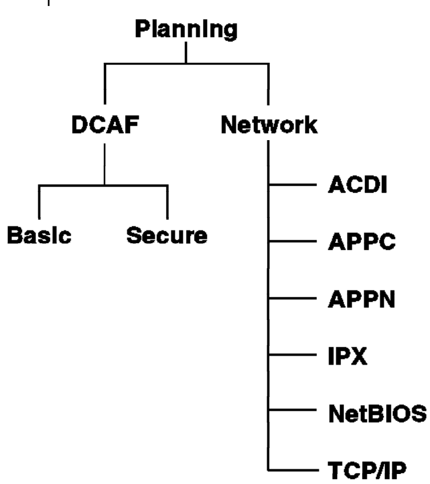
The following diagram (Figure 5) provides an overview of the main tasks for setting up the DCAF. It breaks down planning into four sequential tasks: planning, installing, personalizing, and configuring. Plan each of these tasks in advance to minimize disruption to your user community.



PICTURE 5

Figure 5. Overview of the Four Main Tasks in Setting Up DCAF

1.3.1 Planning



PICTURE 6

Figure 6. Planning for DCAF

Consider two aspects of planning: the DCAF components that you need for your network and your network topology.

- Does it need basic DCAF or additional DCAF security?

- How many help desks (controllers) and how many help desk callers (targets) does it need?

- Which communications protocols does it use and in which combinations?

- Where in relation to your help desk are your help desk callers?

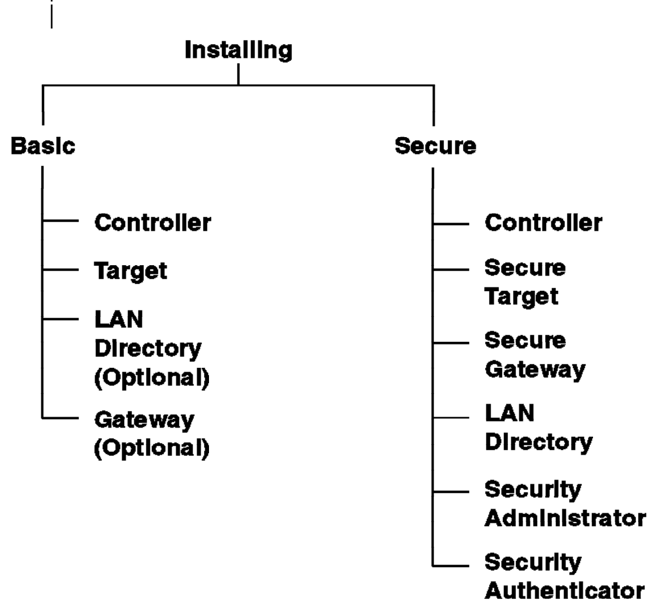
You can install one or more components on a workstation depending on the role that you assign the workstation in the network. See ″Understanding the DCAF Environment″ in topic 1.1.2 for a description of the DCAF environment and the roles of the different components. See ″Levels of DCAF Security″ in topic 1.1.2.3 and ″Installing the Security Administrator and Authenticator″ in topic 2.1.1.4 for details on installing DCAF security in the network.

Install only the necessary components on each workstation. For example, on one workstation install a controller, on another, the gateway and LAN directory, and on a third, a target.

See ″DCAF Fundamentals″ in topic 1.1, and ″Installing the DCAF on OS/2 Workstations″ in topic 2.1, for more information.

1.3.2 Installing

This section describes the components that you should install for basic and for secure DCAF as shown in Figure 7.



PICTURE 7

Figure 7. Installing DCAF

1.3.2.1 For Basic DCAF

For the simplest basic DCAF structure, you need the controller and target. More complex, if the same controller accesses many targets on a LAN, the LAN directory is convenient but not required. The LAN directory provides the controller with a list of targets that are available for a particular communication protocol. Install the LAN directory on the same or any workstation on the same LAN as the targets.

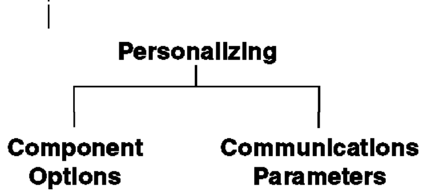
Finally, if your controller connects to targets on a LAN through a gateway, including through a SNA backbone, install the gateway and the LAN directory. Install them on the target workstation or on any workstation on the same LAN as the target. Install these components in the proportions appropriate for your network.

1.3.2.2 For Secure DCAF

For additional security, install the components recommended in "For Basic DCAF." However, install (or reinstall) a <u>secure</u> target. In addition, install a secure gateway, a LAN directory, the security administrator, and a security authenticator.

Install the authenticator on a secure target workstation on the same LAN as the secure target. Install a secure gateway for every LAN on which a secure target resides. Install the administrator on a controller workstation. Install these components in the proportions appropriate for your network. However, install only one administrator for your secure network.

1.3.3 Personalizing



PICTURE 8

Figure 8. Personalizing DCAF

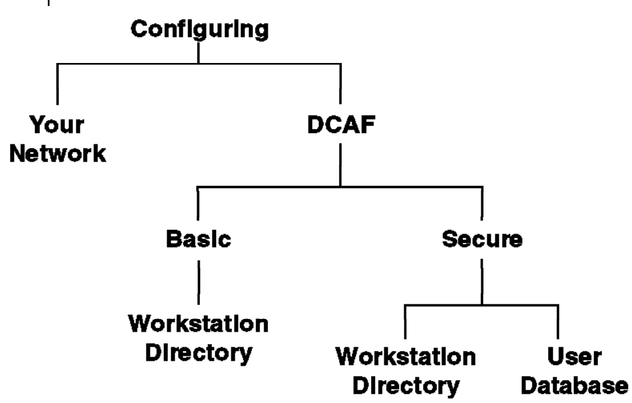
There are two kinds of personalization:

- Component options, for example, the size of the target screen that the controller sees

- Communications parameters, for example, which protocol the controller uses to connect to a particular target.

You can personalize some options during installation only and others while you work on the workstation. See "Personalizing the DCAF Controller and Other Components" in topic 2.7, for more information.

1.3.4 Configuring



PICTURE 9

Figure 9. Configuring DCAF

Configure two things: your communications network and the DCAF. Configure your communications network to identify connecting workstations to one another. See "Configuring" in topic 3.0, for more information.

For basic DCAF, identify to the controller workstation directory the workstations that the controller takes over (see "Adding a Workstation" in topic 3.18.1).

For secure DCAF, identify to the controller workstation directory the workstations that the controller takes over and define user profiles in the security user database for the controllers authorized to access secure targets (see "DCAF Security" in topic 4.0).

2.0 Installing and Personalizing the DCAF

Install the DCAF with one of the following methods:

- Directly from the product diskettes. You can use this method for any of the components, except DOS targets. For instructions, see "Installing Directly (OS/2 Workstations Only)" in topic 2.1.1.

- Using a DCAF installation package, created with DCAF. You can use this method for any of the components, except security administrators and authenticators. Use this method for all DOS targets. For instructions, see "Installing with an Installation Package for OS/2 and DOS" in topic 2.2.

- Using the Configuration/Installation/Distribution (CID) method. You can use this method for all the components.

  If your network has unattended workstations and uses distribution software, use this method. For instructions, see "Installing the DCAF Using the CID Method" in topic 2.4.

- Using CD. You can use this method for all the components, except DOS targets. For instructions, see "Installing the DCAF from a Compact Disc (CD) and from a Remote File Server" in topic 2.5.

- Directly from a remote file server. For instructions, see "Installing the DCAF from a Compact Disc (CD) and from a Remote File Server" in topic 2.5.

2.1 Installing the DCAF on OS/2 Workstations

This chapter provides instructions for installing the following components. For instructions about installing the Windows target, see "Installing the Windows Target" in topic 2.3.

- Controller
- Gateway
- LAN Directory
- Packager
- Security administrator
- Security authenticator
- OS/2 target

2.1.1 Installing Directly (OS/2 Workstations Only)

Read "DCAF Fundamentals" in topic 1.1 and "Setting Up the DCAF" in topic 1.3 as a prerequisite to installing DCAF.

For instructions on installing the Windows target, see "Installing the Windows Target" in topic 2.3. For details on installing the DOS target, see "Installing with an Installation Package for OS/2 and DOS" in topic 2.2.

Note:

- If DCAF is already installed, make sure that it is not running before you begin a new installation.

- When you are using the same DCAF diskettes to install personalized components on more than one workstation, be sure to complete one installation process before starting another. Otherwise, you can inadvertently transfer the personalization options for a given component from one workstation to another.

- Be sure that the CONFIG.SYS file is closed before you begin, so that any changes made in this file during installation will be saved.

2.1.1.1 Choosing the Components

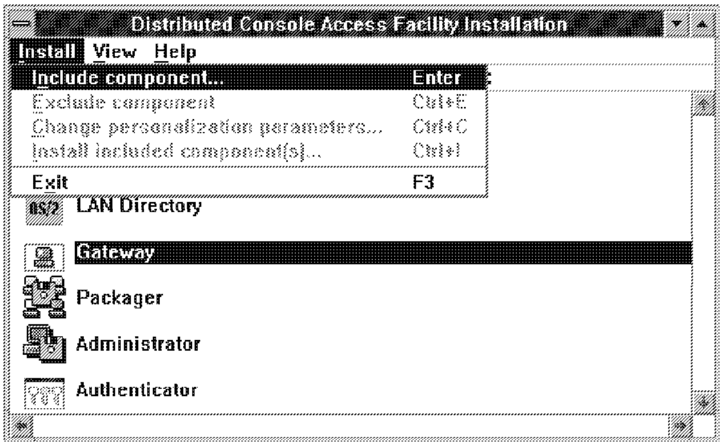
When you install directly, choose the workstation on which you want to install one or more components and begin to install. If you want to add other components after you first install, repeat these steps and DCAF adds the components you install to the components that are already installed on the workstation. To install the DCAF product from the product diskettes onto an OS/2 workstation, perform the following steps:

1. Switch to an OS/2 command prompt.

2. Insert the DCAF product diskette 1 into drive A of the workstation.

3. Type **A:INSTALL**. The DCAF Logo window appears. Press the **OK** push button.

   If DCAF Version 1.0 exists on the workstation, a message appears asking for confirmation to deinstall it and then install DCAF 1.31. Otherwise, DCAF stops installation. If a different version (1.1 or 1.2) of DCAF exists on the workstation, a message appears asking for confirmation to install the DCAF program over the previous version in the same directory. Press **Yes**.



PICTURE 10

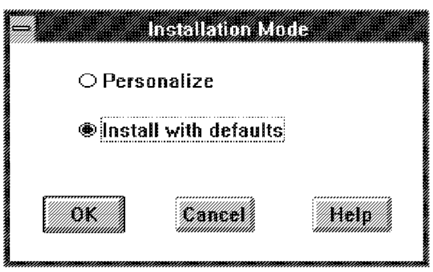
Figure 10. DCAF Installation Main Window

4. The DCAF Installation Main window (Figure 10) appears. It displays a list of components that can be installed on your workstation. Select the DCAF component with the keyboard or mouse. Then choose **Include component...** from the Install pull-down menu. Repeat this process for each component that you want to install.

   If you are not sure which components you should install, see "The DCAF Components" in topic 1.1.2.1 for a description.

   If you decide not to install a highlighted component after you have included it, choose **Exclude component** from the Install pull-down menu. If the component has been personalized, then the last saved personalization information is kept.

   The Installation Mode window (Figure 11) appears.



PICTURE 11

Figure 11. DCAF Installation Mode

5. You can personalize the component or install it with the default options.

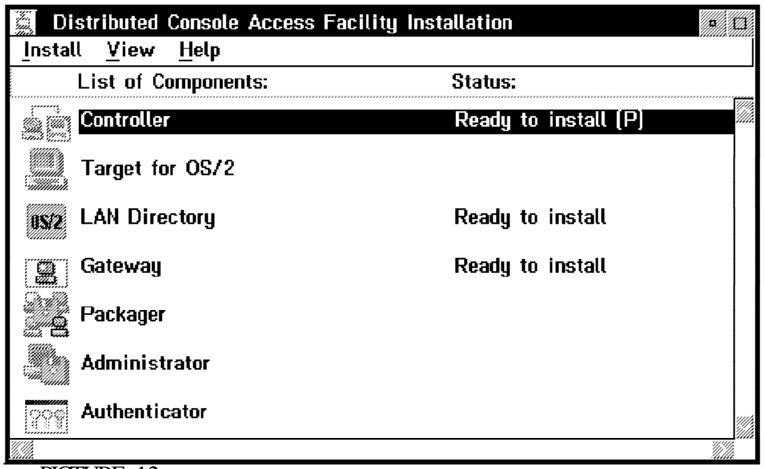
   If you are installing a secure target or gateway, you must personalize it to make it secure. You can choose **Change personalization parameters...**from the Install pull-down menu to personalize it later. The default values for each component are described in "Personalizing the DCAF Controller and Other Components" in topic 2.7. The components that can be personalized during direct installation are:

   - Controller (See page 2.7.1.)
   - Target for OS/2 (See page 2.8.1.) For a secure target, select Personalize.
   - LAN directory (See page 2.7.2.)
   - Gateway (See page 2.7.3.) For a secure gateway, select Personalize.

Press the OK push button after making your choice.

The security administrator and the security authenticator are the security components for secure DCAF sessions. These components can be installed directly or using the CID method. However, you cannot install them using the packager. See "Installing the Security Administrator and Authenticator" in topic 2.1.1.4.

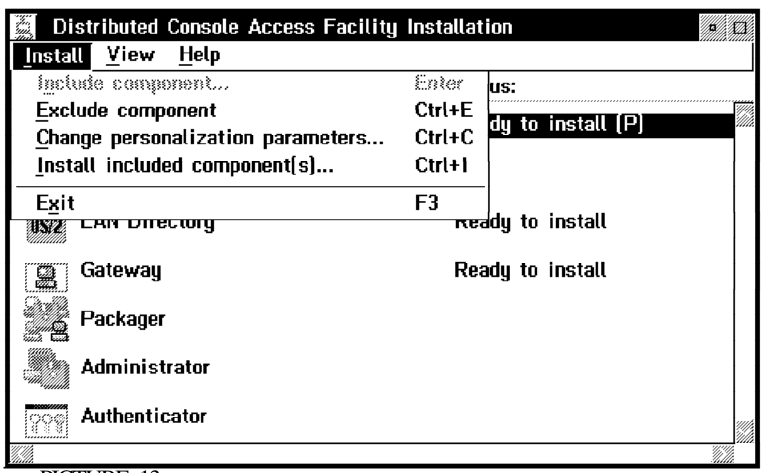
2.1.1.2 Installing the Components



PICTURE 12

Figure 12. DCAF Installation Main Window with Components Ready to Install

1. When the components are included, their status is displayed as "Ready to install." In Figure 12 the (P) indicates that the component has been personalized.

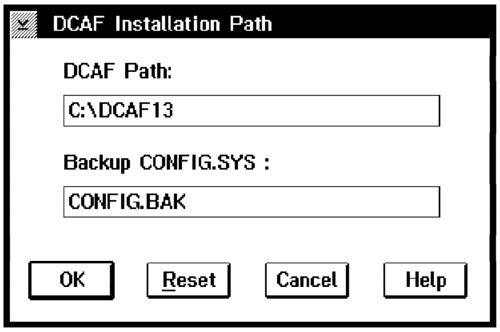


PICTURE 13

Figure 13. DCAF Installation Main Window

2. Under **Install** in the pull-down menu, choose **Install included components** (or the Ctrl+I shortcut key) as shown in Figure 13. DCAF installs all the components that you have selected simultaneously.

   If you have included the security administrator or the security authenticator, you will now be asked for additional information. See "Installing the Security Administrator and Authenticator" in topic 2.1.1.4, for the steps to install these components.



PICTURE 14

Figure 14. DCAF Installation Path

3. The DCAF Installation Path window (Figure 14) appears. You can specify the DCAF path where the DCAF product will be installed. If the directory that you specify does not exist, then the directory will be created on the workstation's fixed disk.

   Type in the path where you want the DCAF product installed or select the default path (C:\DCAF13).

   - The path is 1-50 characters in length.
   - For character guidelines, follow OS/2 conventions for the path.

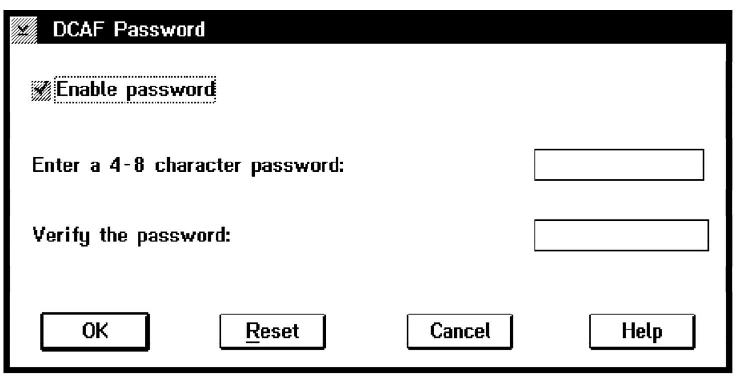
   Type in the backup name for the CONFIG.SYS file.

   - Follow OS/2 file name conventions.

   - The format of the file name depends on whether your hard disk has been formatted with HPFS or FAT.

   - The default is CONFIG.BAK.

   Press the **OK** push button when you have entered all the information.

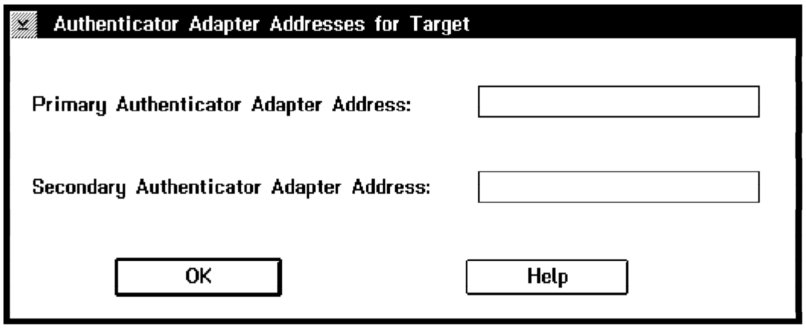


PICTURE 15

Figure 15. DCAF Password

4. If you included the target or gateway, you will be prompted with the DCAF Password window (Figure 15) for target workstations or DCAF gateway workstations. If you press **OK** without typing a password, then you have a nonsecure session (neither password-only security nor secure-session security). If you mark the check box, **Enable password**, then you can type your password.

   The password is 4-8 characters in length and must include at least four alphanumeric characters. Blanks after the last alphanumeric are ignored. Retype the same password exactly in the **Verify the password** field.



PICTURE 16

Figure 16. Authenticator Adapter Addresses for Target

5. If you choose a secure target, the Authenticator Adapter Addresses for Target window (Figure 16) appears.

   The secure target uses the adapter address to identify which security authenticators are authorized to start secure sessions with that target. Type the adapter address for a primary and secondary (backup) security authenticator for the target. For more details about the primary and secondary authenticators, see "About the Security Components" in topic 4.1.1. To get the adapter address, check the LANTRAN.LOG file in the IBMCOM directory on the authenticator workstations. The primary and secondary security authenticators can be the same.

   The security authenticator adapter address must be exactly 12 hexadecimal in length, including:

   - Upper- or lowercase letters (A-F, a-f)
   - Digits (0-9)
   - Blanks not allowed

   Press the **OK** push button when you have typed all of the information.

The DCAF will now install. You will be instructed which DCAF product diskette(s) to insert to complete the installation. If errors occur, then you will be instructed what to do. When the installation is complete and no errors occur, you will receive the following message:

   Installation of the DCAF is successful.
   Before running the DCAF, configure the
   communications, shut down, and then
   restart the workstation.

2.1.1.3 After You Install

After the DCAF product has been installed successfully, exit the installation process by pressing the **OK** push button. Configure the communications protocol on which the workstation will run the DCAF. For instructions on configuring the communications, see "Configuring" in topic 3.0. Then shut down and restart the workstation.

2.1.1.4 Installing the Security Administrator and Authenticator

Before you start, plan where you want to install DCAF security. See "Levels of DCAF Security" in topic 1.1.2.3 and the introduction to "Setting up Secure DCAF Sessions" in topic 4.2.

If the security administrator is already installed and you later decide to install the security authenticator on the same workstation, perform the following tasks:

- Reinstall both the security administrator and the security authenticator (with a new master key and KEK).

- Update the information in the security databases.

  - For the Security Authenticators database, retype the KEK for each remote security authenticator.

  - For the Controller Workstation Users database, retype the pass phrase for each user.

Do the same for the security authenticator.

Access to the security administrator and security authenticator workstations should be restricted to the personnel who are authorized to administer the security system.

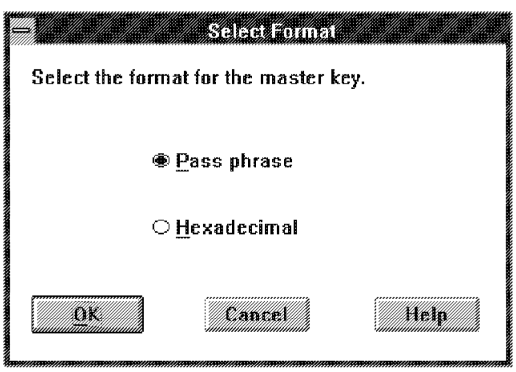
The **Cancel** push button is disabled during the installation of the security administrator and the security authenticator. You cannot close the window, because all of the requested security information is required. To interrupt the installation, close the DCAF installation program.

