SH19-4069-01

Distributed Console Access Facility

User′s Guide

Version 1.31

IBM

Distributed Console Access Facility

SH19-4069-01

User's Guide

Version 1.31

Note

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

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.

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. If the form has been removed, 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.

© **Copyright International Business Machines Corporation 1990, 1995. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 1990, 1995

Figures

© Copyright IBM Corp. 1990, 1995

Tables

© Copyright IBM Corp. 1990, 1995

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.

© Copyright IBM Corp. 1990, 1995

Programming Interface Information

This book is intended to help you to use the Distributed Console Access Facility.

This book also documents General-Use Programming Interface and Associated Guidance Information.

General-Use programming interfaces allow the customer to write programs that obtain the services of the Distributed Console Access Facility.

General-Use Programming Interface and Associated Guidance Information is identified where it occurs by an introductory statement to a chapter or section.

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

About This Book

This book explains how to use the IBM Distributed Console Access Facility (DCAF). DCAF is an IBM product that 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 Should Use This Book

This book is intended for users, such as help desk operators, who will take remote control of target workstations.

As a DCAF user, 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 to Use This Book

This book contains the following parts:

- Part 1, "Introducing the DCAF" on page 1, gives a general concept of DCAF and its uses.
- Part 2, "Using the DCAF" on page 11, explains how to use DCAF.
- Appendix A, "Diagnosis" on page 57, provides an aid to diagnose problems you may encounter while using DCAF.
- Appendix B, "Application Programming Interfaces (APIs)" on page 61, describes the Application Programming Interfaces for the DCAF product.
- "Glossary of Terms and Abbreviations" on page 77 explains the product-specific terms you will encounter while reading this book.
- The "Index" on page 85 helps you find the information you need.

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

© Copyright IBM Corp. 1990, 1995

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

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**

Part 1. Introducing the DCAF

© Copyright IBM Corp. 1990, 1995

Chapter 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 on page 4).

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**).

© Copyright IBM Corp. 1990, 1995

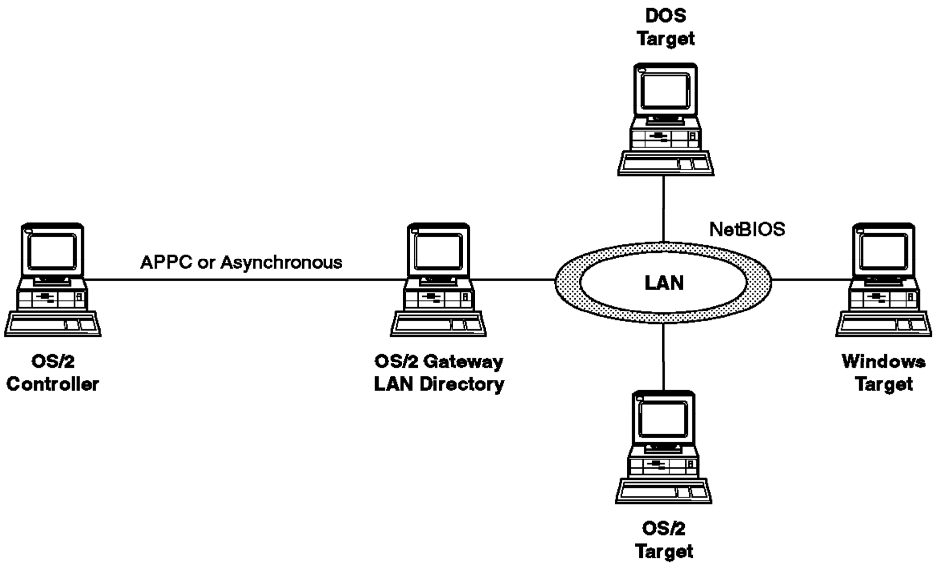

Figure 2. Example of Connection through a DCAF Gateway

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

The DCAF Network

The DCAF network includes the workstations that have DCAF installed and the communications that link them together. Figure 3 on page 8 is one example of a basic DCAF environment.

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.

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.