If you do not have the 4755 Cryptographic adapter card installed on the workstation (you are prompted with a message), continue the installation process with "Installing without the 4755 Cryptographic Adapter Card" in topic 2.1.1.4.1. If you do have the adapter card installed on the workstation (for the security administrator and security authenticators components), then the installation continues with "Supplying the Format for the Key-Encrypting Key" in topic 2.1.1.4.2. The cryptographic card must be initialized and ready to operate before you install the DCAF. For more information see Workstation Security Services Installation and Operating Guide, SA34-2141.

If the security administrator and the security authenticator are installed on the same workstation (typically an OS/2 workstation on the LAN), then this security information is supplied once and it is used by both components.

2.1.1.4.1 Installing without the 4755 Cryptographic Adapter Card

If you do not have the 4755 Cryptographic adapter card installed, the installation starts here. If you do, skip to "Supplying the Format for the Key-Encrypting Key" in topic 2.1.1.4.2.



PICTURE 17

Figure 17. Select Format for Master Key

1. On the Select Format for master key window (Figure 17), choose the format for the master key. The format for the master key can be either of the following:

- A pass phrase (4-80 characters). The master key is created from the Pass phrase.

- A hexadecimal string (exactly 32 hexadecimal characters). The master key is the exact value of the hexadecimal string.

Press the **OK** push button after choosing the format for the master key.

PICTURE 18

Figure 18. Set Master Key with Pass Phrase Format

2. If you select Pass phrase, then the Set Master Key window (Figure 18) appears. Type your pass phrase in the **Key** field. Type your pass phrase a second time, in the **Key confirmation** field.

   The pass phrase is 4-80 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0-9)
   - Special characters: #, @, $, or blank

   Press the **OK** push button after confirming your pass phrase.

PICTURE 19

Figure 19. Set Master Key with Hexadecimal Format

3. If you choose **Hexadecimal** then the Set Master Key window (Figure 19) appears. Type your hexadecimal string in the **Key** field. Type your hexadecimal string a second time, in the **Key confirmation** field.

   The hexadecimal string is exactly 32 characters in length, including:

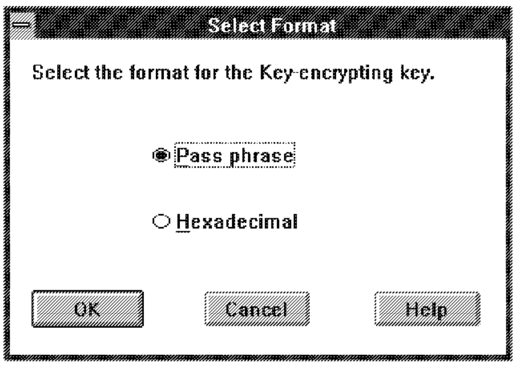
   - Upper- or lowercase letters (A-F, a-f)
   - Digits (0-9).

   Press the **OK** push button after confirming your hexadecimal string.

You continue the installation by supplying the information for the key-encrypting key (KEK).

2.1.1.4.2 Supplying the Format for the Key-Encrypting Key

If you have the 4755 Cryptographic adapter card installed, the installation process starts here.



PICTURE 20

Figure 20. Select Format for Key-Encrypting Key

1. On the Select Format for Key-encrypting key window (Figure 20), choose the format for the key-encrypting key (KEK). The format for the KEK can be either of the following:

   - A pass phrase (4-80 characters). The KEK is created from the pass phrase.

   - A hexadecimal string (exactly 32 hexadecimal characters). The KEK is the exact value of the hexadecimal string.

   Press the **OK** push button after choosing the format for the KEK.

PICTURE 21

Figure 21. Set Key-Encrypting Key with Pass Phrase Format

2. If you choose Pass phrase, then the Set Key-encrypting Key window (Figure 21) appears. Type your pass phrase in the Key field. Type your pass phrase a second time in the **Key confirmation** field.

   The pass phrase is 4-80 characters in length, including:

   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0-9)
   - Special characters: #, @, $ or blank

   Press the **OK** push button after confirming your pass phrase.

PICTURE 22

Figure 22. Set Key-Encrypting Key with Hexadecimal Format

3. If you choose **Hexadecimal**, then the Key-encrypting Key window (Figure 22) appears. Type your hexadecimal string in the **Key** field. Type your hexadecimal string a second time, in the **Key confirmation** field.

   The hexadecimal string is exactly 32 characters in length, including:

   - Upper- or lowercase letters (A-F, a-f)
   - Digits (0-9)

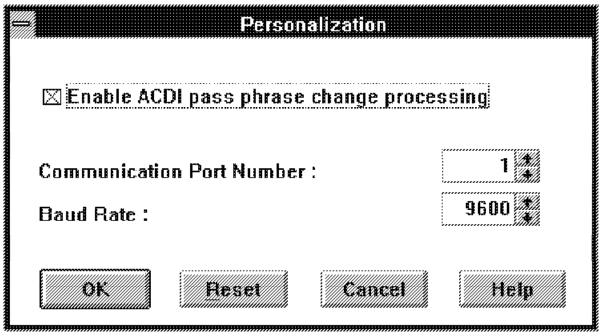
   Press the **OK** push button after confirming your hexadecimal string.

Note: The KEK for the security authenticator must match the same KEK that is typed on the security administrator workstation, when you are adding security authenticators to the security authenticator database. See adding security authenticators in ″Creating the Security Authenticator Database″ in topic 4.2.1.5.

If you are installing the security administrator on the same OS/2 workstation as the security authenticator (on the LAN), then the security authenticator workstation is being <u>locally administered</u>. If you are installing the security administrator on a controller workstation and the security authenticator on an OS/2 target workstation (for example on the LAN), then the security authenticator workstation is being <u>remotely administered</u>. Installation of the security authenticator (both remotely and locally administered) continues with ″Completing Security Authenticator Installation Information″ in topic 2.1.1.4.4.

The installation for the security administrator continues with ″Completing Security Administrator Installation Information″ in topic 2.1.1.4.3.

2.1.1.4.3 Completing Security Administrator Installation Information



PICTURE 23

Figure 23. Security Administrator Personalization

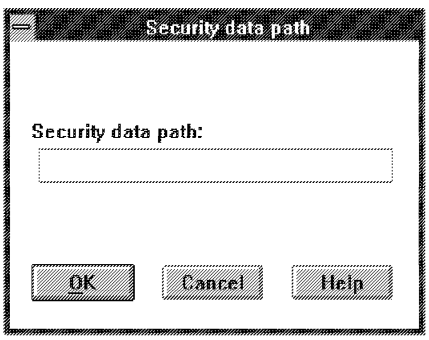
You can customize the three ACDI communication parameters for the security administrator as shown in Figure 23.

1. If you mark the check box, then you enable pass phrase changes for the ACDI communication. You must mark this box to be able to change the other parameters.

2. Choose the communication port number for the asynchronous serial port where the modem is attached. The values are 1-3.

3. Choose the baud rate (modem transmission rate). The choices are 1200, 2400, 4800, 9600, 19200. The default is 9600.

Press the **OK** push button after personalizing the options.



PICTURE 24

Figure 24. Security Administrator Data Path

To complete the installation of the security administrator that is remotely administering the security authenticator workstation, the Security data path window (Figure 24) appears.

Type the security data path where the security data files will be stored on the security administrator. The data files include the databases for the security authenticators, the target workstation access tables, and for the controller users. Specify a path that the security authenticator can access (for example, C:\DCAF13).

- The data path can be any valid path up to 50 characters in length.
- Blank spaces are not allowed between characters.
- For character guidelines, follow the OS/2 conventions for paths.

Press the **OK** push button after typing the data path.

2.1.1.4.4 Completing Security Authenticator Installation Information

To complete both the locally and remotely administered security authenticator installation, continue with the following steps.

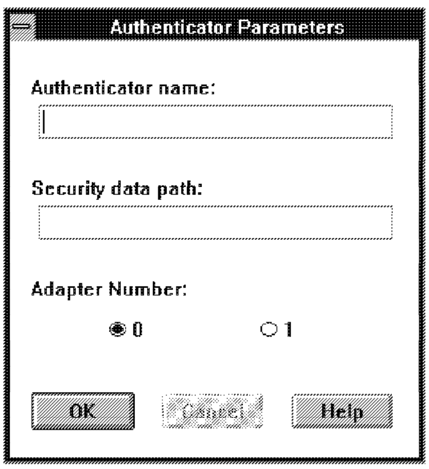
2.1.1.4.5 Security Authenticator Installation without a 4755 Cryptographic Adapter Card

If you do not have the 4755 adapter installed on the security authenticator workstation (for both locally and remotely administered authenticators), then you must supply input for the **Random Seed Values** window (not shown).

- The input to create the random seed for the random number generation is required for the four input fields.
- Type eight or more characters in each of the four input fields.
- The four input fields do not have to be the same.
- You must pause at least 1/2 second between keystrokes, or the keystrokes will not be registered.

Press the **OK** push button when you have completed typing the information.

2.1.1.4.6 Security Authenticator Installation



PICTURE 25

Figure 25. Authenticator Parameters

The Security Parameters (or Authenticator Parameters) window (Figure 25) appears. You must supply information for the following three fields:

1. Type the authenticator name of the unique DCAF security authenticator.

   - The authenticator name can be 1-12 characters in length.
   - Any character is valid except a single (*) or all blanks.
   - It is not case sensitive even if it appears in uppercase.

   Note: The name for the security authenticator typed here must match the security authenticator name typed during the personalization of the DCAF gateway.

2. Type the path (for example, C:\DCAF13) where the security data files will be stored on the security authenticator.

   - The data path can be any valid path up to 50 characters in length.

- For character guidelines, follow the OS/2 conventions for path.

Note: This data path must match the same data path that is typed on the security administrator workstation, when you are adding security authenticators to the security authenticator database.

3. Choose the LAN adapter number. It can be 0 or 1. The default is 0.

Press the **OK** push button when you have typed the information.

2.1.1.5 After You Install

You have completed installation of the security components. Configure the communications. Then set up the security user database. See "Setting up Secure DCAF Sessions" in topic 4.2.

2.1.2 Deinstalling the DCAF

To remove DCAF from an OS/2 workstation, choose Distributed Console Access Facility from the desktop, and then choose **Deinstall the DCAF**. A warning message appears:

```
WARNING: DCAF is going to be deinstalled.
         Press Y to continue deinstallation, or
         any other key to exit.
```

If you press Y, then the deinstallation begins.

On the OS/2 full screen, the message appears:

```
Updating the CONFIG.SYS...
```

This means that all of the statements that were added to the CONFIG.SYS when the DCAF was installed, are being removed. Later, the message appears:

```
Deleting the DCAF group...
```

This means that DCAF is being removed from the desktop. Following this message is a list of the files that are being deleted. When the deinstallation is complete, the message appears:

```
Deinstallation completed successfully.
Now shut down the machine.
Press Enter to exit...
```

To deinstall without entering confirmation to proceed on a remote workstation, you must specify a parameter. To specify the parameter for remote deinstallation, follow these steps:

1. Open the Deinstall the DCAF group folder.
2. Select **Settings**.
3. Select **Program**.
4. For Parameters, type **/n**.
5. Close.

If you deinstall the Distributed Console Access Facility while there are some DCAF components running on your workstation, you may find that the process log files for those components will remain in the DCAF directory on your workstation. These files will not interfere with future installations of the DCAF. However, you can delete them, along with the DCAF directory, from your workstation. To avoid this problem, be sure to stop DCAF completely on your workstation before deinstalling the Distributed Console Access Facility.

If the security data path for the security administrator (Figure 24 in topic 2.1.1.4.3) and the security authenticator (Figure 25 in topic 2.1.1.4.6) is not the same as the path where the DCAF product is installed, then the security information files will not be deleted.

It may happen that after shutting down and restarting the workstation, the DCAF directory still remains. This occurs if there are log files or other files that you copied to the directory and they are not recognized by the DCAF product. Even if the directory is present, the DCAF product has been removed successfully.

To deinstall the Windows target, see "Deinstalling the Windows Target" in topic 2.3.4.

2.1.3 Changing Operating Systems

The way that you install the DCAF product depends on the operating system that is running on the workstation and the DCAF internal support necessary for that particular operating system. This means that when you change operating systems on a workstation where DCAF is installed you must deinstall and then reinstall it on the new operating system. Remember to perform any personalization that is required.

2.1.4 Supporting Multiple Operating Systems for the DCAF

If two operating systems are installed on the same workstation, then the DCAF components must be installed twice (once for each operating system). The DCAF product is installed on each operating system separately while the operating system is running. It is important that you install DCAF in unique installation paths for each operating system that you use.

2.2 Installing with an Installation Package for OS/2 and DOS

You can use the installation package to install the DOS target and the following OS/2 components:

- Controller
- Gateway
- LAN Directory
- OS/2 target

The packager can make your job easier by packaging the components along with the personalization options. For the DOS target, using an installation package is required. For the OS/2 components, it is not. However, you must package OS/2 and DOS components separately.

The OS/2 workstation that you use to create the installation package must have the DCAF packager installed. See "Installing Directly (OS/2 Workstations Only)" in topic 2.1.1, for instructions on installing the packager.

You can select online window help at any time while creating an installation package. To display the help window, press the **F1=Help** key or select the **Help** push button when it is displayed. To exit the Help window, press **Esc**.

2.2.1 Creating an Installation Package

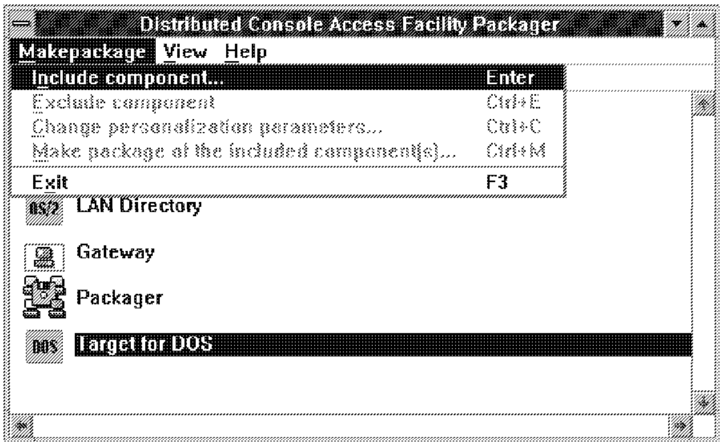
> **Important Information**
>
> Be sure to create the DCAF package on a workstation running on the same operating system level as the workstations where you plan to unpack and install the DCAF package.

For example, if you have DOS workstations in your network, you must create an installation package and save it on a diskette by using an OS/2 workstation on which the packager is installed. Then you can use that installation package diskette to install the DCAF product on all the DOS workstations in the network.

To create an installation package, perform the following steps.

1. From the Desktop Manager menu, choose the **Distributed Console Access Facility** group. The Group - DCAF menu appears.

2. From the Group - DCAF menu, choose **Packager for the DCAF**.



PICTURE 26

Figure 26. DCAF Packager

3. The Distributed Console Access Facility Packager window (Figure 26) appears. Select the DCAF component, and then choose **Include component...** from the Makepackage pull-down menu. Repeat this process for each component that you want to include in the package.

   Note:

   - Do not include the packager in a package to be stored on a diskette.

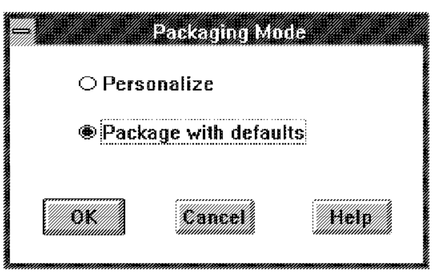
   - For the Target for OS/2, be sure to create the installation package on a workstation that runs on the same level of operating system as the workstation where you will install the package.

   If you decide not to package a highlighted component after you have included it, choose **Exclude component** from the Makepackage pull-down menu. If the component has been personalized, then the last saved personalization information is kept.

   The components for the package are the same as the components for installing directly, with two exceptions:

   - You cannot install the target for DOS directly. Install it using either the packager or the CID method.

   - You cannot install the security administrator and security authenticator using the packager. Install them either directly or using the CID method.



PICTURE 27

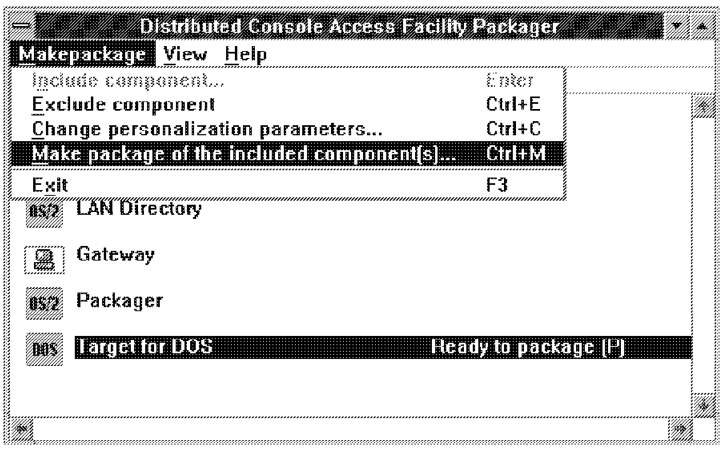
Figure 27. Packaging Mode

4. When you choose each component that can be personalized, the Packaging

Mode window (Figure 27) appears. You can choose to personalize the information for that particular component or accept the default options. You can also choose **Change personalization parameters...** from Makepackage on the pull-down menu for any component that has been included. See "Personalizing the DCAF Controller and Other Components" in topic 2.7, for instructions for personalizing the components or choosing their default values. The components that can be personalized for an installation package are:

- Controller (See page 2.7.1.)
- Target for OS/2 (See page 2.8.1.) For a secure target, select Personalize.
- Target for DOS (See page 2.8.3.) For a secure target, select Personalize.
- LAN directory (See page 2.7.2.)
- Gateway (See page 2.7.3.) For a secure gateway, select Personalize.

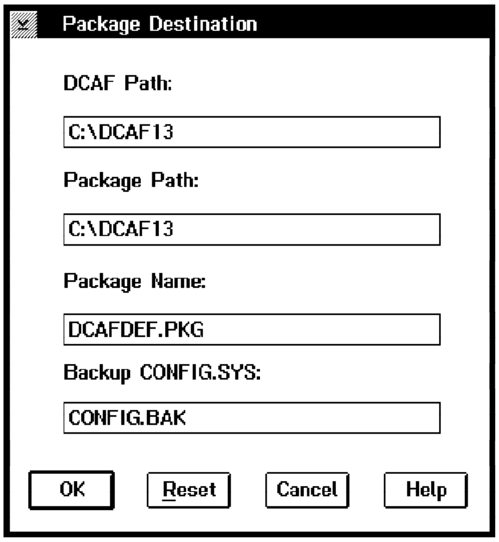
Press the **OK** push button after making your choice. The components that you chose for the installation package will not affect the components that are already installed on the workstation that you are using to create the package.



PICTURE 28

Figure 28. DCAF Packager

5. When the components are included, their status is displayed as 'Ready to package'. The (P) indicates that the component has been personalized. Choose **Make package of the included components...** (or the Ctrl+M shortcut key) from the Makepackage pull-down menu, as shown in Figure 28.



PICTURE 29

Figure 29. Package Destination

6. The Package Destination window (Figure 29) appears. You can define:

   - The DCAF Path. Type the path on the fixed disk of the destination workstation where you want to install the package. The default is C:\DCAF13.

     - The path is 1-50 characters in length.
     - For character guidelines, follow OS/2 conventions for the path.

   - The Package Path. It is the path for the destination of the package. For example, if you are creating a package to be stored on diskette, change the package path to **A:\DCAF13**. The default is C:\DCAF13. For character guidelines, follow OS/2 conventions for the path.

   - The Package Name. It is the name of the package that will be created. You must use the .PKG filename extension. Follow OS/2 file name conventions. The default is DCAFDEF.PKG.

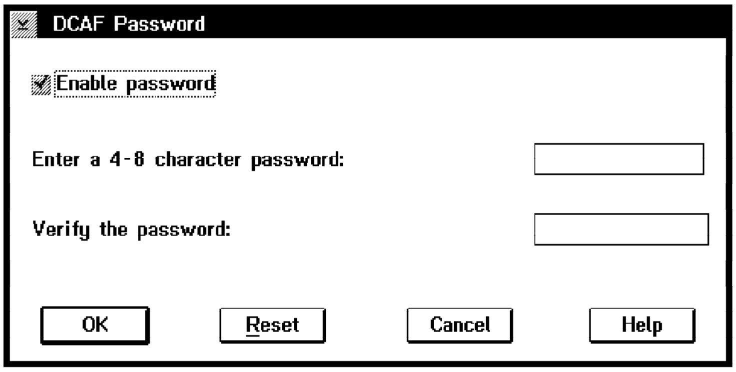
   - The Backup Config.Sys file name. It is the backup name for the CONFIG.SYS file.

     - Follow OS/2 file name conventions.

     - The format of the file name depends on whether your hard disk has been formatted with HPFS or FAT.

     - The default is CONFIG.BAK.

7. If you included the target or gateway for password-only sessions, you will be prompted with the DCAF Password window (Figure 30) for target workstations or DCAF gateway workstations.

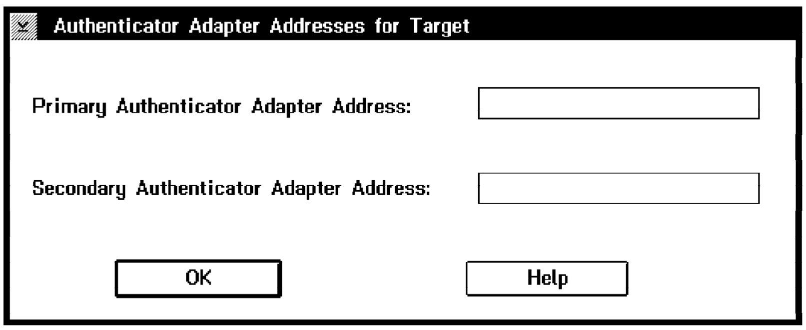


PICTURE 30

Figure 30. DCAF Password

If you press **OK** without typing a password, then you have a nonsecure session (neither password-only security nor secure-session security). If you mark the check box, **Enable password**, then you can type your password.