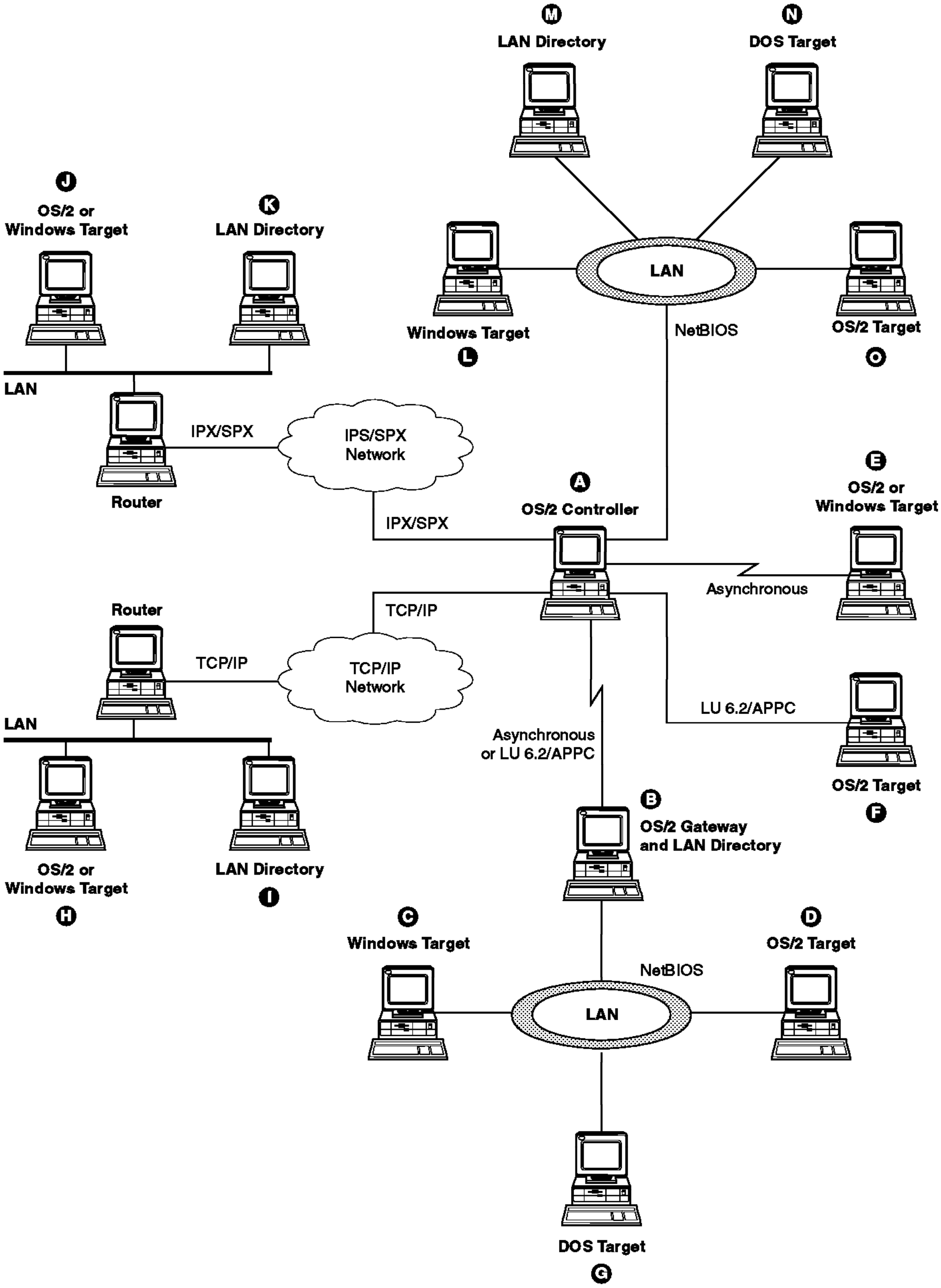

Figure 3. Example of a Distributed Console Access Facility Environment

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.

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.