The password is 4-8 characters in length and must include at least four alphanumeric characters. Retype the same password exactly in the **Verify the password** field.



PICTURE 31

Figure 31. Authenticator Adapter Addresses for Target

8. If you choose a secure target, the Authenticator Adapter Addresses for Target window (Figure 31) appears.

   The secure target uses the adapter address to identify which security authenticator(s) are authorized to start secure sessions with that target. Type the adapter address for a primary and secondary (backup) security authenticator for the target. For more details about the primary and secondary authenticators, see "About the Security Components" in topic 4.1.1. To get the adapter address, check the LANTRAN.LOG file in the IBMCOM directory on the authenticator workstations. The primary and secondary security authenticators can be the same.

   The security authenticator adapter address must be exactly 12 hexadecimal characters in length, including:

   - Upper- or lowercase letters (A-F, a-f)
   - Digits (0-9)
   - Blanks not allowed

   Press the **OK** push button when you have typed all of the information.

The installation package will be created and saved on a diskette or hard disk. If there are errors during the creation of the installation package, you will be instructed what to do. If there are no errors, you will receive the following message:

```
Package (file name) successfully created.
Type (file name) to install the package.
```

The DCAF package is ready to install on the workstation. See "Installing a DCAF Package" in topic 2.2.2, for installation instructions.

2.2.2 Installing a DCAF Package

> **Important Information about Installation**
>
> - Do not start any DCAF components or have a DCAF session in process during the installation of the DCAF package. If other DCAF components are running or if a session has been established, a failure may occur during the DCAF installation.
>
> - If you are installing the DCAF installation package on a workstation that already has the current version of the DCAF installed, then you must install the package in the same directory (as the current DCAF version).

The procedures for installing the DCAF package are the same for both DOS and OS/2 workstations. To install a package on a workstation, perform the following steps.

1. If you are using a diskette, then insert the package diskette into drive A and switch to the A drive (**A:**).

2. After the **A:** prompt appears, change to the directory where the package is stored and type the name of the package. If the directory that has been specified for the destination of the package does not exist, then the directory will be created on the workstation's fixed disk.

3. Remove the package diskette from drive A, and shut down and restart the workstation.

4. Some personalization options for the packaged components can be personalized after the package has been successfully installed and is enabled. See "Personalizing the DCAF Controller and Other Components" in topic 2.7, for instructions. DOS personalization options can be personalized only while you are creating a DOS installation package.

2.2.3 After You Install

After you install, configure the communications protocol on which the workstation will run the DCAF. For instructions on configuring the communications, see "Configuring" in topic 3.0.

2.3 Installing the Windows Target

This chapter describes how to install the Windows target both directly and by using a package.

2.3.1 Before You Install the Windows Target

> **Important Information about Installation**
>
> Do not start any DCAF components or have a DCAF session running during the installation. If other DCAF components are running or if a session has been established, it will cause a failure during the DCAF installation.

To begin installation of the Windows target, follow these steps:

1. Make sure that Windows is running on your workstation.

2. Insert the DCAF 1.31 product diskette 4 into drive A of the workstation.

3. Select **Run...** from the pull-down menu of the Windows Program Manager or File Manager.

4. In the **Command Line** box, type **a:\install** and choose the **OK** button. If you are not using a diskette, type the letter of the drive (and directory name, if applicable) where you have the DCAF Windows target installation files (for example, **z:\dcaf13\install** where z=drive and dcaf13=directory). The DCAF Logo window appears.

5. Choose the **OK** button. The DCAF - Target Installation Type window (Figure 32) appears.

PICTURE 32

Figure 32. Example of DCAF - Target Installation Type Window

It enables you to choose how you want to install the DCAF Windows target on your workstation.

- To install the Windows target on the workstation now, see ″Installing Directly″ in topic 2.3.2.

- To prepare an installation package with the Windows target, which can be installed later or on multiple workstations, see ″Preparing an Installation Package″ in topic 2.3.3.1.

- To install the Windows target from an installation package on the workstation now, see "Installing a DCAF Windows Target Package" in topic 2.3.3.2.

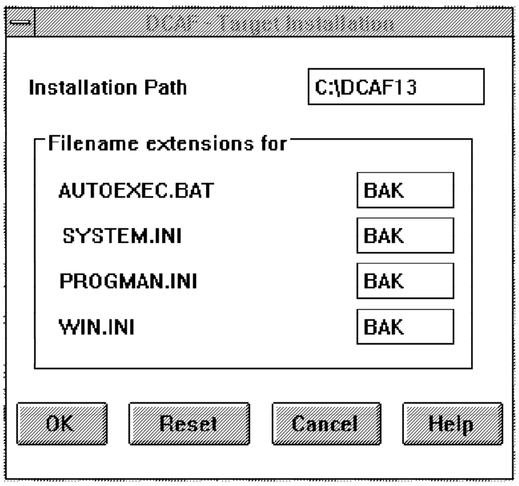
2.3.2 Installing Directly

To install the Windows target on the workstation directly, perform the following steps:

1. Select **Install a target** from the DCAF - Target Installation Type (Figure 32 in topic 2.3.1) window. The **Personalization** check box is already turned on. For more information on Personalization, see "Personalizing the Windows Target" in topic 2.8.2. To use the default setup options, turn off the **Personalization** check box.

   Remember that for a secure target, select Personalize.

2. Choose the **OK** button. The DCAF - Target Installation window (Figure 33) appears.



PICTURE 33

Figure 33. Example of DCAF - Target Installation Window

3. In the Installation Path box, type the letter of the drive and the directory name where you want to install the DCAF Windows target on the workstation. The default is C:\DCAF13

   Note: You cannot install DCAF on Drive B unless it is a physical drive.

   Directory name guidelines:

   - It can be 1-8 characters.

   - Upper- or lowercase letters (A-Z). It is not case sensitive even if it is displayed in uppercase.

   - Digits (0-9).

4. In the Filename extensions for box, type the filename extensions for the backup copy of the AUTOEXEC.BAT, SYSTEM.INI, PROGMAN.INI, and WIN.INI files on your workstation. Backup copies are made of the original files before DCAF modifies them for the DCAF target. The default is BAK.

   Character guidelines:

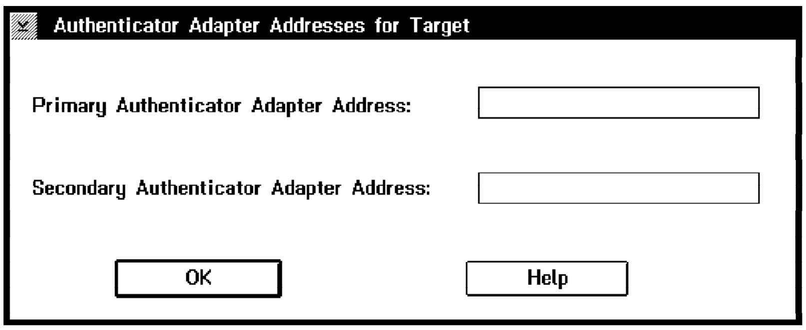
- It can be 1-3 characters.
- Upper- or lowercase letters (A-Z).
- Digits (0-9).

5. Choose the **OK** button. If you selected Personalization, continue with the steps that follow. If you did not select Personalization, skip to Step 10.

6. The DCAF Target Personalization window appears (see "In the Windows Environment" in topic 2.8.2.1). When you have completed personalizing all the options for the Windows target, choose the **OK** button to make your entries valid.

7. If, on the DCAF Target Personalization window, you enabled the target to be a secure target, continue with the steps that follow. If you did not enable the target to be a secure target, skip to10 .

8. The Authenticator Adapter Addresses for Target window (Figure 34) appears.



PICTURE 34

Figure 34. Example of Windows Authenticator Adapter Addresses for Target Window

You assigned the security authenticator name when you installed the secure gateways on the LAN. This keeps unauthorized authenticators from connecting to the LAN and starting sessions with secure targets. You can assign a maximum of two authenticators per LAN. For more details, see "About the Security Components" in topic 4.1.1. To get the adapter address, check the LANTRAN.LOG file in the IBMCOM directory on the authenticator workstations. The primary and secondary security authenticators can be the same.

In the Primary Authenticator Adapter Address box, type the adapter address of the workstation where the security authenticator for the secure target is installed. This field is required.

Character guidelines for hexadecimal format:

- It is exactly 12 characters.
- Upper- or lowercase letters (A-F).
- Digits (0-9).

9. In the Secondary Authenticator Adapter Address box, type the unique LAN adapter address of a backup authenticator. This field is required, but you can type the same adapter address that you typed in the Primary Authenticator Adapter Address box.

Character guidelines for hexadecimal format:

- It is exactly 12 characters.
- Upper- or lowercase letters (A-F).
- Digits (0-9).

Skip to Step 13 to begin installation, if you do not want to assign a password.

10. The DCAF Password window appears. You can use it to assign a password.

    It enables you to set up password security (as opposed to session security through a security authenticator) for the target workstation.

    It is optional. If you do not want to assign a password, skip to Step 13. To assign a password, select the Enable password check box. The target workstation user can change the password at any time.

11. The password boxes will become available after you select the Enable password check box. In the Enter a 4-8 character password box, type the password.

    Character guidelines:

    - It is 4-8 characters.
    - Upper- or lowercase letters (A-Z).
    - Digits (0-9).
    - Blanks after the last alphanumeric are ignored.

12. In the Verify the password box, type the same password again. Be sure to give this password to the controller user who will be starting sessions with the Windows target workstation.

13. Choose the **OK** button. DCAF installation will begin. When it is complete, you will see the message:

        Installation completed successfully.
        Before running the DCAF, configure the
        communications, remove the diskette,
        and restart the workstation.

    Complete the next step only if you plan to connect to the target via NetBIOS.

14. Because the way communication resources are allocated and used varies from network to network, the values provided are approximate and only suggestions. Use trial and error to find the values that are right for your network.

    Edit the SYSTEM.INI file. In the group of the Windows mode that you use, it is recommended that you have the following statement:

    - In the [386Enh] group,

      NetHeapSize=180

    - In the [Standard] group,

      NetHeapSize=60

15. Save and close the SYSTEM.INI file.

16. Remove the diskette and restart the workstation.

    If you have Program Manager, the DCAF group with a target icon inside will appear immediately on the shell. To start the DCAF target program, select the target icon.

    If you have a shell other than Program Manager, you must add the DCAF group manually (see your instruction manual to find out how). To start the DCAF target program, you must run the EQNWTUI.EXE file from the path where you have installed DCAF. For example, type: **c:\dcaf13\eqnwtui.exe** where c=drive and dcaf13=directory where DCAF is installed.

2.3.3 Installing the Windows Target with an Installation Package

By creating and installing an installation package, you can distribute targets to workstations all over your network. If you need to install a number of Windows targets with the same options on different workstations, you can personalize the setup options of the target and create a package that can be installed on numerous workstations.

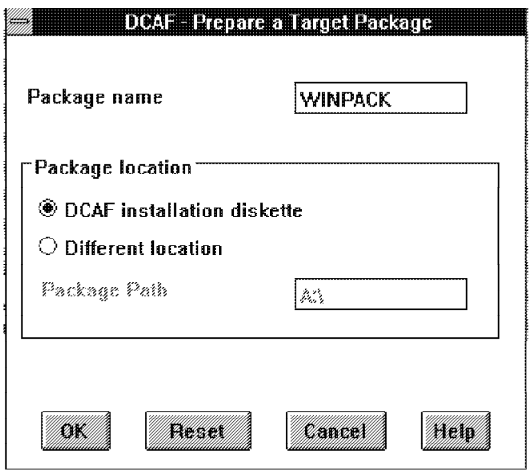
2.3.3.1 Preparing an Installation Package

To create an installation package on a diskette,

1. Follow the steps listed in "Before You Install the Windows Target" in topic 2.3.1.

2. Choose **Prepare a target package** from the DCAF - Target Installation Type window (Figure 32 in topic 2.3.1). To create a secure target or to create a number of targets with the same customized setup options, select the **Personalization** check box. For more information on Personalization, see "Personalizing the Windows Target" in topic 2.8.2.

3. Choose the **OK** button. The DCAF - Prepare a Target Package window (Figure 35) appears.



PICTURE 35

Figure 35. Example of Creating a Windows Target Package

4. In the Package name box, type the name that you want to use to identify the package. This field is required.

   Character guidelines:

   - It is 1-8 characters.
   - Upper- or lowercase letters (A-Z).
   - Digits (0-9).

5. For Package location, select where you want for the package to be copied. You can copy a package either onto a diskette (it must be the DCAF installation diskette) or to the hard-disk of your workstation.

   - DCAF installation diskette. If you will be using a diskette to install the target package on one or more workstations, select this option.

   - Different location. If you will be installing target packages from the hard disk on your workstation, select this option. If you select this option, the Package Path box becomes available.

6. In the Package Path box, type the drive and directory where the installation will copy the package you are creating (for example, C:\DIR\... or Z:\DIRn..., where C or Z=drive and DIR or DIRn=directory). If you selected Different location, this field becomes required. If you begin creating a package from a diskette and type a directory in drive A:\, this field becomes unavailable and only the file with personalization options will be copied to that directory.

   In all other cases, you cannot type the same directory as the one where you started running the DCAF installation to create the package. Make sure that there is enough space in the drive that you choose. The default is C:\PACK13.

   Character guidelines:

   - It is 1-8 characters.
   - Upper- or lowercase letters (A-Z). It is not case sensitive even if it is displayed in uppercase.
   - Digits (0-9).

7. Choose the **OK** button. The DCAF - Target Installation window (Figure 33 in topic 2.3.2) appears

8. In the Installation Path box, type the drive and directory where you want to install the DCAF Windows target on the workstation. The default is C:\DCAF13.

   Note: You cannot install the DCAF on drive B unless it is a physical drive.

   Directory name guidelines:

   - It can be 1-8 characters.
   - Upper- or lowercase letters (A-Z). It is not case sensitive even if it is displayed in uppercase.
   - Digits (0-9).

9. In the Filename extensions for box, type the filename extensions for the backup copy of the AUTOEXEC.BAT, SYSTEM.INI, PROGMAN.INI, and WIN.INI files on your workstation. Backup copies are made of the original files before DCAF Installation modifies them for the DCAF target. The default is BAK.

   Character guidelines:

   - It can be 1-3 characters.
   - Upper- or lowercase letters (A-Z). It is not case sensitive even if it is displayed in uppercase.
   - Digits (0-9).

10. Choose the **OK** button. If you selected Personalization, continue with the steps that follow. If you did not select Personalization, skip to Step 15.

11. The DCAF Target Personalization window appears (see "In the Windows Environment" in topic 2.8.2.1). When you have completed personalizing all the options for the Windows target, choose the **OK** button to make your entries valid.

12. If, on the DCAF Target Personalization window (Figure 57 in topic 2.8.2.1), you enabled the target to be a secure target, continue

with the steps that follow. If you did not enable the target to be a secure target, skip to 15.

13. The Authenticator Adapter Addresses for Target window (Figure 34 in topic 2.3.2) appears. The security authenticator name is assigned during the installation of the secure gateways on the LAN. This keeps unauthorized authenticators from connecting to the LAN and starting sessions with secure targets. You can assign a maximum of two authenticators per LAN. For more details, see "About the Security Components" in topic 4.1.1. To get the adapter address, check the LANTRAN.LOG file in the IBMCOM directory on the authenticator workstations. The primary and secondary security authenticators can be the same.

    In the Primary Authenticator Adapter Address box, type the universally administered address of the workstation where the security authenticator for the secure target is installed. This field is required.

    Character guidelines for hexadecimal format:

    - It is exactly 12 characters.
    - Upper- or lowercase letters (A-F).
    - Digits (0-9).

14. In the Secondary Authenticator Adapter Address box, type the unique LAN adapter address of a backup authenticator. This field is required, but you can type the same adapter address that you typed for the Primary Authenticator Adapter Address box.

    Character guidelines for hexadecimal format:

    - It is exactly 12 characters.
    - Upper- or lowercase letters (A-F).
    - Digits (0-9).

    Skip to Step 18, if you do not want to set up a password.

15. The DCAF Password window appears. It enables you to set up password security (as opposed to session security through a security authenticator) for the target workstation.

    It is optional. If you do not want to assign a password, skip to Step 18. To assign a password, select the Enable password check box. The target workstation user can change the password at any time.

16. The password boxes will become available. In the Enter a 4-8 character password box, type the password.

    Character guidelines:

    - It is 4-8 characters.
    - Upper- or lowercase letters (A-Z).
    - Digits (0-9).
    - Blanks after the last alphanumeric are ignored.

17. In the Verify the password box, type the same password again. Be sure to give this password to the controller user who will be starting sessions with the Windows target workstation.

18. Choose the **OK** button. DCAF installation will begin. When it is complete, you will see the message:

        Package preparation completed successfully.

19. Choose the **OK** button. You are now ready to install the package at any time.

2.3.3.2 Installing a DCAF Windows Target Package

To install a Windows target package on a workstation, either local or remote, perform the following steps:

1. Make sure that Windows is running on your workstation.

2. If you are installing the package from the installation diskette, insert the DCAF 1.31 product diskette 4 into drive A of the workstation.

3. Select **Run...** from the pull-down menu of the Windows Program Manager or File Manager.

4. If you are installing the package from the installation diskette, in the **Command Line** box, type **a:\install**, and choose the **OK** button. If you are not using the installation diskette, type the letter of the drive (and directory name, if applicable) where you have the DCAF Windows target installation files (for example, **z:\dcaf13\install** where z=drive and dcaf13=directory).

5. The DCAF Logo window appears.

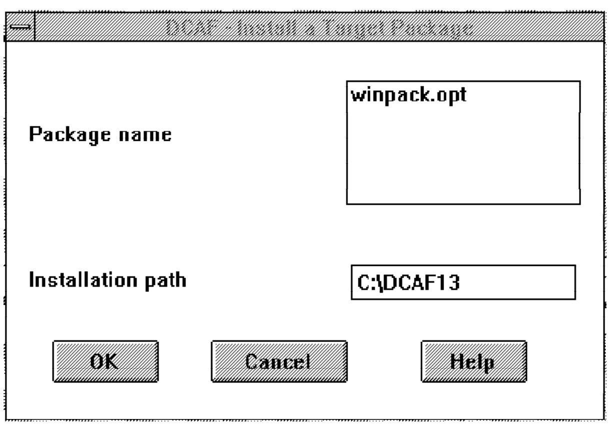
   Choose the **OK** button.

6. The DCAF - Target Installation Type window (Figure 36) appears.

PICTURE 36

Figure 36. Example of DCAF - Target Installation Type Window

7. Choose **Install a Target Package**. The DCAF - Install a Target Package window (Figure 37) appears.



PICTURE 37

Figure 37. Example of Installation of a Windows Target Package

This window enables you to choose, from a list of existing packages, the package that you want to install on the workstation.

8. From the Package name box, select the name of the package that you want to install. When you select it, the destination drive and directory (path) associated with the package when it was created appears in the Installation path box. If you want to install the package in a different path, type the new path in the Installation path box. This field is required and must contain a drive and directory (for example, C:\DCAF13).

   Note: You cannot install DCAF on Drive B unless it is a physical drive.

   Directory name guidelines:

   - It can be 1-8 characters.

   - Upper- or lowercase letters (A-Z). It is not case sensitive even if it is displayed in uppercase.

   - Digits (0-9).

9. Choose the **OK** button. The installation of the DCAF package will proceed. When it is complete, you will see the message:

   ```
   Installation completed successfully.
   Before running the DCAF, configure the
   communications, remove the diskette,
   and restart the workstation.
   ```

   Complete the next step only if you plan to connect to the target via NetBIOS.

10. Because the way communication resources are allocated and used varies from network to network, the values provided are approximate and only suggestions. Use trial and error to find the values that are right for your network.

    Edit the SYSTEM.INI file. In the group of the Windows mode that you use, it is recommended that you have the following statement in all the instances where the NetHeapSize statement appears:

    - In the [386Enh] group,

      NetHeapSize=180

    - In the [Standard] group,

      NetHeapSize=60

11. Save and close the SYSTEM.INI file.

12. Remove the diskette and restart the workstation.

    If you have Program Manager, the DCAF group with the target icon will appear immediately on the shell. To start the DCAF target program, select the target icon.

    If you have a shell other than Program Manager, you must add the DCAF group manually (see your instruction manual to find out how). To start the DCAF target program, you must run the EQNWTUI.EXE file from the path where you have installed DCAF. For example, type: **c:\dcaf13\eqnwtui.exe** where c=drive and dcaf13=directory where DCAF is installed.

2.3.4 Deinstalling the Windows Target

To deinstall the DCAF Windows target from the workstation, you must replace the Windows system files that were modified when you installed the DCAF with the backup system files made during the installation (see Step 4 in topic 2.3.2 and Step 9 in topic 2.3.3.1 for Filename extensions).

If, for some reason, you cannot access the backup system files, you can make the changes in each file manually. See "Manual Deinstallation" in topic APPENDIX1.5.2. The system files are WIN.INI, PROGMAN.INI, and SYSTEM.INI in the Windows directory and AUTOEXEC.BAT in the root directory.

To deinstall the Windows target from the workstation,

1. Exit from your Windows session by choosing Exit Windows from the File menu.

   A confirmation dialog box appears, prompting you to confirm that you want to end your Windows session.

2. Choose the **OK** button. The native DOS full-screen appears.

3. At the DOS prompt, type:

   copy win.backupfile **win.ini**, where win.backupfile is the name of the backup of your WIN.INI file, and press **Enter**.

   So, for example, if you used the default filename extensions during the installation, it might look like this:

   ```
   C:\Windows>copy win.bak win.ini
   ```

4. Repeat Step 3 for the PROGMAN.INI and SYSTEM.INI files, substituting the backup file names for these files.

5. At the DOS prompt, type **del dcaf.ini** and press **Enter**. Confirm your choice.

6. Then at the DOS prompt, type **dir *.grp** an press **Enter**. You will see a list of all the files with the file type **GRP**.

7. To delete the DCAF group files, type **del dcaf*.grp** and press **Enter**. Confirm your choice.

8. To delete the DCAF directory, type **del** directory, where directory is the directory in which you installed DCAF, and press **Enter**. Confirm your choice.

9. To remove the DCAF directory, type **rd** directory.

10. At the DOS prompt, change to the root directory by typing **cd..** and pressing **Enter**. Confirm your choice.

11. Then type: **copy** autoexec.backupfile **autoexec.bat**, where autoexec.backupfile is the name of the backup of your AUTOEXEC.BAT file, and press **Enter**.

    So, for example, if you used the default filename extensions during the installation, it might look like this:

    ```
    C:\>copy autoexec.bak autoexec.bat
    ```

    The next time you open Windows, you will not see the DCAF group and target icon included in the Program Manager.

2.4 Installing the DCAF Using the CID Method

The CID method of installation enables you to install large numbers of the DCAF remotely at unattended workstations. The primary goals of CID are to:

- Eliminate human intervention at the remote workstation for the configuration, installation, migration, and maintenance of the DCAF.
- Enable the code executed at the remote workstation to perform all required configuration and installation tasks.
- Centralize human intervention at a central preparation site.

2.4.1 Basic Elements of CID-Enabled System Environments

CID requires the following elements:

- Software distribution manager
- Response files
- Command driven execution
- Redirected drives
- Progress indication and logging facilities

2.4.1.1 Software Distribution Manager

Your network must have a software distribution manager which is a remote installation procedure that is not dialog-driven. The software distribution manager is not a specific product. There are products such as NetView* DM/2 or the Network Transport Services/2 LAN CID Utility that perform the functions of a software distribution manager.

2.4.1.2 Response Files

Response files contain prepared responses that users normally provide during the installation, personalization, and configuration process. Response files contain ASCII data and may therefore be created using any tool that creates ASCII output, such as an ASCII editor or REXX procedures.

Because personalization information can be recorded in response files, manual intervention at the time of installation is not required. You can specify this configuration information anywhere at any time. You do not have to be involved in the process as it is going on.

2.4.1.3 Command Driven Execution

Command driven execution is required for the CID method because using a dialog-driven execution would require manual intervention.

2.4.1.4 Redirected Drives

Drive redirection means installing software from a drive other than diskette drives. This drive, which is represented by a disk drive letter, can be an alternative drive on the local system, a drive on a LAN or other network, or some other device that appears to the installation program as a logical drive (such as a CD-ROM).

2.4.1.5 Progress Indication and Logging Facilities

DCAF CID generates a log file that stores information about the progress and results of installation, personalization, configuration, or maintenance. These files contain information such as installation, maintenance, configuration, and update history, and error information.

Log information is stored in ASCII format. Using only command line parameters, you define the drive and path in which these files are written.

2.4.2 Overview of CID Installation

There are three main tasks in CID installation:

1. Unpacking the DCAF CID files for the components you need onto a server machine in your network.

2. Preparing the response file with the component personalization options.

3. Starting the installation on the client workstation.

2.4.2.1 Unpacking the DCAF CID files

To copy the files for the components that you need to the server, you must unpack the DCAF CID files.

2.4.2.1.1 For OS/2 Components

For OS/2 components, unpack the self-extracting file OS2CID.EXE and copy the .PKG files for the components that you are installing. The OS/2 component .PKG file names follow:

- CONTROL for the controller
- GATEWAY the gateway
- LANDIR for the LAN directory
- OS2TGT for the OS/2 target
- SECADMIN for the security administrator
- SECAUTH for the security authenticator

To copy the files for the components that you need to the server, perform the following steps:

1. Insert the CID Installation Programs diskette **5** into drive A.

2. At the command prompt of the source directory, type copy a:\os2cid.exe and press **Enter**.

3. Copy the .PKG file for each OS/2 component that you are installing. Insert into drive A the CID Basic Package Files diskette **6** for the following components:

   - Controller
   - Gateway
   - LAN directory
   - OS/2 target

   Insert into drive A the CID Security Package Files diskette **7** for the security administrator and security authenticator.

4. Type copy a:\component.pkg, where component is one of the .PKG file names above, and press **Enter**.

5. Repeat Step 4 for all the OS/2 components that you are installing on

the client workstation.

6. Type os2cid and press **Enter**. The DCAF unpacks the CID installation files onto the server workstation.

2.4.2.1.2 For the Windows Target

To unpack the self-extracting file WINCID.EXE, perform the following steps:

1. Insert the CID Installation Programs diskette into drive A.

2. At the command prompt of the source directory, type copy a:\wincid.exe and press **Enter**.

3. Select **Run...** from the pull-down menu of the Windows Program Manager or File Manager.

4. In the **Command Line** box, type wincid and press the **OK** push button. The DCAF unpacks the CID installation files onto the server workstation.

2.4.2.1.3 For the DOS Target

To unpack the self-extracting file DOSCID.EXE, perform the following steps:

1. Insert the CID Installation Programs diskette into drive A.

2. At the command prompt of the source directory, type copy a:\doscid.exe and press **Enter**.

3. Type doscid and press **Enter**. The DCAF unpacks the CID installation files onto the server workstation.

2.4.2.2 Preparing the Response File

Prepare a response file that contains the personalization options for each component that you are installing on the client workstation. It can contain information for one or more components that you will install on the same client, for example, the LAN directory and target.

Personalize the sample response files included on the DCAF CID diskettes or create your own response files. See Appendix C, ″Response Files″ in topic APPENDIX1.3 for the correct format and parameters.

2.4.2.3 Starting the Installation on the Client Workstations

Start installation on the client workstation by typing the command and any parameters that you want specify.

2.4.2.3.1 Parameters for the Installation Command

The following list describes the parameters in the installation command. If you omit a parameter from the installation command, DCAF CID uses the default value. The parameters can be listed in any order. If you specify a parameter more than once, the command uses the last value.

/s: (or **/sd:** for Windows target)
: The drive and path in which DCAF is installed on the SDM server. The default is the directory in which you are working when you send the installation command.

/r:
: The drive and path in which the response file is installed on the SDM server and the response file name. The default is the <source directory>\DCAF.RSP for OS/2 components. The default is the <source directory>\DCAFWIN.RSP for the Windows target. The default is the <source directory>\DCAFDOS.RSP for the DOS

target.

/l1: The drive and path in which the installation log file is installed, typically at the central preparation site. The default log file name is the <source directory>\EQNCID.LOG

/t: The drive and path in which DCAF is installed on the client workstation. The default is c:\DCAF13 or the directory in which DCAF 1.31 is already installed on the client.

To start installation on the client workstations, type the following commands.

2.4.2.3.2 For OS/2 Components

To start installation on the client workstation, type the following command at the command prompt on an OS/2 full-screen at the client workstation:

```
eqnresp /s:<sourcedir> /r:<response file> /l1:<logfile> /t:<targetdir>
```

2.4.2.3.3 For the Windows Target

To start installation on the client workstation, perform the following steps:

1. Select **Run...** from the pull-down menu of the Windows Program Manager or File Manager.

2. In the **Command Line** box, type

   ```
   eqnwresp /sd:<sourcedir> /r:<response file> /l1:<logfile> /t:<targetdir>
   ```

   and press the **OK** push button.

2.4.2.3.4 For the DOS Target

To start installation on the client workstation, type the following command at the command prompt on an DOS full-screen at the client workstation:

```
eqndresp /s:<sourcedir> /r:<response file> /l1:<logfile> /t:<targetdir>
```

2.4.3 Deinstalling DCAF from Unattended Workstations

To deinstall from an unattended workstation, type the following command at the command line on the remote workstation: **eqninsds /n**. Then reboot the workstation.

2.5 Installing the DCAF from a Compact Disc (CD) and from a Remote File Server

You can install the DCAF from a CD-ROM and from a remote file server.

2.5.1 From CD-ROM

To install the DCAF on an OS/2 workstation from a CD-ROM, perform the following steps:

1. Insert the CD into the CD reader.

2. At the command prompt of the workstation on which you are installing DCAF, type x:**install**, where x is the drive from which the CD can be accessed, and press **Enter**.

3. Continue the installation procedure from "Installing Directly (OS/2 Workstations Only)" in topic 2.1.1.

To install the Windows target on a Windows workstation from a CD-ROM, perform the following steps:

1. Insert the CD into the CD reader.

2. Select **Run...** from the pull-down menu of the Windows Program Manager or File Manager on the workstation on which you are installing DCAF.

3. In the **Command Line** box, type x:**install**, where x is the drive from which the CD can be accessed, and press the **OK** push button.

4. Continue the installation procedure from "Installing the Windows Target" in topic 2.3.

2.5.2 From a Remote File Server

You can install DCAF from the hard disk of a remote file server, a workstation that each workstation on a network can use to access files that can be shared among the connected workstations. The workstation on which you will install the DCAF must be a client of the server workstation. For example, DCAF is installed in a directory of the hard disk on a remote server in your network. If your client workstation has redirected drives (see "Redirected Drives" in topic 2.4.1.4 for an explanation), you can install the DCAF on your client workstation from the remote server.

To install DCAF from remote file server onto an OS/2 client workstation, perform the following steps:

1. On the remote file server, create a directory for DCAF.

2. Copy the DCAF diskettes to the new DCAF directory.

3. At the command prompt on the client workstation, type z:, where z is the drive from which you access files from the file server, and press **Enter**.

4. Type z:\directory**install**, where directory is the directory on the file server in which the DCAF files are stored, and press **Enter**. The DCAF diskettes are copied to the client workstation.

5. Continue the installation procedure from "Installing Directly (OS/2

Workstations Only)" in topic 2.1.1.

To install the Windows target from remote file server onto a Windows client workstation, perform the following steps:

1. On the remote file server, create a directory for DCAF.

2. Copy the Windows target diskette to the new DCAF directory.

3. Select **Run...** from the pull-down menu of the Windows Program Manager or File Manager on the Windows workstation.

4. In the **Command Line** box, type z:\directory**install**, where z is the drive from which you access files from the file server and where directory is the directory on the file server in which the DCAF files are stored, and press the **OK** push button. The Windows target diskette is copied to the client workstation.

5. Continue the installation procedure from "Installing the Windows Target" in topic 2.3.

2.6 Installing and Accessing DCAF Information Online

DCAF online information consists of online books, help, and messages.

2.6.1 Using Online Books

The online books (see "Where to Find More Information" in topic WHERE for titles) are available for the workstations through IBM BookManager* READ/2, Library Reader*, and CD-ROM. The DCAF package includes Library Reader to enable you to view the books if you do not have IBM BookManager READ/2.

2.6.1.1 Installing the DCAF Online Books

To install the DCAF online books, perform the following steps:

1. Switch to a full-screen.

2. Insert the DCAF Online Books diskette into drive A of the workstation.

3. At the command prompt, type **a:\instbook**.

4. Follow the instructions on the screen. DCAF checks whether you have IBM BookManager READ/2 or Library Reader. If you have neither one, you must install the Library Reader. DCAF provides a Library Reader diskette.

If any errors occur, you will be instructed what to do.

2.6.1.2 Installing Library Reader for OS/2

If you do not have IBM BookManager READ/2, you need to install the Library Reader, which is provided with the product diskettes. The Library Reader diskette contains the following files:

BOOKENG.AGR Information on authorized use of IBM online books.

PLALRENG.AGR Before installing Library Reader, read this Program License Agreement.

README.TXT General information on how to use the product. All these files can be viewed with any editor (for example, the OS/2 editor).

EZ2INST Directory This directory contains all the Program and Installation files.

To install the Library Reader, do the following:

1. At the command prompt, insert the Library Reader diskette and type:**a:**.

2. From the A: drive, type **cd ez2inst** and press **Enter**.

3. Type **install**.

4. On the second panel type **4** in the Selection Number field.

5. On the next panel, replace the default value with the letter of the drive and the directory that will contain your IBM Books (for example, READIBM2). Choose Y in the field to update your CONFIG.SYS file.

6. Press F10 when you are ready to install.

7. After installation of Library Reader is complete, type **c:** (or the drive in which you installed Library Reader) and press **Enter**.

8. Type **cd readibm2** and press **Enter**.

9. Insert the DCAF Online Books diskette, and type **a:\instbook** to start the book installation process.

10. Follow the instructions online.

11. When installation of the books is complete, edit your CONFIG.SYS file. At the SET READIBM statement, add the following: c:dir**\READIBM2;** where c:dir is the drive and directory in which you installed Library Reader.

12. Save and close the file.

13. Restart your workstation.

You have installed Library Reader and the DCAF online books.

2.6.1.3 Viewing the Online Books with Library Reader

To view the online books with Library Reader, do the following:

1. Open the IBM Online Library folder from the Workplace Shell*.

2. From the IBM Online Library, choose All Available Bookshelves. The BookManager Books and Bookshelves appear.

3. Choose All from the View action bar to see a list of the DCAF books. The installed DCAF books appear. (″The DCAF Online Library″ in topic 2.6.1.5 provides a list of the titles.)

4. Open the book that you want to view.

2.6.1.4 Viewing the Online Books with IBM BookManager READ/2

After you install the books, open IBM BookManager READ/2 and choose the book that you want to view.

2.6.1.5 The DCAF Online Library

The following list provides the file name and the corresponding title for each book:

File	**Title**
DCAFINST.BOO	Distributed Console Access Facility Installation and Configuration Guide
DCAFMSGS.BOO	Distributed Console Access Facility Messages and Codes
DCAFTARG.BOO	Distributed Console Access Facility Target User′s Guide
DCAFUSER.BOO	Distributed Console Access Facility User′s Guide

2.6.2 Displaying Online Help

After the DCAF Logo window appears when you install the DCAF, you can select online window help at any time. To display the help window, press the **F1=Help** key or select the Help push button when it is displayed. To exit from the Help window, press **Esc**.

Different kinds of help are available. There are two ways to open any help item or term of interest:

- Move the mouse pointer to a topic and double-click.
- Tab to the topic and press **Enter**.

To get help for an item on the menu bar or in a pull-down window, you can use the mouse or the keyboard.

- To use the mouse, move the pointer over the item for which you want help. Press F1 while you are holding down mouse button 1.

- To use the keyboard, press F10 or the Alt key to move to the menu bar. Next use the arrow keys to select the item on which you want help and press F1.

2.7 Personalizing the DCAF Controller and Other Components

Most DCAF components can be personalized during direct installation, during creation of an installation package, or when you are using the component.

Some personalization options, such as making components secure, are available only during installation and packaging. These are noted for each component.

To personalize an installation package, perform the following steps:

1. Choose the component from the Distributed Console Access Facility Packager main window.

2. On the Packaging Mode window (Figure 27 in topic 2.2.1), choose **Personalize** and press the **OK** push button. You can go on to personalize the component.

To change personalization options before you install DCAF components or create installation packages, perform the following steps:

1. Select the component that you want to personalize again.

2. Choose **Change personalization parameters...** from the pull-down menu. You can go on to personalize the component.

Each personalization window has the following push buttons:

- **Reset**, which returns the last saved values.

- **OK**, which validates your choices.

- **Help**, which gives you online window help.

- **Cancel**, which closes the current operation and returns you to the previous window.

2.7.1 Personalizing the Controller

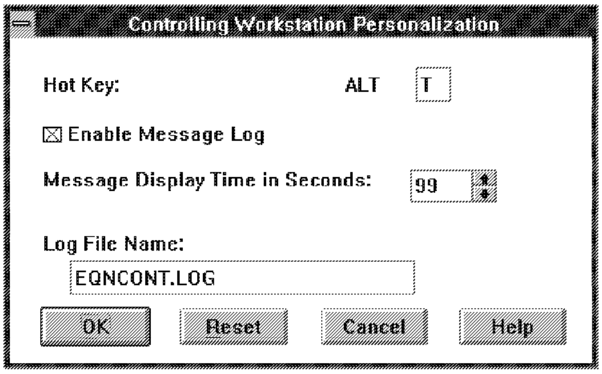
You can personalize the following parameters:

- Controller hot key
- Message log
- Message display

To personalize the controller after it is installed, perform the following steps:

1. Choose **Personalization** from the **Services** pull-down menu on the controller main window as shown in the Distributed Console Access Facility User's Guide.

2. The Controller Workstation Personalization window (Figure 38) appears.



PICTURE 38

Figure 38. DCAF Controller Workstation Personalization

3. For Hot Key, choose the hot key combination. This is a combination of the Alt key and another key of your choice (A-Z) pressed simultaneously. It allows the controller to interrupt a DCAF session and, for example, switch from keystrokes remote (manipulating the target workstation display) to keystrokes local (manipulating the controller display). The default key combination is Alt+T.

4. For Enable Message Log, select the check box to keep a log for error and informational messages.

5. For Message Display Time in Seconds, choose the length of time that the message should be displayed.

   - The range is from 0-99 seconds.

   - The default (99) displays the message indefinitely until it is acknowledged by the user.

   - If you choose 0 seconds, the message will not be displayed.

6. For Log File Name, type the name for this file. This field becomes available only when Enable Message Log is selected.

   - The log file name is 1-8 characters, with a 0-3 character extension.

   - The log file is created where the DCAF product is installed. The default message log file name for the controller is EQNCONT.LOG.

To personalize the controller during installation, perform the following steps:

1. On the Installation Mode window (Figure 11 in topic 2.1.1.1), choose **Personalize** and press the **OK** push button. To change your personalization choices, choose **Change personalization parameters...** from the Install pull-down menu.

2. Begin with Step 2 and complete all the steps in the previous procedure.

2.7.2 Personalizing the LAN Directory

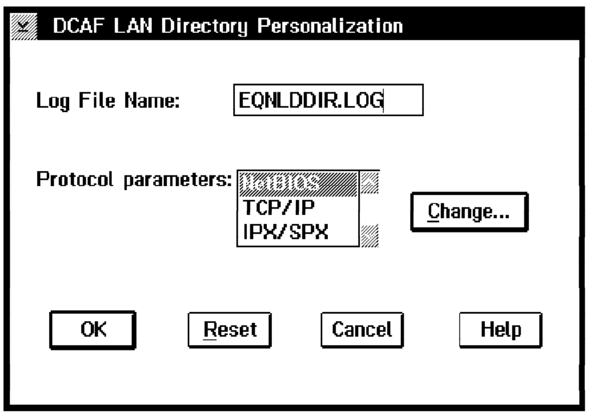
You can personalize the following parameters:

- Log file
- NetBIOS parameters
- TCP/IP parameters
- IPX/SPX parameters
- LAN directory name. DCAF provides a utility that performs this task once from the command line.

To personalize the LAN directory after it is installed, perform the following steps:

1. From Options on the menu bar of the DCAF LAN Directory window, choose Personalization.... The DCAF LAN Directory Personalization window (Figure 39) appears.

2. The DCAF LAN Directory Personalization window (Figure 39) appears.



PICTURE 39

Figure 39. DCAF LAN Directory Personalization

3. For Log File Name, type the name of the log file that tracks error and informational messages as an audit trail for DCAF sessions.

   - The log file name is 1-8 characters, with a 0-3 character extension.

   - The log file is created where the DCAF product is installed. The default message log file name for the controller is EQNLDDIR.LOG.

4. For Protocol parameters, personalize all the communication protocols that the LAN directory uses to link to the controller. The LAN directory, depending on the protocols present in your network, uses the following protocols to connect to the controller:

   - NetBIOS (see "NetBIOS Parameters" in topic 2.7.2.1)
   - TCP/IP (see "TCP/IP Parameters" in topic 2.7.2.2)
   - IPX/SPX (see "IPX/SPX Parameters" in topic 2.7.2.3)

   Select the protocol and press the Change... push button. The window for the protocol parameters you select appears. When you complete personalizing the protocol parameters, press the **OK** push button. The DCAF LAN Directory Personalization window reappears.

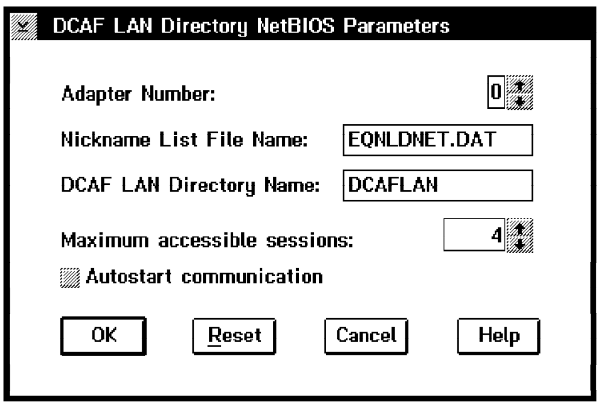
5. To personalize other protocol parameters, repeat the previous step. When you complete personalizing the LAN directory, press the **OK** push button.

For these changes to take effect, you must stop and restart the LAN directory.

2.7.2.1 NetBIOS Parameters

To personalize the LAN directory for connections using NetBIOS with the controller, perform the following steps:

1. From the Protocol parameters list box on the DCAF LAN Directory Personalization window, select NetBIOS. The DCAF LAN Directory NetBIOS Parameters window (Figure 40) appears.