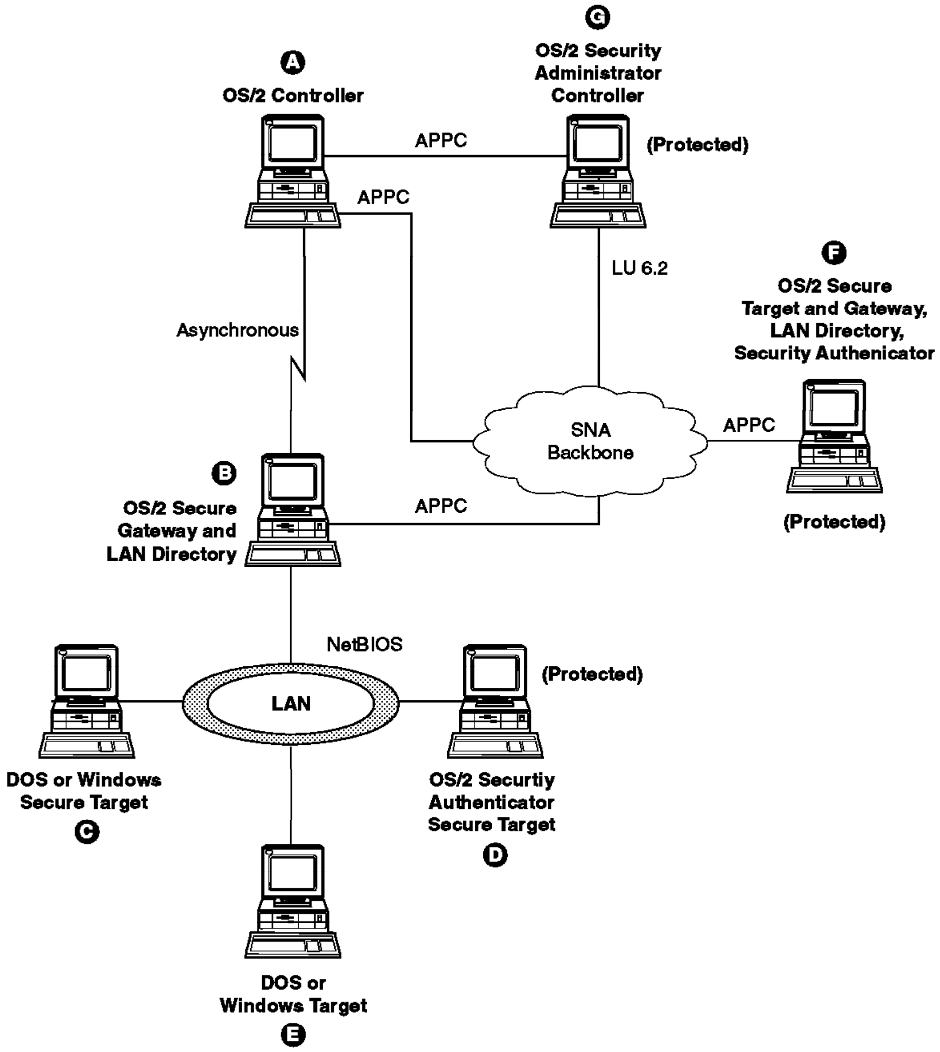

Figure 4. Example of DCAF Environment with Session Security

Part 2. Using the DCAF

© Copyright IBM Corp. 1990, 1995

Chapter 2. Optimizing the DCAF

This chapter provides some tips to help you get the best out of DCAF. In addition, you can find helpful suggestions on the DCAF forum through your IBM marketing representative or system engineer and on the DCAF customers′ forum.

Use these tips to improve DCAF performance.

- Avoid using wallpaper and background patterns in the graphic environment on the target during a session. It could interrupt the session.
- Avoid unnecessary mouse movements on the controller during connections on slow lines (such as asynchronous). These movements use up resources and slow down the connection.
- Before you start an MS-DOS** prompt on the Windows target from the controller, be sure that:
  - If you work in drive A (or physical drive B), the diskette is not write-protected and has been inserted in the drive on the target.
  - If you use the printer, there is paper in the printer.

  Otherwise, the target will switch to a DOS prompt, and keystrokes from the controller will not work on the target. You must restart the target on site.
- On the target, avoid using any PM applications, other than the one with which you are working, that require DCAF to refresh the screen continually.
- Because of the way the OS/2 window works, use the OS/2 full-screen on the target to avoid slow screen relays.

© Copyright IBM Corp. 1990, 1995

Chapter 3. Using the Controller

From the controller, you control the keyboard and mouse input and monitor the display output of a target workstation. You can start a session with one or more target workstations. You see the target workstation display of each target with which the controller workstation is connected, in a different DCAF session window.

The controller communicates directly with any target workstation or through a DCAF gateway with secure targets. To connect to a secure target, see "Secure Sessions" on page 30.

Starting the DCAF Controller

To start the DCAF controller, first choose the DCAF folder from the desktop, and then choose the DCAF Controller icon. First, the IBM logo, then the Distributed Console Access Facility - Controller window appears.

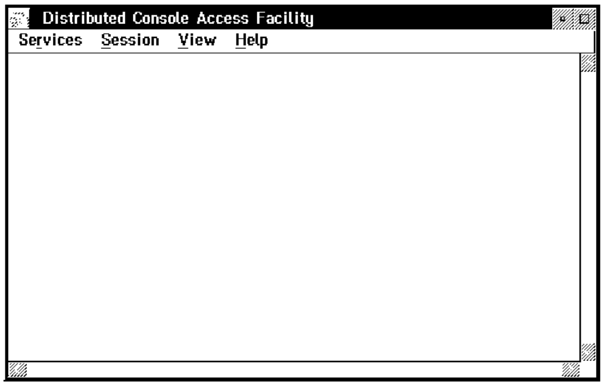

Figure 5. DCAF Controller Window

The controller is running.

Managing the Workstations in Your Directory

The DCAF Directory window lists all the workstations (target or gateway) directly available to you. This section describes how to manage these workstations.

Note: The EQNLR.INI file, which keeps a record of the workstations in the DCAF directory, can be corrupted. It is recommended that you always make a backup copy of the EQNLR.INI file after you have established a stable list of workstations in the DCAF directory.

Adding a Workstation

For every workstation with which you want to start a session, add a workstation description to your directory.

- Add the target for a direct session with a target.
- Add the LAN directory, not the target, for a session on a LAN through a LAN directory. The target is added to the LAN directory, not to the DCAF directory.

© Copyright IBM Corp. 1990, 1995

- Add the gateway for a basic session through a gateway.
- Add the gateway and define the administrator for a secure session. You define the administrator in “Defining or Changing the Security Administrator Description” on page 26.

Each workstation has a two-part description:

- General. The general description contains information about the name and kind of workstation, its communication protocol, and its level of security.
- Protocol. The protocol description contains configuration information specific to the workstation communication protocol.

Note: During the session, only the Find choice is available on the Workstation pull-down menu of the DCAF - Directory window.

General Description

To add a workstation to your directory, perform the following steps:

1. Ensure that the controller is running (see “Starting the DCAF Controller” on page 15).
2. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window (Figure 6) appears.