PICTURE 40

Figure 40. DCAF LAN Directory NetBIOS Parameters

2. For Adapter Number, select the LAN adapter number for your workstation. The range is 0-3. The default is 0.

3. For the Nickname List File Name field, type the name of a file that defines, by adapter address and nickname, targets registered with this LAN directory. This field is optional. The nickname list file name is 1-8 characters, with a 0-3 character extension. It is installed in the same directory in which DCAF is installed. The default name for the nickname list file is EQNLDNET.DAT. The DCAF sample file included in the DCAF diskettes is EQNLDNET.TXT.

4. The DCAF LAN directory name. It is the name assigned to the LAN directory. The LAN directory keeps an internal list of names of the DCAF-enabled target workstations and also contains the nickname file list. Each target and gateway workstation is registered with one DCAF LAN directory. If there is more than one LAN directory on a logical LAN, the DCAF LAN directory names must be unique.

   - The DCAF LAN directory name is 1-12 characters.
   - It cannot be a single asterisk (*) or all blanks, and it is case sensitive.
   - The default name for the LAN directory name is DCAFLAN.

5. In the Maximum accessible sessions field, enter the maximum number of LAN directory sessions that can occur simultaneously between the LAN directory and the controller. The sessions can be between the LAN directory and different DCAF gateways or with several instances of the same DCAF gateway workstation.

- The default number of sessions is 4.

- The range is 1-254.

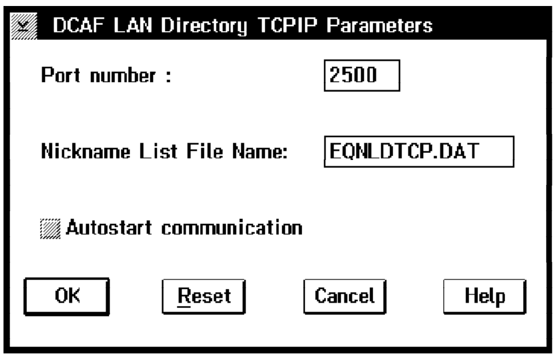
- This option reserves the necessary number of NetBIOS resources for the sessions. If there are insufficient NetBIOS resources, increase the number of available NetBIOS resources in the OS/2 Communications Manager.

6. Select the Autostart communication check box to start NetBIOS automatically when you start the LAN directory. This choice is optional.

2.7.2.2 TCP/IP Parameters

To personalize the LAN directory for connections using TCP/IP with the controller, perform the following steps:

1. From the Protocol parameters list box on the DCAF LAN Directory Personalization window, select TCP/IP. The DCAF LAN Directory TCP/IP Parameters window (Figure 41) appears.



PICTURE 41

Figure 41. DCAF LAN Directory TCP/IP Parameters

2. For Port Number, type the number used to differentiate between different applications using the same protocol. The range is 1024-65534. The default is 2500.

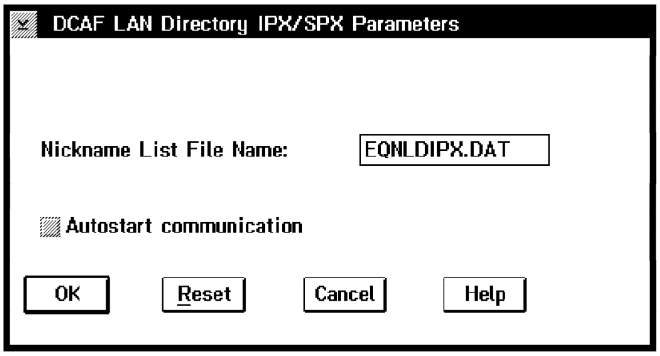
3. For the Nickname List File Name field, type the name of a file that defines, by adapter address and nickname, targets registered with this LAN directory. This field is optional. The nickname list file name is 1-8 characters, with a 0-3 character extension. It is installed in the same directory in which DCAF is installed. The default name for the nickname list file is EQNLDTCP.DAT. The DCAF sample file included in the DCAF diskettes is EQNLDTCP.TXT.

4. Select the Autostart communication check box to start TCP/IP automatically when you start the LAN directory. This choice is optional.

2.7.2.3 IPX/SPX Parameters

To personalize the LAN directory for connections using IPX/SPX with the controller, perform the following steps:

1. From the Protocol parameters list box on the DCAF LAN Directory Personalization window, select IPX/SPX. The DCAF LAN Directory IPX/SPX Parameters window (Figure 42) appears.



PICTURE 42

Figure 42. DCAF LAN Directory IPX/SPX Parameters

2. For the Nickname List File Name field, type the name of a file that defines, by adapter address and nickname, targets registered with this LAN directory. This field is optional. The nickname list file name is 1-8 characters, with a 0-3 character extension. It is installed in the same directory in which DCAF is installed. The default name for the nickname list file is EQNLDIPX.DAT. The DCAF sample file included in the DCAF diskettes is EQNLDIPX.TXT.

3. Select the Autostart communication check box to start IPX/SPX automatically when you start the LAN directory. This choice is optional.

To personalize the LAN directory during installation, perform the following steps:

1. On the Installation Mode window (Figure 11 in topic 2.1.1.1), choose **Personalize**, and press the **OK** push button. To change your personalization choices, choose **Change personalization parameters...** from the Install pull-down menu.

2. Begin with Step 2 and complete all the steps in the previous procedure.

2.7.2.4 Updating the LAN Directory Name

The utility EQNRPLLD.EXE updates the LAN Directory name for the LAN directory, gateway, and OS/2 target.

Because the LAN directory name has a maximum length of 12 characters, DCAF truncates longer names to the first 12 characters. The string is case sensitive.

Start this program from the directory in which the DCAF is installed. When the process is complete, restart the workstation.

For example, to change the LAN directory name to LANNEW, type the following:

<drive>:\<directory>\EQNRPLLD LANNEW

2.7.3 Personalizing the DCAF Gateway

You can personalize the following parameters:

- Log file
- Enable secure gateway

- Authenticator name

- Session number

- LAN parameters

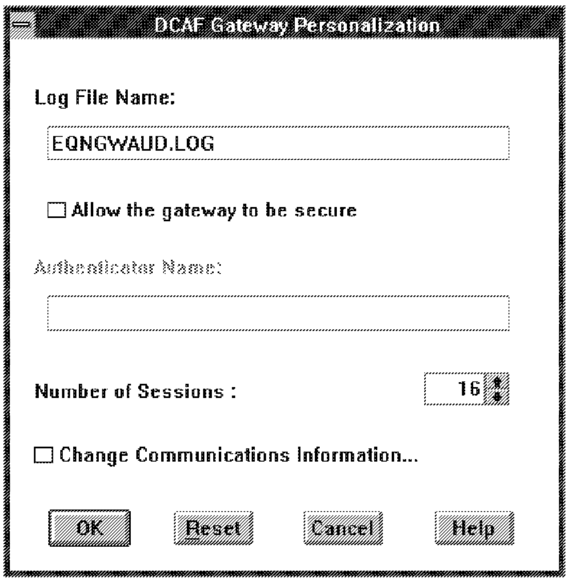
- Authenticator name for secure gateways. DCAF provides a utility that enables you to personalize the authenticator name for secure gateways once from the command line.

- LAN directory name. DCAF provides a utility that enables you to personalize the LAN directory name once from the command line. See "Updating the LAN Directory Name" in topic 2.7.2.4.

To personalize the gateway after it is installed, perform the following steps:

1. Open the Distributed Console Access Facility from your desktop and choose **Gateway Personalization**.

2. The DCAF Gateway Personalization window (Figure 43) appears.



PICTURE 43

Figure 43. DCAF Gateway Personalization

For Log File Name, type the name of the log file that tracks error and informational messages as an audit trail for secure and password-only sessions.

- The log file name is 1-8 characters, with a 0-3 character extension.

- The log file is created in the same directory where the DCAF product is installed. The default message log file name for the DCAF gateway workstation is EQNGWAUD.LOG.

3. To designate the DCAF gateway for secure sessions with controllers, select Allow the gateway to be secure. This option is available during installation only. To change it, you must deinstall and reinstall the DCAF. If you select this option, you must supply the adapter addresses for a primary and a secondary security authenticator of the secure target. See Figure 16 in topic 2.1.1.2 (direct installation) and Figure 31 in topic 2.2.1 (packaging) for descriptions.

If you do not select this option, password-only security will be used. See Figure 15 in topic 2.1.1.2 (direct installation) and Figure 30 in topic 2.2.1 (packaging) for descriptions.

4. For Authenticator Name, type the name of the authenticator on the LAN that authenticates secure sessions that are routed through the secure DCAF gateway. This option is available during installation only. To change it, use the utility EQNRPLAN.EXE. See "Updating the Authenticator Name for Secure Workstations" in topic 2.7.3.2.

   - The name must match the name assigned to the security authenticator. See Figure 25 in topic 2.1.1.4.6 for a description of the security authenticator name field that is defined during the security authenticator installation.

   - The name is 1-12 characters.

   - It cannot be a single asterisk (*) or all blanks.

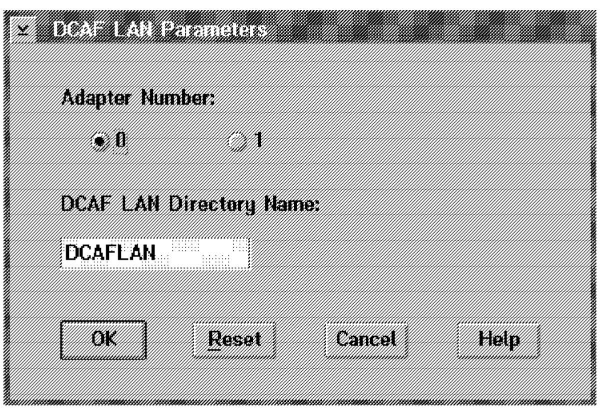
5. Choose the number of DCAF gateway sessions (1 to 254) between the DCAF gateway workstation and the controllers that can simultaneously occur at the DCAF gateway.

   - The default number of sessions is 16.

   - Choosing the number of sessions is actually designating NetBIOS resources to be reserved for the sessions. If there is an insufficient number of NetBIOS resources, you may need to increase the number of available NetBIOS resources in the OS/2 Communications Manager.

6. To change the gateway options for NetBIOS connections, select the Change Communications Information... check box and press the **OK** push button. The DCAF LAN Parameters window appears. See Figure 44 in topic 2.7.3.1.

2.7.3.1 DCAF LAN Parameters



PICTURE 44

Figure 44. DCAF LAN Parameters

When you use the NetBIOS communication protocol for your DCAF gateway workstation on the LAN, you can personalize (Figure 44) three DCAF LAN parameters:

1. The LAN adapter number for your workstation. It can be 0 or 1. The default is 0.

2. The DCAF LAN directory name. It is the name assigned to the LAN

directory with which the DCAF gateway workstation registers. The LAN directory keeps an internal list of names of the DCAF-enabled target workstations and also contains the nickname file list. Each DCAF gateway workstation is registered with one DCAF LAN directory. If there is more than one LAN directory on a logical LAN, the DCAF LAN directory names must be unique.

- The DCAF LAN directory name is 1-12 characters.
- It cannot be a single asterisk (*) or all blanks.
- It is case sensitive.
- The default name for the LAN directory name is DCAFLAN.

For these changes to take effect, shut down and restart the DCAF gateway workstation.

To personalize the DCAF gateway during installation, perform the following steps:

1. On the Installation Mode window (Figure 11 in topic 2.1.1.1), choose **Personalize** and press the **OK** push button. To change your personalization choices, choose **Change personalization parameters...** from the Install pull-down menu.

2. Begin with Step 2 and complete all the steps in the previous procedure.

2.7.3.2 Updating the Authenticator Name for Secure Workstations

The utility EQNRPLAN.EXE updates the authenticator name for secure gateways and authenticators.

Since the authenticator name has a maximum length of 12 characters, DCAF truncates longer names to the first 12 characters. The string is case sensitive.

Start this program from the directory in which the DCAF is installed. When the process is complete, restart the workstation.

For example, to change the authenticator name to AUTHNEW, type the following:

```
<drive>:\<directory>\EQNRPLAN AUTHNEW
```

2.7.4 Personalizing the Security Administrator

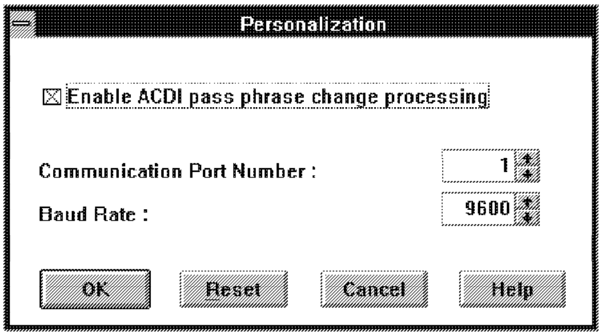
The following ACDI parameters can be personalized:

- Enable pass phrase change
- Communication port number
- Baud rate

To personalize the security administrator after it is installed, perform the following steps:

1. Choose **Personalization...** (or Ctrl+P shortcut key) from the **Options** pull-down menu on the DCAF Security Administrator main window.

2. The Personalization window (Figure 45) appears.



PICTURE 45

Figure 45. Security Administrator Personalization

If you select the check box, then you enable Pass phrase changes for the ACDI communication. You must select this box to be able to change the other parameters.

3. Choose the communication port number for the asynchronous serial port where the modem is attached. The values are 1-3.

4. Choose the baud rate (modem transmission rate). For asynchronous connections, use the highest line speed supported by your modem.

   The values are 1200, 2400, 4800, 9600, 19200, 38400, 48000, 56000, 57800, or 64000. The default is 9600.

5. Press the **OK** push button.

To personalize the security administrator during installation, perform the following steps:

1. On the Installation Mode window (Figure 11 in topic 2.1.1.1), choose **Personalize** and press **OK**. To change your personalization choices, choose **Change personalization parameters...** from the Install pull-down menu.

2. Begin with Step 2 and complete all the steps in the previous procedure.

2.7.5 Personalizing the Security Authenticator

You can personalize the following parameters:

- Adapter number

- Authenticator name

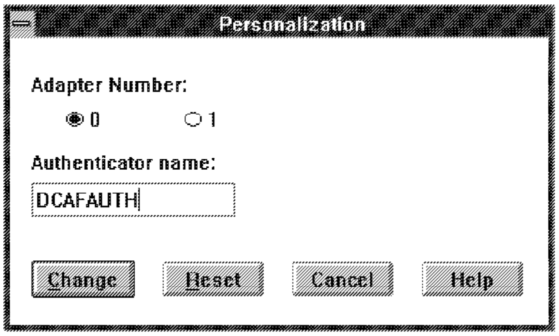
- Authenticator name from the command line. DCAF provides a utility that performs this task once. See "Updating the Authenticator Name for Secure Workstations" in topic 2.7.3.2.

.

To personalize the security authenticator after it is installed, perform the following steps:

1. Choose **Personalization...** from the **Options** pull-down menu on the DCAF Security Authenticator main window (Figure 148 in topic 4.2.2.3).

2. The Personalization window (Figure 46) appears.



PICTURE 46

Figure 46. Security Authenticator Personalization

3. Choose the LAN adapter number. It can be 0 or 1. The default is 0.

4. Type the authenticator name of the unique DCAF security authenticator.

   - The authenticator name can be 1-12 characters in length.

   - Any character is valid characters except a single asterisk (*) or all blanks.

   - It is not case sensitive even if it is displayed in uppercase.

   Note: The name for the security authenticator that you type must match the security authenticator name that you entered during the personalization of the gateway.

   To change the authenticator name from the command prompt, use the utility EQNRPLAN.EXE. See ″Updating the Authenticator Name for Secure Workstations″ in topic 2.7.3.2.

5. Press the **Change** push button.

To personalize the security authenticator during installation, perform the following steps:

1. On the Installation Mode window (Figure 11 in topic 2.1.1.1), choose **Personalize** and press the **OK** push button. To change your personalization choices, choose **Change personalization parameters...** from the Install pull-down menu.

2. Begin with Step 2 and complete all the steps in the previous procedure.

2.8 Personalizing the DCAF Targets

Most DCAF components can be personalized during direct installation, during creation of an installation package, or when you are using the component.

Some personalization options, such as making components secure, are available only during installation and packaging. These are noted for each component.

To personalize an installation package, perform the following steps:

1. Choose the component from the Distributed Console Access Facility Packager main window.

2. On the Packaging Mode window (Figure 27 in topic 2.2.1), choose **Personalize** and press the **OK** push button. You can go on to personalize the component.

To change personalization options before you install DCAF components or create installation packages, perform the following steps:

1. Select the component that you want to personalize again.

2. Choose **Change personalization parameters...** from the pull-down menu. You can go on to personalize the component.

Each personalization window has the following push buttons:

- **Reset**, which returns the last saved values.
- **OK**, which validates your choices.
- **Help**, which gives you online window help.
- **Cancel**, which closes the current operation and returns you to the previous window.

Not all changes take effect immediately. Table 6 shows when each change takes effect.

Table 6. Target Personalization Options

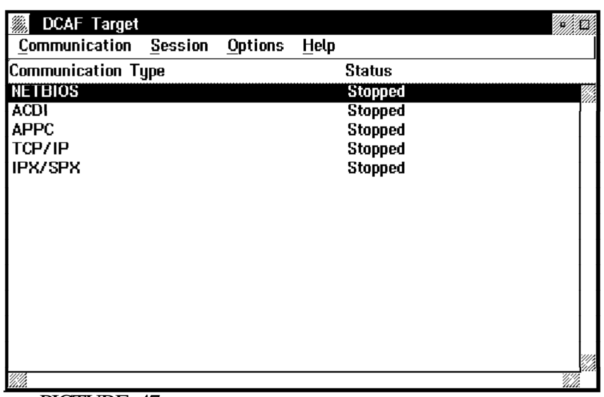
Option	**Takes Effect**
Allow the target to terminate a session	With the next session
Start DCAF sessions in Active Mode	With the next session
DCAF NetBIOS Parameters	Next time you open NetBIOS communications
DCAF TCP/IP Parameters	Next time you open TCP/IP communications
DCAF IPX/SPX Parameters	Next time you open IPX/SPX communications
DCAF Asynchronous Parameters	Next time you open asynchronous communications
Status Indicator	With the next session
DCAF Message Information	With the next session
Hot Keys	With the next session

2.8.1 Personalizing the OS/2 Target

You can personalize the following parameters:

- Enable target to terminate session
- Enable target security
- Start sessions in active mode
- Refresh rate
- DCAF NetBIOS parameters
- DCAF TCP/IP parameters
- DCAF IPX/SPX parameters
- DCAF ACDI parameters
- Status indicator attributes
- Hot Keys. Enable or install the hot key either during direct installation or the creation of an installation package only. It cannot be enabled or installed when it is already installed.
- Message Information
- Access Levels (for basic or password-only sessions). This option is available during direct installation or the creation of an installation package only.
- Authenticator adapter addresses for secure targets. DCAF provides a utility that enables you to change the authenticator adapter addresses for secure targets once from the target command line.
- LAN directory name. DCAF provides a utility that enables you to change the LAN directory name assigned to OS/2 targets once from the command line. See "Updating the LAN Directory Name" in topic 2.7.2.4.

After you have personalized the target options, refer to Table 6 in topic 2.8 to know when these changes will take effect.



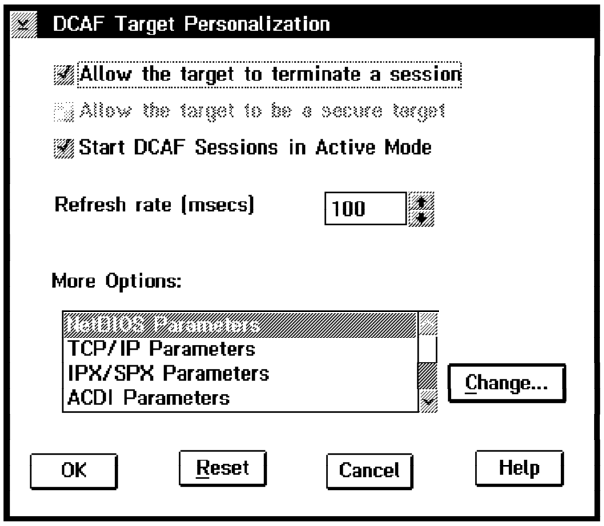
PICTURE 47

Figure 47. DCAF OS/2 Target Main Window with Options Pull-Down Menu

To personalize the OS/2 target after it is installed, perform the following steps:

1. On the DCAF Target window, choose **Personalization...** from the **Options** pull-down menu as shown in Figure 47.

2. The Target for OS/2 Personalization window (Figure 48) appears.



PICTURE 48

Figure 48. DCAF Personalization for OS/2 Target

To select one or more of the three check boxes, press the spacebar or click on the box with the mouse. The Target for OS/2 Personalization window (Figure 48) contains the following choices:

- Allow the target to terminate (end) a session with a controller only if the hot key combination is enabled. This option is available only if you enable a hot key combination. To enable and personalize the hot key combination, see "Hot Key Information" in topic 2.8.1.6.

- Allow the target workstation to be a secure target. You can choose this option only when you are installing directly or creating an installation package. It can only be changed if you deinstall and then reinstall it.

  If you make the target secure:

  - The option to personalize Access Levels Table for password-only or nonsecure OS/2 target workstations is not available.

  - During direct installation or the creation of an installation package, designate the authenticator adapter addresses for a primary and a secondary security authenticator for the target workstation.

  If the target is not secure:

  - You can personalize the Access Levels Table for password-only or nonsecure OS/2 target workstations.