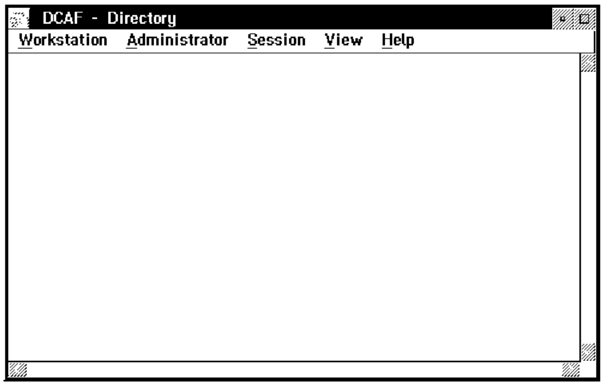

Figure 6. DCAF Directory Window

3. From Workstation on the menu bar, choose Add.... The Add a workstation notebook (Figure 7 on page 17) appears.

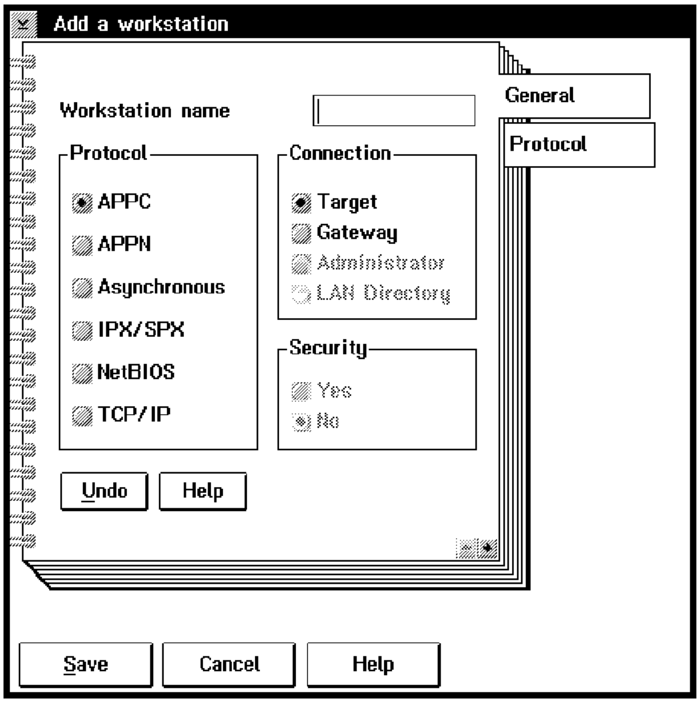

Figure 7. Add Workstation General Notebook

4. In the Workstation name field, type the workstation name. This is a name that you or the network administrator create in order to recognize the workstation, for example, IPX_TARGET_PHOENIX.

   Character guidelines for the workstation name:

   - 1–62 characters in length.
   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0–9)
   - Embedded blanks are not valid.

5. From the Protocol list box, select the communications protocol that you use to connect to the workstation.

   - APPC
   - APPN*
   - Asynchronous
   - IPX/SPX
   - NetBIOS
   - TCP/IP

6. From the Connection list box, select the kind of workstation that you connect to.

   - Target
   - Gateway
   - LAN Directory

7. From the Security list box, select whether the workstation needs DCAF security. Select Yes if the workstation uses DCAF security; select No if the workstation uses basic DCAF (no password or password only). The Security list box is unavailable if you select the IPX/SPX or TCP/IP protocol.

You are ready to provide the protocol description.

Protocol Description

Provide a protocol description for each workstation in the DCAF directory. Select the Protocol tab. If, on the General notebook page, you select:

- APPC, the APPC page appears (see Figure 8)
- APPN, the APPN page appears (see Figure 9 on page 19)
- Asynchronous, the Asynchronous page appears (see Figure 10 on page 20)
- IPX/SPX, the IPX/SPX page appears (see Figure 11 on page 21)
- NetBIOS, the NetBIOS page appears (see Figure 12 on page 22)
- TCP/IP, the TCP/IP page appears (see Figure 13 on page 23)

APPC Protocol Description: Define the following APPC parameters for the workstation.

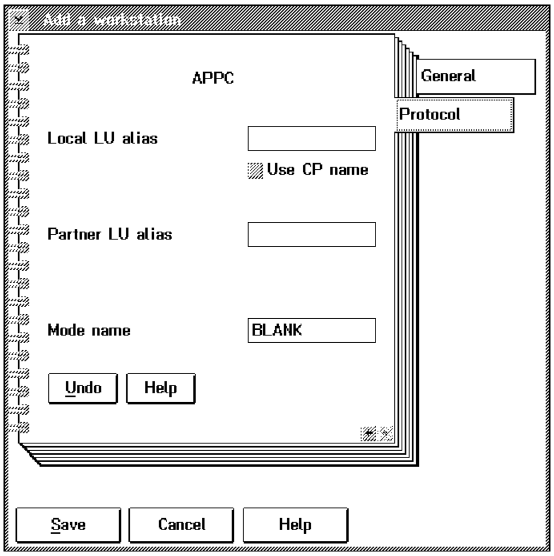

Figure 8. APPC Protocol Page

1. If you are using the CP name (local node name) of the workstation, select the Use CP Name check box. When the check box is selected, the Local LU Alias field is unavailable. Skip to Step 3. Otherwise, leave it unselected.
2. In the Local LU Alias field, type your controller *LU name*.

   Character guidelines:

   - It is 1–8 characters in length.
   - It can be any combination of characters, except left parenthesis, right parenthesis, comma, semicolon, blank.
   - It cannot start with @.
3. In the Partner LU Alias field, type the *LU name* of the workstation to which you are connecting.

   Character guidelines:

   - It is 1–8 characters in length.
   - It can be any combination of characters, except left parenthesis, right parenthesis, comma, semicolon, blank.
   - It cannot start with @.

4. In the Mode Name field, type the *mode name* for DCAF in your network. Valid characters are the same as for the local LU alias.

If you add more than one workstation to the directory, press the Save push button after each workstation description.

When you have completed the workstation descriptions, close the notebook. The added workstations appear in your workstation directory list when you close the notebook. Be sure that the communications are configured before you start a session with a new workstation. See *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

APPN Protocol Description: Define the following APPN parameters for the workstation.

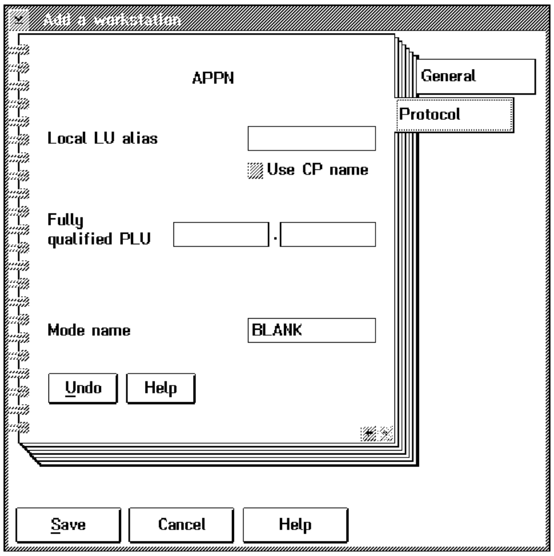

Figure 9. APPN Protocol Page

1. If you are using the CP name (local node name) of the workstation, select the Use CP Name check box. When the check box is selected, the Local LU Alias field is unavailable. Skip to Step 3. Otherwise, leave it unselected.
2. In the Local LU Alias field, type your controller *LU name*.

   Character guidelines:

   - It is 1–8 characters in length.
   - It can be any combination of characters, except left parenthesis, right parenthesis, comma, semicolon, blank.
   - It cannot start with @.
3. In the Fully Qualified PLU field, type the destination *network ID* in the first box and the destination *workstation LU name* in the second box.

   Character guidelines are the same as for the local LU alias.
4. In the Mode Name field, type the *mode name* for DCAF in your network.

If you add more than one workstation to the directory, press the Save push button after each workstation description.

When you have completed the workstation descriptions, close the notebook. The added workstations appear in your workstation directory list when you close the notebook. Be sure that the communications are configured before you start a session with a new workstation. See *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

Asynchronous Protocol Description: Define the following asynchronous parameters for the workstation.

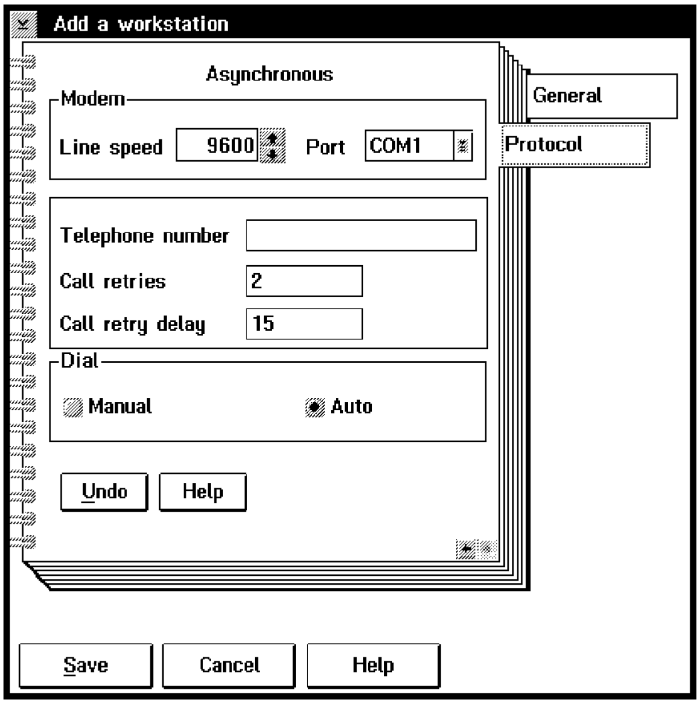

Figure 10. Asynchronous Protocol Page

1. From the Modem list box, in the Line Speed field, select the modem transmission 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
   - 64000

   The default is 9600.

2. In the Port field, select the asynchronous communication port number that the destination workstation uses.

   The range is 1–3. The default is 1.

3. In the Telephone Number field, type the modem telephone number of the workstation.

The maximum number of characters is 250.