  - During direct installation or the creation of an installation package, you will be asked for the DCAF password.

- Start DCAF Session in Active Mode. If you do not choose this option, the target workstation will start up in the monitoring state. That is, the controller views the target display but does not control the target input.

- Refresh rate (msecs).

  The interval between updates of your screen that are sent to the controller display. If the connection with the controller is slow or has heavy traffic increase the value. If you enter a higher value, the screen updates are sent to the controller display less frequently.

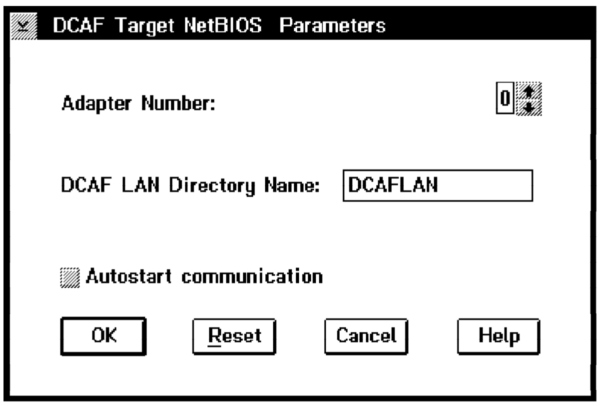
  The default is 100 milliseconds.

  The range, in multiples of one hundred, is from 100 to 4000.

3. To personalize an option in the More Options list box, select it, and press the **Change** push button. Each of these options is discussed on the following pages.

4. When you have completed personalizing the OS/2 target, press the **OK** push button to make your entries valid.

2.8.1.1 DCAF NetBIOS Parameters



PICTURE 49

Figure 49. DCAF NetBIOS Parameters

When you use the NetBIOS communication protocol for your target workstation on the LAN, you can personalize (Figure 49) the following DCAF NetBIOS parameters:

- Adapter Number.

  The range is 0-3. The default is 0.

- The DCAF LAN directory name. It is the name assigned to the LAN directory with which the target workstation registers. The LAN directory keeps an internal list of names of the DCAF-enabled target workstations and also contains the nickname file list. Each target workstation is registered with one DCAF LAN directory. If there is more than one LAN directory on a logical LAN, the DCAF LAN directory names must be unique.

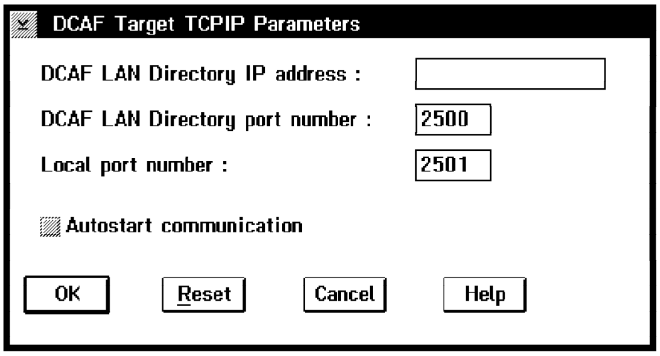
  - The DCAF LAN directory name is 1-12 characters.

  - It can be all characters; it cannot be a single asterisk (*) or all blanks, and it is case sensitive.

  - The default name for the LAN directory name is DCAFLAN.

- Select the Autostart communication check box to start NetBIOS automatically when you start the target.

2.8.1.2 DCAF - TCP/IP Parameters



PICTURE 50

Figure 50. DCAF TCP/IP Parameters

To personalize the DCAF TCP/IP parameters (Figure 50) for communication with a target using the TCP/IP protocol, make your choice for the following options:

- DCAF LAN Directory IP address

  The address assigned to the LAN directory during TCP/IP installation. It is a string composed of four substrings of numbers, divided by a period (nnn.nnn.nnn.nnn.). The range for each substring is 1-255.

- DCAF LAN Directory port number

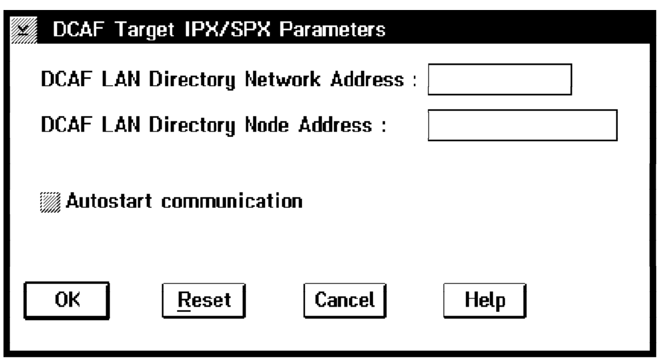
  The port number assigned to the LAN directory during installation. The range is 1024-65 534. The default is 2500.

- Local port number

  The port number assigned to the target. The range is 1024-65 534. The default is 2501.

- Select the Autostart communication check box to start TCP/IP automatically when you start the target.

2.8.1.3 DCAF - IPX/SPX Parameters



PICTURE 51

Figure 51. DCAF IPX/SPX Parameters

To personalize the DCAF IPX/SPX parameters (Figure 51) for communication with a target using the IPX/SPX protocol, make your choice for the following options:

- DCAF LAN Directory Network Address

  A unique hexadecimal number that identifies the network that the LAN directory workstation is on to the target. It must be exactly 8 digits in length in any combination of hexadecimal numbers.

  Character guidelines for hexadecimal format:

  - It is exactly 8 characters in length.
  - Upper- or lowercase letters (A-F, a-f).
  - Digits (0-9).
  - The range is 00000000-FFFFFFFE.

- DCAF LAN Directory Node Address

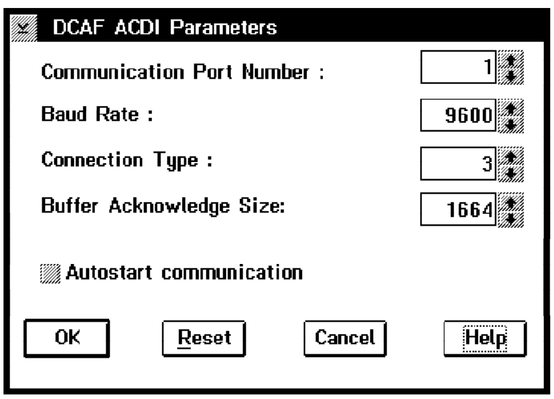
  A unique hexadecimal number that identifies the LAN directory workstation to the network that it is on. Typically, it matches the adapter address of the LAN directory. It must be exactly 12 digits in length in any combination of hexadecimal numbers.

  Character guidelines for hexadecimal format:

  - It is exactly 12 characters in length.
  - Upper- or lowercase letters (A-F, a-f).
  - Digits (0-9).
  - The range is 000000000000-FFFFFFFFFFFF.

- Select the Autostart communication check box to start IPX/SPX automatically when you start the target.

2.8.1.4 DCAF ACDI Parameters



PICTURE 52

Figure 52. DCAF ACDI Parameters

When you use the asynchronous communication protocol for your target workstation, you can personalize (Figure 52) the following DCAF ACDI parameters:

- The asynchronous serial (communication) port number (1-3). The default is port number 1.

- The modem baud rate in bits per second. For asynchronous connections, use the highest line speed supported by your modem for best performance.

  The values are 1200, 2400, 4800, 9600, 19200, 38400, 48000, 56000, 57800, or 64000. The default value is 9600 baud.

- The number of the connection type (1 and 3).

  - Type 1 is the manual connection with the answer frequency. It responds to a manual connection with the answer frequency.

- Type 3 is automatic data answering. It responds to automatic data dialing with automatic data answering.

The default DCAF connection type value is Type 3.

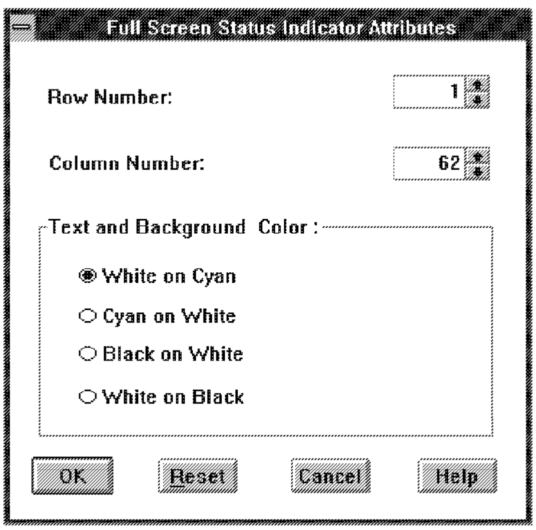
- The buffer acknowledge size enables the target to send a specific amount of data to the controller and wait for the controller's acknowledgment before it sends new data. If you enter a higher value, you improve the performance but decrease the stability of the session. Use a higher value if you use a high speed modem (for example, faster than 19200 bps).

  If you enter a lower value, you increase the stability but lower the performance of the session. Use a lower value if you do not use a high speed modem.

  The default is 1664 bytes.

  The range, in multiples of 128, is from 128 to 8192.

2.8.1.5 Full Screen Status Indicator Attributes



PICTURE 53

Figure 53. Full Screen Status Indicator Attributes

The Full Screen Status Indicator Attributes window (Figure 53) allows you to change the position and the color of the DCAF status indicator. The status indicator displays the current state of operation (for example, active or monitoring). The indicator itself is 18 columns wide and 1 row high. To change the position where the status indicator is displayed, you select both of the following:

- Row number (0-60) with the default of 1
- Column number (1-116) with the default of 62.

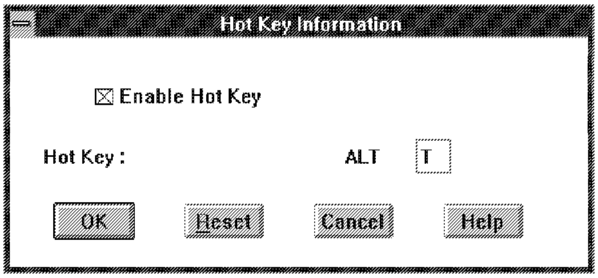
It is recommended that you choose row number 1 for applications that scroll. If you have non-scrolling applications, you may choose a different row. If you choose row 0, then no status indicator is displayed.

Note: These are the maximum values supported by the OS/2 mode command. Your actual maximums may differ depending on the display type and the display driver used at the target workstation.

You can also choose the color of the text and background for the status indicator. The foreground and background colors are:

- White on Cyan (the default)
- Cyan on White
- Black on White
- White on Black

2.8.1.6 Hot Key Information



PICTURE 54

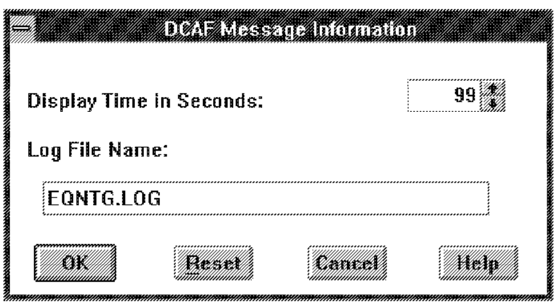
Figure 54. OS/2 Target Hot Key Information

The Hot Key Information window (Figure 54) allows you to enable a hot key combination for the OS/2 target workstation user and also define the hot key combination. If the **Enable Hot Key** check box is selected, then the OS/2 target workstation user is given permission to interrupt and change the current state of operation (for example, from active to monitoring).

The hot key combination is composed of the Alt key and another key of your choice (A-Z) pressed simultaneously. The default hot key combination is Alt+T.

The hot key is enabled either during direct installation or the creation of an installation package only. If the hot key is not enabled, you cannot personalize this option when you are using the target, and the **Allow a target to terminate a session** option is disabled.

2.8.1.7 DCAF Message Information



PICTURE 55

Figure 55. DCAF Message Information

When informational and error messages are displayed on the target workstations, you can customize (Figure 55) how they are handled. You can personalize the length of time that the message is displayed.

- The range is from 0-99 seconds.

- The default (99) displays the message indefinitely until it is acknowledged by the user.

- If you choose 0 seconds, the message will not be displayed.

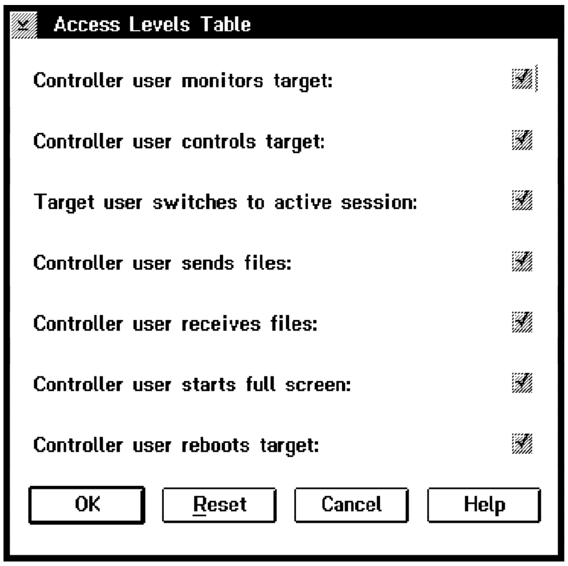
You can personalize the name of the log file that tracks informational and error messages for the OS/2 target workstation.

- The log file name is 1-8 characters with a 0-3 character extension.

- Do not use BAT, CMD, COM, DAT, DIR, DLL, EXE, or REC as the file extension.

- The log file is created where the DCAF product is installed. The default log file name for the OS/2 target workstation is EQNTG.LOG.

2.8.1.8 Access Levels Table



PICTURE 56

Figure 56. Access Levels Table

When the session with the OS/2 target workstation is password-only or nonsecure, you can personalize (Figure 56) the access levels (privileges) for the session between the controller and the OS/2 target workstation. This personalization option is available during direct installation or the creation of an installation package only. The default is that all of the seven check boxes are selected. For a description of the session states, see the User's Guide.

If you select the check boxes by pressing the spacebar or clicking the mouse, then you give permission for the following:

1. Controller monitors target. The controller can monitor the target workstation when it is in the monitoring state. When the controller monitors the target workstation, the target workstation keyboard remains unlocked.

2. Controller controls target. The controller can control the target workstation during an active DCAF session. The target keyboard is locked in the active state.

3. Target user switches to active session. The target workstation user can switch the DCAF session to the active state. To choose this privilege, you must also select either Controller monitors target, or Controller controls target.

4. Controller sends files. The controller can send files to the target workstation. To choose this privilege, you must also select either

Controller monitors target, or Controller controls target.

5. Controller receives files. The controller can receive files from the target workstation. To choose this privilege, you must also select either Controller monitors target, or Controller controls target.

6. Controller starts full screen. The controller can initiate a full-screen session on the target workstation. To choose this privilege, you must also select Controller controls target.

7. Controller reboots target. The controller can restart the target workstation. To choose this privilege, you must also select Controller controls target.

To personalize the OS/2 target during installation, perform the following steps:

1. On the Installation Mode window (Figure 11 in topic 2.1.1.1), choose **Personalize** and press the **OK** push button. To change your personalization choices, choose **Change personalization parameters...** from the Install pull-down menu.

2. Begin with Step 2 in topic 2.8.1 and complete all the steps in the previous procedure.

2.8.1.9 Updating the Authenticator Adapter Addresses on Secure Targets

The utility EQNRPLAA.EXE updates the authenticator adapter addresses for secure targets. It updates two parameters, the primary and secondary authenticator adapter addresses for the secure target.

The first parameter is required, the second is optional. If you specify only the first parameter, DCAF assumes that the second parameter matches the first. If you include more than two parameters, DCAF accepts only the first two.

Parameters must be exactly 12 hexadecimal characters in length. DCAF truncates longer names to the first 12 characters. The strings must be valid adapter addresses.

In order to start this utility successfully, type *** for both the primary and secondary authenticator adapter addresses when you install a target or when you create the package for it.

Important:

- Make sure that the target is not running when you start EQNRPLAA.
- Start EQNRPLAA from the directory in which the DCAF is installed.
- Run EQNRPLAA on the same target only once.

For example, to change the primary authenticator adapter address to 10005AAE9167 and the secondary authenticator adapter address to 400000000001, type the following:

```
<drive>:\<directory>\EQNRPLAA 10005AAE9167 400000000001
```

2.8.2 Personalizing the Windows Target

You can personalize the following parameters:

- Enable target to terminate session

- Enable target security

- Start sessions in active mode

- DCAF NetBIOS parameters

- DCAF TCP/IP parameters
- DCAF IPX/SPX parameters
- DCAF asynchronous parameters
- Status indicator attributes
- Hot Keys. Enable or install the hot key either during direct installation or the creation of an installation package only. It cannot be enabled or installed when it is already installed.
- Message Information
- DOS options
- Authenticator adapter addresses for secure targets. DCAF provides a utility that performs this task once from the target command line. See "Updating the Authenticator Adapter Addresses on Secure Targets" in topic 2.8.1.9.

After you have personalized Windows target options, refer to Table 6 in topic 2.8 to know when these changes will take effect.

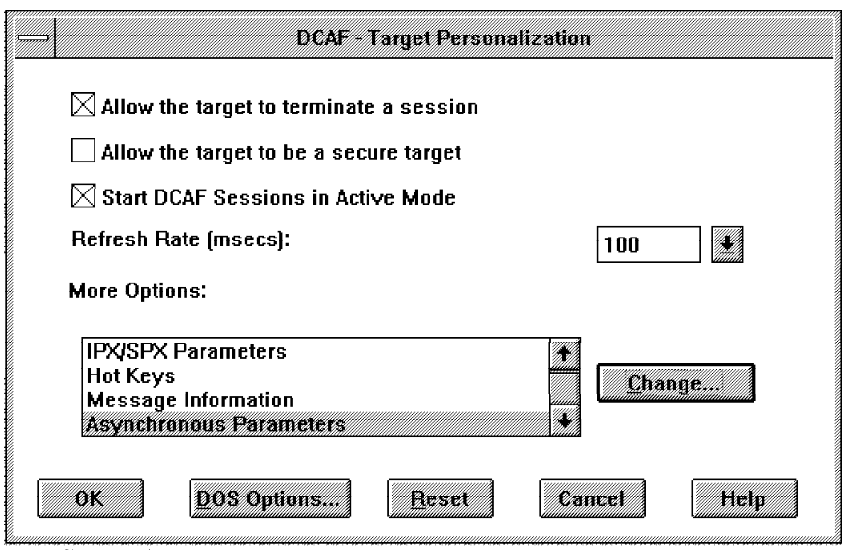
2.8.2.1 In the Windows Environment

To personalize the setup options on the Windows target after it is installed, perform the following steps:

1. On the DCAF Target window, choose **Personalization...** from the Options drop-down menu (see the Distributed Console Access Facility Target User's Guide).

2. The DCAF Target Personalization window (Figure 57) appears.

   Some options (they will be identified when they are described) can be personalized only during installation or packaging. After the Windows target has been installed, to change these options, you must deinstall the Windows target and reinstall it with the new personalized options.



PICTURE 57

Figure 57. DCAF Personalization for Windows Target

On the DCAF Target Personalization window (Figure 57) there are the following choices:

To select one or more of the three check boxes, press the spacebar or click on the box with the mouse.

- Allow the target workstation to terminate a session. This option is available only if you enable a hot key combination. To enable and personalize the hot key combination, see "Hot Key Information" in topic 2.8.2.1.5.

- Allow the target workstation to be a secure target. You can choose this option only when you are installing directly or creating an installation package. If you choose this option, the Security Data window (see Step 8 in topic 2.3.2) appears after you choose the **OK** button. To change this option, you must deinstall the and then reinstall it. To deinstall the Windows target, see "Deinstalling the Windows Target" in topic 2.3.4.

  If you do not make the target secure, you will be asked to provide the DCAF password (see Step 10 in topic 2.3.2).

- Start DCAF Sessions in Active Mode. Otherwise, the target starts in monitoring mode. That is, the controller views the target display but does not control the target input.

- Refresh rate (msecs). The interval between updates of your screen that are sent to the controller display. If the connection with the controller is slow or has heavy traffic increase the value. If you enter a higher value, the screen updates are sent to the controller display less frequently.

  The default is 100 milliseconds.

  The range, in multiples of one hundred, is from 100 to 4000.

To personalize the selections in the More Options list box, perform the following steps:

1. Select the option you want to personalize by scrolling through the list.

2. Press the **Change...** button.

   One of the following windows appears:

   - NetBIOS Parameters
   - TCP/IP Parameters
   - IPX/SPX Parameters
   - Asynchronous Parameters
   - Hot Keys
   - Message Information

3. Select the appropriate options and type in, where applicable, the requested information.

4. When you have completed personalizing the option, choose the **OK** button.

   The DCAF Target Personalization window reappears. Repeat these steps for each of the options that you want to personalize.

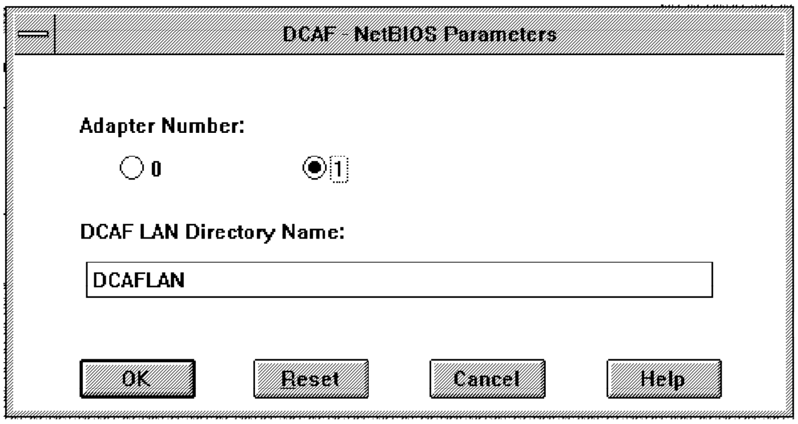
5. To personalize options for the Windows target when it is running in native DOS, press the **DOS Options...** push button on the DCAF Target Personalization window. The DCAF DOS Options window appears. For details and instructions, see "In Native DOS" in topic 2.8.2.2.

6. When you have completed personalizing all the options for the Windows target, press the **OK** button on the DCAF Target Personalization window to make your entries valid.

To undo your selections and return to the last saved selections on a window, press the **Reset** button.

To cancel an operation and return to the previous window, choose the **Cancel** button.

2.8.2.1.1 DCAF - NetBIOS Parameters



PICTURE 58

Figure 58. DCAF NetBIOS Parameters

To personalize the DCAF NetBIOS parameters (Figure 58) for when you use the NetBIOS protocol to communicate with a target on the LAN, make your choice for the following options:

- Adapter Number

  This is part of the LAN profile configuration on your workstation. To choose the LAN adapter you want to set up on your workstation, select the radio button for Adapter Number.

  The range is 0-3. The default is 0.

- DCAF LAN directory name

  The DCAF LAN directory keeps an internal list of the LAN target workstation names. Each target workstation on a LAN must be registered with one DCAF LAN directory if it will be accessed through a DCAF gateway. If you want to have more than one LAN directory name on one logical LAN, then each directory must have a unique name.

  In the text box, type the DCAF LAN directory name.

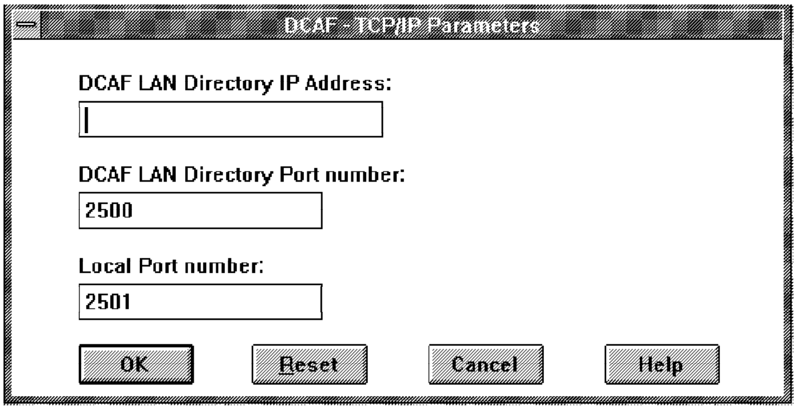
  Character guidelines:

  - It is 1-12 characters.

  - All characters except a single asterisk (*) or all blanks. It is case sensitive.

  - The default is DCAFLAN.

2.8.2.1.2 DCAF - TCP/IP Parameters



PICTURE 59

Figure 59. DCAF TCP/IP Parameters

To personalize the DCAF TCP/IP parameters (Figure 59) for communication with a target using the TCP/IP protocol, make your choice for the following options:

- DCAF LAN Directory IP address

  The address assigned to the LAN directory during TCP/IP installation. It is a string composed of four substrings of numbers, divided by a period (nnn.nnn.nnn.nnn.). The range for each substring is 1-255.

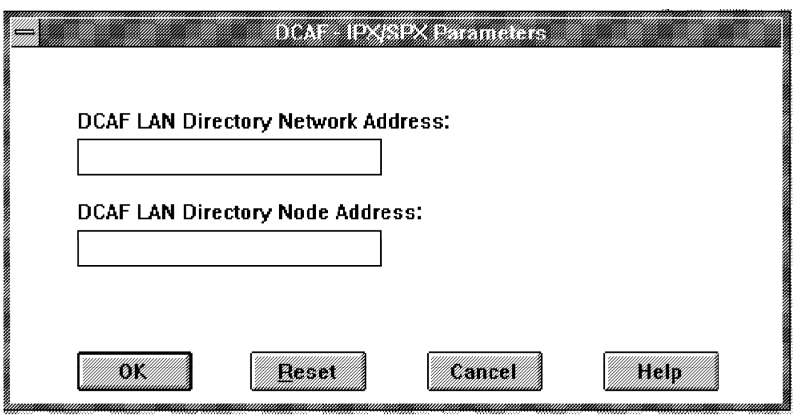
- DCAF LAN Directory port number

  The port number assigned to the LAN directory during installation. The range is 1024-65 534. The default is 2500.

- Local port number

  The port number assigned to the target. The range is 1024-65 534. The default is 2501.

2.8.2.1.3 DCAF - IPX/SPX Parameters



PICTURE 60

Figure 60. DCAF IPX/SPX Parameters

To personalize the DCAF IPX/SPX parameters (Figure 60) for communication with a target that is using the IPX/SPX protocol, make your choice for the following options:

- DCAF LAN Directory Network Address

  A unique hexadecimal number that identifies the network that the LAN directory workstation is on to the target. It must be exactly 8 digits in length in any combination of hexadecimal numbers.

Character guidelines:

- Upper- or lowercase letters (A-Z, a-z)
- Digits (0-9)
- The range is 000000000-FFFFFFFE.

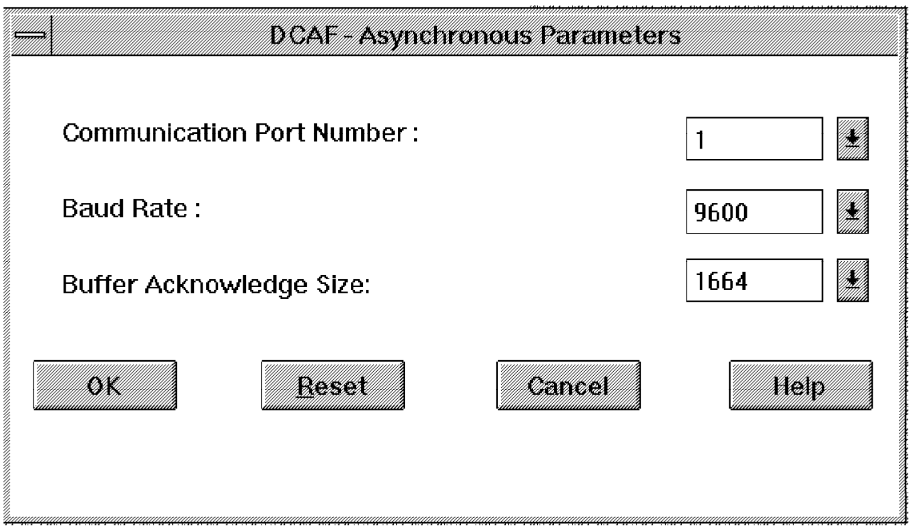
- DCAF LAN Directory Node Address

  A unique hexadecimal number that identifies the LAN directory workstation to the network that it is on. Typically, it matches the adapter address of the LAN directory. It must be exactly 12 digits in length in any combination of hexadecimal numbers.

  Character guidelines:

  - Upper- or lowercase letters (A-Z, a-z)
  - Digits (0-9)
  - The range is 000000000000-FFFFFFFFFFFF.

2.8.2.1.4 DCAF Asynchronous Parameters



PICTURE 61

Figure 61. DCAF Asynchronous Parameters

Note: DCAF supports modem connections with target workstations operating on Windows Version 3.1 only. If your workstation does not run on Windows Version 3.1, skip to the next section.

To personalize (Figure 61) the DCAF asynchronous parameters for when you use the modem (the asynchronous communication protocol) to communicate with your target workstation, make your choice for the following options:

- Communication Port Number

  This is the number of the asynchronous serial port to which the modem can be attached. Depending on the serial ports you have set up on your workstation to connect to modems, other terminals, and so on, you can decide which port to reserve for the asynchronous modem.

  In the Communication port number box, select using the arrows or type the value you want.

  The values are 1 to 3; the default is port number 1.

- Baud Rate

The modem transmission rate in bits per second. For asynchronous connections, use the highest line speed supported by your modem for best performance.

In the Baud rate field select, using the arrows or typing the value you want.

The values are 1200, 2400, 4800, 9600, 19200, 38400, or 56000.

The default value is 9600.

- Buffer Acknowledge Size

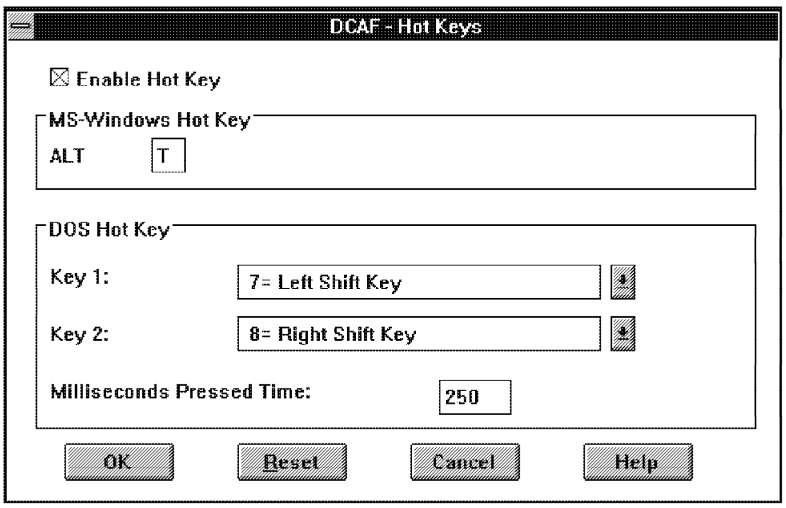
  Enables the target to send a specific amount of data to the controller and wait for the controller's acknowledgment before it sends new data. If you enter a higher value, you improve the performance but decrease the stability of the session. Use a higher value if you use a high speed modem (for example, faster than 19200 bps).

  If you enter a lower value, you increase the stability but lower the performance of the session. Use a lower value if you do not use a high speed modem.

  The default is 1664 bytes.

  The range, in multiples of 128, is from 128 to 8192.

2.8.2.1.5 Hot Key Information



PICTURE 62

Figure 62. DCAF - Hot Keys

To interrupt and change the current session state (for details on session states, see <u>Distributed Console Access Facility User's Guide</u>.), use the hot key combination. You can enable the hot key combination when you install directly or when you create an installation package. To enable the hot key combination manually after the is installed on your workstation, see "Manual Personalization" in topic APPENDIX1.5.1. However, it is recommended that you deinstall the Windows target and reinstall it with the hot key enabled.

To enable and personalize the hot key combinations for the target in both the Windows and DOS environments, choose Hot Key Information (Figure 62) from the DCAF Target Personalization window. To personalize the hot key combination for just one of the target environments, make your changes for the environment you want and keep the default option for the other.

- Enable Hot Key

  You must select this box if you want the hot key to be available. To enable the target workstation to unload the DCAF program from memory, you must enable the hot key also.

  This enables the hot key combinations for both the Windows target and the DOS target.

  To enable the target workstation user to interrupt a DCAF session and change the current state of operation, select the Enable Hot Key check box. Even if the hot key is not enabled, you can proceed to personalize both hot key combinations for future use.

- MS-Windows Hot Key

  The hot key combination for the Windows target workstation is composed of the Alt key and another alphabetical key of your choice pressed simultaneously. The default is Alt+T.

  To change the hot key combination for the Windows target workstation, type the value for the second key in the text box next to Alt.

  The range is from A to Z.

- DOS Hot Key

  The hot key combination for the native DOS target workstation is composed of any two keys listed here pressed simultaneously. The default key combination is Left Shift Key+Right Shift Key.

  To change them, scroll through the Key 1 and Key 2 text boxes.

  The choices for hot key combinations include:

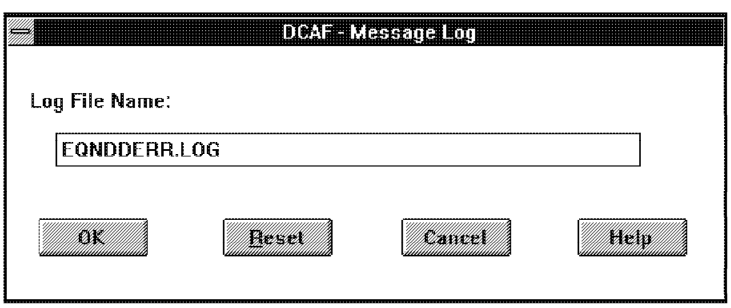
  Left Alt key, Right Alt key
  Left Control key, Right Control key
  Left Shift key, Right Shift key
  Caps Lock key
  Num Lock key
  Scroll Lock key
  System Request key

- Milliseconds Pressed Time

  This is the minimum amount of time (in milliseconds) that you must hold down the two keys together in order for them to be effective. The default time is 250 milliseconds.

  In the text box, type the Milliseconds Pressed Time. The range is from 50 to 9999.

2.8.2.1.6 DCAF Message Information



PICTURE 63

Figure 63. DCAF Message Log

To indicate the name of the log file (Figure 63) that tracks informational and error messages for the Windows target workstation, choose DCAF Message Information. The log file is created on the directory where the DCAF product is installed.

In the text box, type the log file name:

Character guidelines:

- It is 1-12 characters with a 0-3 character extension.

- Do not use BAT, CMD, COM, DAT, DIR, DLL, EXE, HLP, or REC as the file extension.

- The default is EQNDDERR.LOG.

2.8.2.2 In Native DOS

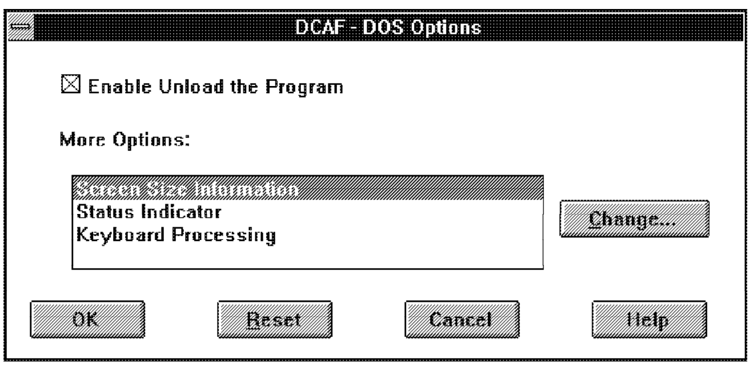
You can personalize the following parameters:

- Enable target to unload DCAF
- Screen size information
- Status indicator
- Keyboard processing

To personalize options for the Windows target when it is running in the DOS environment, perform the following steps:

1. Press the **DOS Options...** button on the DCAF Target Personalization window (Figure 57 in topic 2.8.2.1).

2. The DCAF DOS Options window appears.



PICTURE 64

Figure 64. Personalizing the DOS Options for a Windows Target

The DCAF DOS Options window (Figure 64), gives you the following choices:

- Enable Unload the Program

  This option enables you to erase the DCAF program from the workstation memory in native DOS. You can do this from a native DOS full screen only. The DCAF program will remain in memory for the Windows environment until you exit from Windows and return to a native DOS full-screen. For details on unloading the Windows target from the workstation memory, see the Distributed Console Access Facility User's Guide.

  To enable the DOS target workstation user to unload the DCAF program from the workstation memory, select the check box.

- You can personalize the items in the More Options list box.

To personalize the selections listed in the More Options list box, perform the following steps:

1. Select the option you want to personalize by scrolling through the list.

2. Press the **Change** button.

   One of the following windows appears:

   - Screen size information
   - Status indicator
   - Keyboard processing.

3. Select the appropriate options and type, where applicable, the requested information.

4. Press the **OK** button.

   The DCAF Options window reappears.

5. Repeat these steps for each option that you want to personalize.

6. When you have completed personalizing all the DOS options, press the **OK** button to make your entries valid.

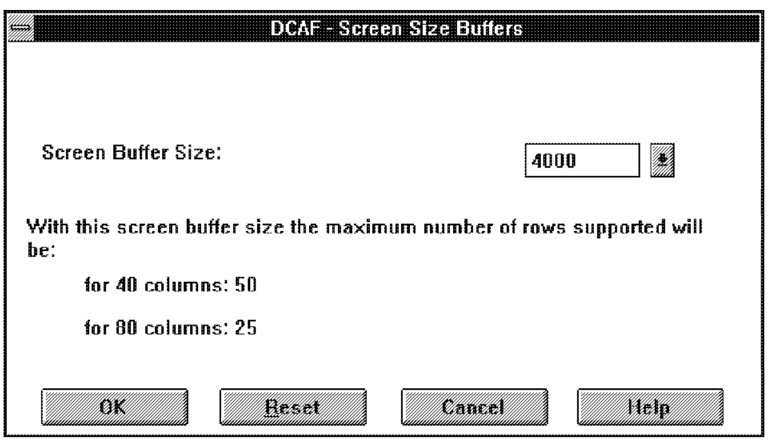
   The DCAF target Personalization window reappears.

7. If you have completed personalizing the options on this window, press the **OK** button. To continue personalizing options on the DCAF target Personalization window, see "In the Windows Environment" in topic 2.8.2.1.

To undo your selections and return to the last saved selections on a window, press the **Reset** button.

To cancel an operation and return to the previous window, choose the **Cancel** button.

2.8.2.2.1 Screen Size Information



PICTURE 65

Figure 65. DCAF - Screen Size Buffers

To change the size of the target workstation screen that will be displayed on the controller screen during a DCAF session, choose Screen Size Information (Figure 65).

The number of bytes that you choose for Screen Buffer Size determines the size (in columns and rows) of the target workstation screen that is displayed on the controller screen.

Your choice of bytes for Screen Buffer Size will affect the way applications work. If you choose a lower value, you will limit the size of the screen that will be seen on the controller workstation during a DCAF session. If you choose the maximum value of 8000 bytes for a screen size of 80 columns by 50 rows, the screen will use twice as much memory as the minimum value. This will reduce memory capacity for other applications and slow them down or even keep some of the applications from running on your workstation.

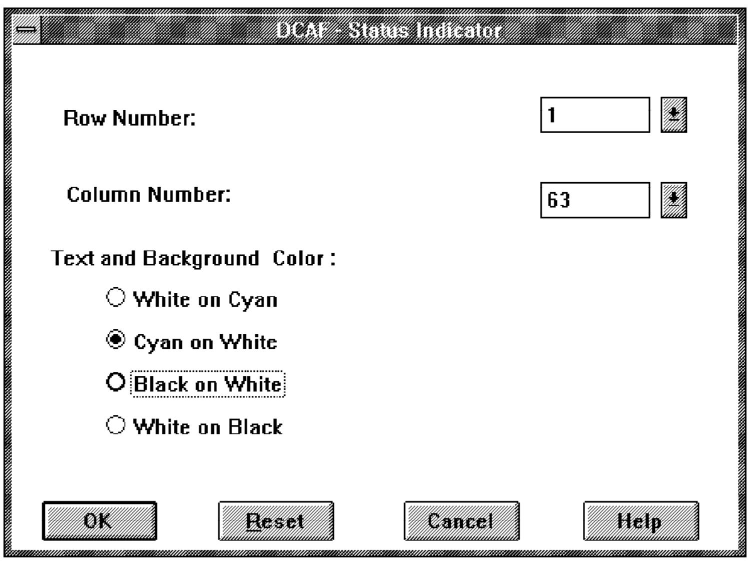
In the Screen Buffer Size box, choose the maximum number of bytes you want to use and you will see the corresponding number of rows supported for a screen of 40 columns and for a screen of 80 columns. The minimum number of bytes to support a screen of 80 columns is 4000. So, if you choose a lower value, the line for 80 columns will disappear.

- The values are 2000, 3440, 4000, 6880, and 8000 bytes.

  The default is 4000 bytes. This is the minimum number of bytes for characters needed for a screen of 80 columns and 25 rows.

- When you choose the size, the window will automatically display the maximum number of rows for a screen of 40 columns and 80 columns.

2.8.2.2.2 Status Indicator



PICTURE 66

Figure 66. DCAF - Status Indicator

To set the position and the color of the DCAF status indicator, choose Status Indicator (Figure 66). The status indicator displays a message that indicates the current state of operation (e.g., active or monitoring). The indicator itself is 18 columns wide and 1 row high. To change the position where the status indicator is displayed, designate both of the following:

- Row number

  For applications that scroll, it is recommended that you choose a value of 1. To keep the status indicator from being displayed, choose a value of 0.

  The range is from 0 to 50.

  The default is 1.

- Column number

  The range is from 1 to 63.

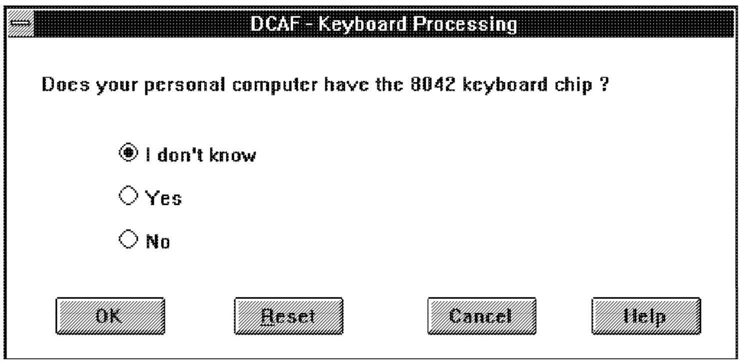
  The default is 63.

Note: These are the maximum values supported by the Windows mode command. The actual maximums for your workstation may differ depending on the display type and the display driver it uses.

To change the color of the text and background for the status indicator, select the foreground and background colors from the following:

- White on Cyan (the default)
- Cyan on White
- Black on White
- White on Black

2.8.2.2.3 Keyboard Processing



PICTURE 67

Figure 67. DCAF - Keyboard Processing

To choose how the keyboard input will be processed on the DOS target workstation, choose Keyboard Processing (Figure 67). For **Does your personal computer have the 8042 keyboard chip?** select your response from the following responses:

1. **I don't know**: If you choose this option, the DCAF program will run a test to see whether the 8042 chip is present and will attempt to use it. In most cases, this choice is appropriate. If the 8042 keyboard processing chip is present, the DCAF uses the keyboard-chip stuffing technique to handle the keystrokes that are typed. If the 8042 chip is not present, the DCAF program uses interrupt 16H to handle the keystrokes.

   I don't know is the default option.

2. **Yes**: If you choose this option, the DCAF program registers the keyboard input during a DCAF session directly on the workstation 8042 keyboard chip for the DOS applications. See "DOS Target Keyboard Processing" in topic APPENDIX1.4.4 for the DOS applications that the DCAF program does not support.

3. **No**: Choose this option if you know that your workstation does not have an 8042 keyboard chip. Smaller model PS/2 workstations do not have the 8042 chip. The DCAF supports applications that use software keyboard processing (interrupt 16H).

The type of keyboard processing that is being used by the DOS-Windows target is logged in the DOS target message log file. The default name for this file is EQNDDERR.LOG.

To personalize the setup options for the Windows target during installation or packaging,

1. On the DCAF - Target Installation Type window (Figure 32 in topic 2.3.1), select **Personalization** and press the **OK** push button.

2. Begin with Step 2 in topic 2.8.2.1 and complete all the steps in the previous procedure.

2.8.3 Personalizing the DOS Target

You can personalize the following parameters:

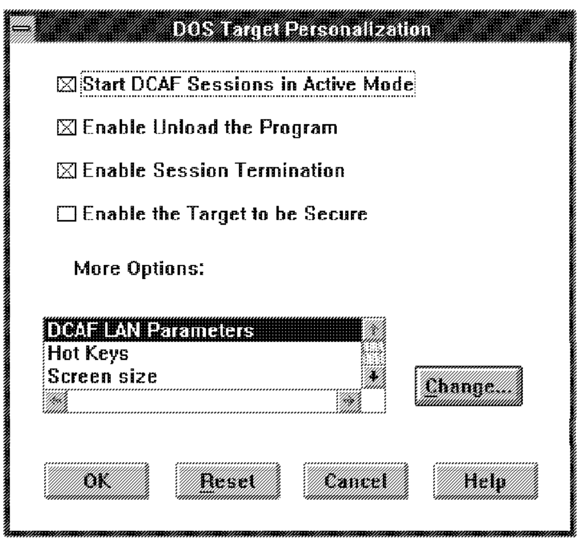
- Start sessions in active mode
- Enable target to unload DCAF
- Enable target to terminate session
- Enable target security
- LAN parameters
- Screen size
- Status indicator
- Log file
- Keyboard processing

The personalization options are available only during the creation of an installation package for the DOS target. The DOS Target can be chosen from the Distributed Console Access Facility Packager window. See "Creating an Installation Package" in topic 2.2.1.

To personalize the DOS target after it is installed, you must run the DCAF packager, create a new DOS target with the personalization choices you want, and reinstall the new DOS target component.

1. On the Packaging Mode window (Figure 27 in topic 2.2.1), choose **Personalize** and press the **OK** push button. To change your personalization choices, choose **Change personalization parameters...** from the Makepackage pull-down menu.

2. The DOS Target Personalization window (Figure 68) appears.



PICTURE 68

Figure 68. DOS Target Personalization

There are four personalization choices followed by More Options. Mark any of the four check boxes by pressing the spacebar or clicking on them with your mouse.

- Allow the target workstation to begin in active state at startup time. If you do not choose this option, the target workstation will start up in the monitoring state.

- Allow the DOS target to unload from memory.

- Allow the target workstation to end (terminate) a session with a controller.

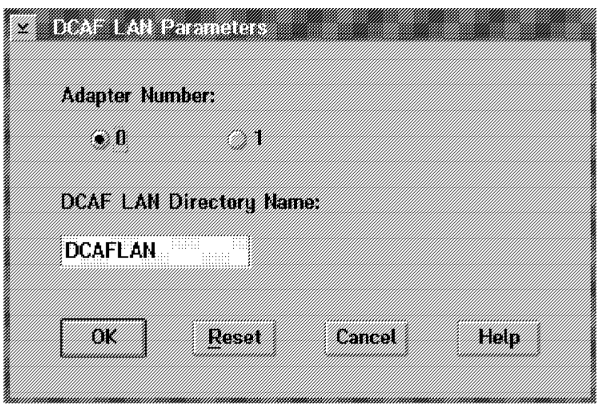
- Designate the target workstation as a secure target for secure-session security. If you select this option, designate the authenticator adapter addresses for a primary and a secondary security authenticator for the secure target workstation. See Figure 31 in topic 2.2.1 for a description.

  If you do not select this option, you will be asked to type a DCAF password. See Figure 30 in topic 2.2.1 for a description.

3. To personalize an option in the More Options list box, select it, and press the **Change...** push button. Each of these options is discussed on the following pages.

4. When you have completed personalizing the DOS target, press the **OK** push button to make your entries valid.

2.8.3.1 DCAF NetBIOS Parameters



PICTURE 69

Figure 69. DCAF LAN Parameters

The DOS target workstation uses the NetBIOS communication protocol on the LAN. You can personalize (Figure 69) the following DCAF LAN parameters:

- The LAN adapter number for your workstation.

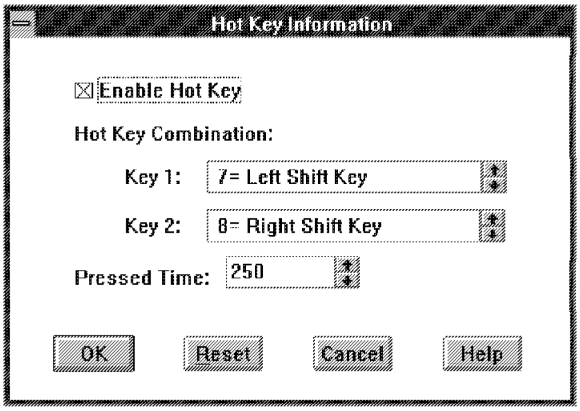
  It can be 0 or 1. The default is 0.

- The type of LAN adapter address for your workstation. It can be the locally administered address (LAA) or the universally administered address (UAA). The LAA is a unique user-defined address that is defined in the OS/2 Communications Manager. The UAA is a unique address name for the adapter preassigned by the manufacturer. The LAA is the default.

- The DCAF LAN directory name. It is the name assigned to the LAN directory with which the target workstation registers. The LAN directory keeps an internal list of names of the DCAF-enabled target workstations and also contains the nickname file list. Each target workstation is registered with one DCAF LAN directory. If there is more than one LAN directory on a logical LAN, the DCAF LAN directory names must be unique.

- The DCAF LAN directory name is 1-12 characters.
- It cannot be a single asterisk (*) or all blanks.
- It is case sensitive.
- The default name for the LAN directory name is DCAFLAN.

2.8.3.2 Hot Key Information



PICTURE 70

Figure 70. Hot Key Information

On the Hot Key Information window (Figure 70), there are the following personalization options:

- Enable a hot key combination for the DOS target workstation user.

  If the Enable Hot Key check box is marked, then the DOS target workstation user can interrupt and change the current state of operation (for example, from active to monitoring). **Enable Hot Key** is optional.

- Define the hot key combination.

  The hot key combination is composed of key 1 and key 2 pressed simultaneously. The default key combination is Left Shift Key + Right Shift Key.

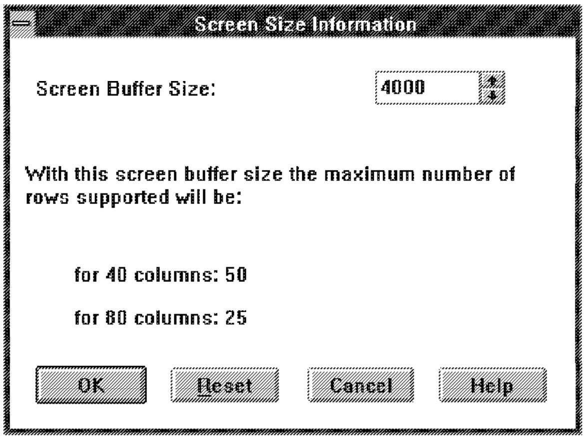
  The choices for hot key combinations include:

  Left Alt key
  Left Control key
  Left Shift key
  Right Alt key
  Right Control key
  Right Shift key
  Caps Lock key
  Num Lock key
  Scroll Lock key
  System Request key

- Define the minimum amount of time that the two keys must be pressed to be recognized as hot keys.

  You can choose the amount of time (in milliseconds) that the hot key combination is pressed. The default time is 250 milliseconds.

2.8.3.3 Screen Size Information



PICTURE 71

Figure 71. Screen Size Information

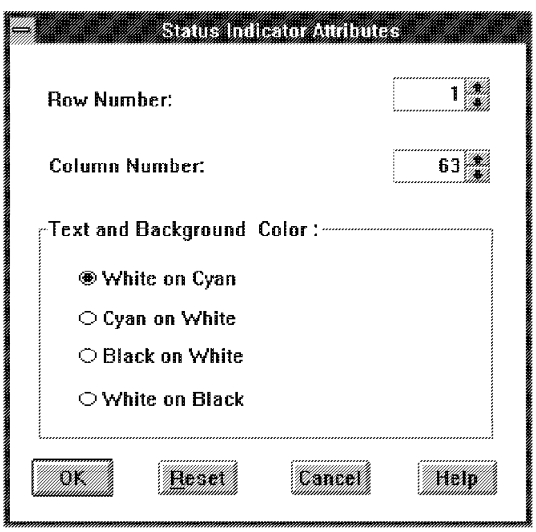
On the Screen Size Information window (Figure 71), you can choose the screen buffer size (in number of bytes). This is the size of the target workstation screen that will be displayed on the controller screen.

Your choice of bytes for Screen Buffer Size will affect the way applications work. If you choose a lower value, you will limit the size of the screen that will be seen on the controller workstation during a DCAF session. If you choose the maximum value of 8000 bytes for a screen size of 80 columns by 50 rows, the screen will use twice as much memory as the minimum value. This will reduce memory capacity for other applications and slow them down or even keep some of the applications from running on your workstation.

For the screen buffer size:

- The choices are 2000, 3440, 4000, 6880, and 8000 bytes. The default is 4000 bytes. This is the minimum number of bytes for characters plus attributes for a screen of 80 columns and 25 rows.
- When you choose the size, the window will automatically display the maximum number of rows for a screen of 40 columns and 80 columns.

2.8.3.4 Status Indicator Attributes



PICTURE 72

Figure 72. Status Indicator Attributes

The Status Indicator Attributes window (Figure 72) allows you to change the position and the color of the DCAF status indicator. The status indicator displays the current state of operation (for example, active or monitoring). The indicator itself is 18-columns wide and 1-row high. To change the position where the status indicator is displayed, you select both of the following:

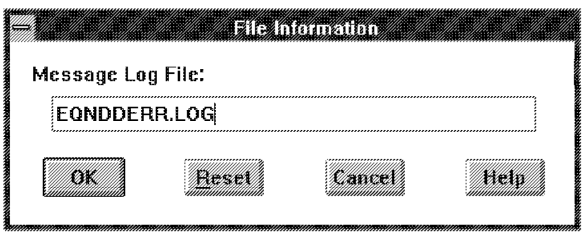
- Row number (0-50) with the default of 1
- Column number (1-63) with the default of 63.

It is recommended that you choose row number 1 for applications that scroll. If you have non-scrolling applications, you may choose a different row. If you choose row 0, then no status indicator is displayed.

You can also choose the color of the text and background for the status indicator and also for the DOS user interface panel. The foreground and background colors are:

- White on Cyan (the default)
- Cyan on White
- Black on White
- White on Black

2.8.3.5 File Information



PICTURE 73

Figure 73. File Information

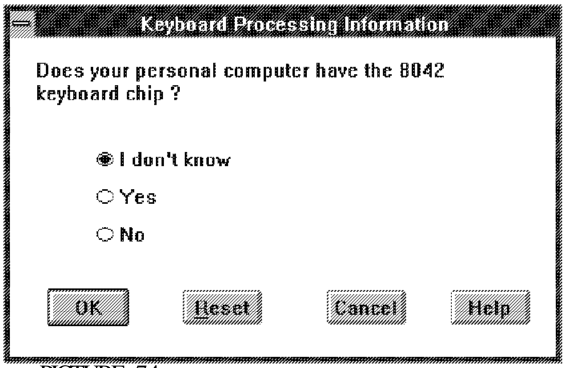
On the File Information window (Figure 73), you can personalize the name of the message log file that tracks informational and error messages for the DOS target workstation. For the message log file:

- The log file name is 1-8 characters, with a 0-3 character extension.

- The log file is created where the DCAF product is installed.

- The default message log file name for the DOS target workstation is EQNDDERR.LOG.

2.8.3.6 Keyboard Processing Information



PICTURE 74

Figure 74. Keyboard Processing Information

The Keyboard Processing window (Figure 74) allows you to choose how the keyboard input will be processed on the DOS target workstation. You are asked whether your personal computer has the 8042 keyboard chip. There are three choices:

1. **I don't know**. Choose this option if you do not know whether your workstation is equipped with an 8042 keyboard chip. The DCAF will run a test to see whether the 8042 chip is present and will attempt to use the chip (if it is present).

   I don't know is the default option.

2. **Yes**. Choose this option if you know that your workstation uses an 8042 keyboard chip. The DCAF supports DOS applications use the hardware directly for keyboard processing if the 8042 chip is present. See "DOS Target Keyboard Processing" in topic APPENDIX1.4.4, for the exceptions.

3. **No**. Choose this option is you know that your workstation does not have an 8042 keyboard chip. Smaller model PS/2 workstations do not have the 8042 chip. The DCAF supports applications that use software keyboard processing (interrupt 16H).

In most cases, the choice I dont know is appropriate. If the 8042 keyboard processing chip is present, then the DCAF uses the keyboard-chip stuffing technique to handle the keystrokes. If the 8042 chip is not present, then the interrupt 16H is used to handle the keystrokes.

The type of keyboard processing that is being used by the DOS target is logged in the DOS target message log file. The default name for this file is EQNDDERR.LOG.

2.9 Setting up DCAF Workstations to Start Automatically

You can set up targets, gateways, or LAN directory to start automatically so that they are ready for a session immediately. The way you accomplish this task depends on the DCAF workstation and communication protocol you want to start automatically.

2.9.1 Autostarting Targets

You can set the target to start automatically.

2.9.1.1 OS/2 Targets

You can autostart OS/2 targets for the following protocols:

2.9.1.1.1 APPC/APPN Connections

For OS/2 ES 1.0, perform the following steps:

1. From the SNA Network Definitions Selection window, open the Local Node Characteristics configuration window. Choose the Activate Attach Manager at Startup check box.

2. Open the SNA Network Definitions Selection window.

3. Open the Additional SNA Features and then the Transaction Program Definition window. Press the Continue... push button.

4. Select the Non-queued, Attach manager started check box.

For Communications Manager/2, perform the following steps: (See "Starting the Communications Manager Setup" in topic 3.1.2 for information about defining Communications Manager/2 parameters.)

1. When you define the Local node name, open the Local Node Characteristics window. Make sure that the Activate Attach Manager at Startup check box is selected.

2. When you define the Transaction program, open the Additional TP Parameters window. In the Operation type box, make sure that the Non-queued, Attach Manager started radio button is selected.

2.9.1.1.2 All Other Connections

To autostart OS/2 targets for asynchronous, IPX/SPX, NetBIOS, and TCP/IP connections, do the following:

- Set up DCAF to start automatically.

  You can accomplish this in one of two ways:

  - Create a shadow of the DCAF Target icon and put it in the Startup - Icon View folder of the OS/2 System folder.

    To minimize the target window when the target starts, open the Settings for the target and, in the Parameters field, add **/m** to the text in the field.

  - Type the following command, where /m is the optional parameter to minimize the target window when the target starts, in the

STARTUP.CMD file:

start "dcaf target" <dcafpath>eqntgaut.exe nocomm /m

- Set up the communication protocol to start automatically.

  Check the target personalized options and make sure that the Autostart communication check box is selected for the protocol you use. For more information, see "Personalizing the OS/2 Target" in topic 2.8.1.

2.9.1.2 Windows Targets

To autostart Windows targets, add program items for the protocols you use to the Startup group in Program Manager. Complete the following steps:

1. On the Program Manager window, choose **Startup** from the Window drop-down menu. The Startup window appears.

2. Choose **New...** from the File drop-down menu on the Program Manager window. The New Program Object dialog box appears.

3. In the New box, select the Program Item option button and press the **OK** push button. The Program Item Properties dialog box appears.

4. In the Description box, type a description, for example, Start NetBIOS target

5. In the Command Line box, type the path and program to be autostarted, for example, c:\DCAF13\eqnwldnb where c:\DCAF13\ are the drive and directory in which DCAF is installed and eqnwldnb is the program to be autostarted. Choose the program name for the protocol you use from the following list.

   Program Name Protocol

   EQNWLDAC.EXE Asynchronous

   EQNWLDIP.EXE IPX/SPX

   EQNWLDNB.EXE NetBIOS

   EQNWLDTC.EXE TCP/IP

6. In the Working Directory box, type the path in which DCAF is installed, for example, c:\DCAF13 Press the **OK** push button. The DCAF program that you specified starts automatically the next time you open Windows.

2.9.1.3 DOS Targets

To autostart DOS targets for NetBIOS connections, do the following:

1. Add the DCAF installation path to the DOS path statement in the AUTOEXEC.BAT file (as shown in the following example): PATH=C:\DCAF13;

2. Add the following call statement to the AUTOEXEC.BAT file:

   call DCAFDOS

   The DOS workstation loads the DOS target when it starts up.

2.9.2 Autostarting Gateways

The gateway can use either APPC or ACDI communications to communicate with the controller. This section discusses autostarting for both of these.

2.9.2.1 APPC/APPN Connections

The DCAF gateway workstation that uses APPC cannot be autostarted by the user. It will be autostarted by the Attach Manager when a DCAF controller attempts to connect to the DCAF gateway workstation. To enable the Attach Manager to autostart the DCAF gateway workstation, you must configure the OS/2 Communications Manager.

2.9.2.1.1 For OS/2 ES 1.0

Perform the following steps:

1. From the SNA Network Definitions Selection window, open the Local Node Characteristics configuration window. Choose the Activate Attach Manager at Startup check box.

2. Open the SNA Network Definitions Selection window, and then open the Additional SNA Features configuration window.

3. In the Transaction Program Defaults window, for the transaction program for the DCAF gateway choose Non-queued, Attach manager started.

2.9.2.1.2 For Communications Manager/2

Perform the following steps:

1. When you define the Local node name, open the Local Node Characteristics window. Make sure that the Activate Attach Manager at Startup check box is selected.

2. When you define the Transaction program, open the Additional TP Parameters window. In the Operation type box, make sure that the Non-queued, Attach Manager started radio button is selected.

See "Starting the Communications Manager Setup" in topic 3.1.2 for information about defining Communications Manager/2 parameters.

2.9.2.2 Asynchronous Connections

Use one of the following methods to autostart a DCAF gateway workstation that uses asynchronous communication (a direct communication via ACDI). A unique copy of EQNGWASY must be started for each communication port to be placed in auto-answer mode.

If you do not use the communications port and baud rate, the EQNGWASY program will use the default values of communications port COM1, and baud rate of 9600.

- Using the OS/2 System folder

  Perform the following steps:

  1. Open the Distributed Console Access Facility - Icon View folder.

  2. Create a shadow of the Gateway ACDI Auto-Answer for the DCAF and put it in the Startup - Icon View folder of the OS/2 System folder.

Note: Be sure that the correct parameters are set up in the program settings.

- Using the STARTUP.CMD file

  Perform the following steps:

  1. In the STARTUP.CMD file, type one of the following statements:

     Call GATEACDI

     or

     Start DCAF GATEWAY Auto-Answer GATEACDI.CMD

  2. Create the following REXX program and name it GATEACDI.CMD:

```
/* Auto-answer mode for DCAF gateway       */
do forever
  SAY'DCAF gateway is waiting for a call. Port=<communications port>
       Baud rate=<speed>'
  EQNGWASY <communications port <speed>>
end
```

     For example, EQNGWASY <communications port <speed>> is EQNGWASY <1 <9600 >>.

     This statement starts the DCAF product automatically on the DCAF gateway workstation for asynchronous communication and for direct communication via ACDI. The statement "do forever" returns the communication port to auto-answer mode when the connection ends.

2.9.3 Autostarting the LAN Directory

To autostart the LAN directory for IPX/SPX, NetBIOS, and TCP/IP connections, do the following:

- Set up DCAF to start automatically.

  You can accomplish this in one of two ways:

  - Create a shadow of the DCAF LAN directory icon and put it in the Startup - Icon View folder of the OS/2 System folder.

    To minimize the LAN directory window when the LAN directory starts, open the Settings for the LAN directory and, in the Parameters field, type **/m**.

  - Type the following command, where /m is the optional parameter to minimize the LAN directory window when it starts, in the STARTUP.CMD file:

    start "dcaf LAN directory" <dcafpath>eqnldaut.exe /m

- Set up the communication protocol to start automatically.

  Check the personalization options of the LAN directory and make sure that the Autostart communication check box is selected for the protocol you use. For more information, see "Personalizing the LAN Directory" in topic 2.7.2.

DSMBEG323I STARTING PASS 2 OF 2.
DSMPGL708E TEXT EXCEEDS RIGHT PAGE BOUNDARY ON PAGE 19.