4. In the Call Retries field, type the number of times you want DCAF to redial the telephone number if it cannot make the connection immediately. The range is 0–20. The default is 2.
5. In the Call Retry Delay field, type the pause in between retries in seconds. The range is 1–1200. The default is 15.
6. In the Dial box, select the kind of dialing, automatic or manual, for the workstation modem.

If you add more than one workstation to the directory, press the Save push button after each workstation description.

When you have completed the workstation descriptions, close the notebook. The added workstations appear in your workstation directory list when you close the notebook. Be sure that the communications are configured before you start a session with a new workstation. See *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

IPX/SPX Protocol Description: Define the following IPX/SPX parameters for the workstation:

- Network address
- Node address

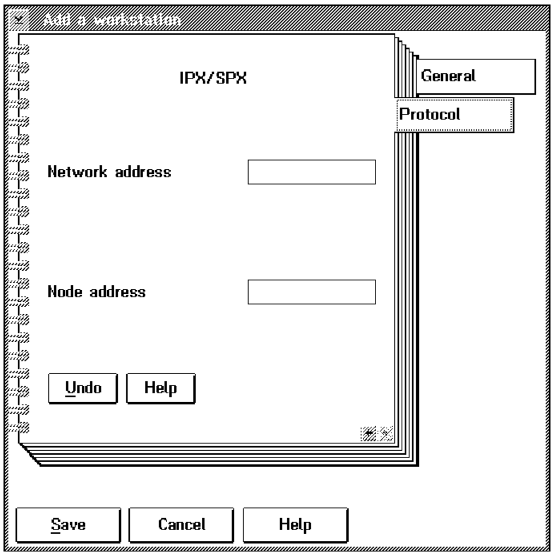

Figure 11. IPX Protocol Page

1. In the Network Address field, type the *network address* of the workstation. For instructions on determining the network address, see "Determining the Network and Node Address" on page 50.

   Character guidelines for hexadecimal format:

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

2. In the Node Address field, type the *node address* of the workstation. For instructions on determining the node address, see "Determining the Network and Node Address" on page 50.

   Character guidelines for hexadecimal format:

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

If you add more than one workstation to the directory, press the Save push button after each workstation description.

When you have completed the workstation descriptions, close the notebook. The added workstations appear in your workstation directory list when you close the notebook. Be sure that the communications are configured before you start a session with a new workstation. See *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

NetBIOS Protocol Description: Define the following NetBIOS parameters for the workstation:

- Network address
- Adapter number

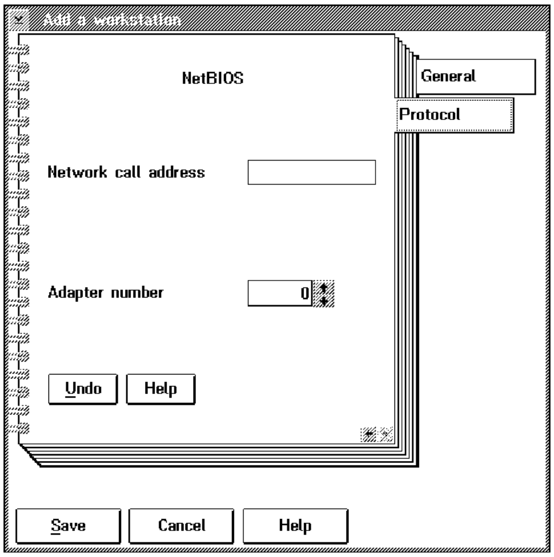

Figure 12. NetBIOS Protocol Page

1. In the Network Call Address field, type the *network call address* of the workstation if you are defining a target. For instructions, see "Determining the LAN Identifier Number (Adapter Address)" on page 53. Type the *LAN directory name* if you are defining a LAN directory. The default LAN directory name is DCAFLAN. It is case sensitive.

   Character guidelines for hexadecimal format:

   - Exactly 12 characters in length.
   - Upper- or lowercase letters (A-F, a-f)
   - Digits (0–9)
   - Special characters

2. In the Adapter Number field, select the *adapter number* of the workstation.

   The range is 0 – 3. The default is 0.

If you add more than one workstation to the directory, press the Save push button after each workstation description.

When you have completed the workstation descriptions, close the notebook. The added workstations appear in your workstation directory list when you close the notebook. Be sure that the communications are configured before you start a session with a new workstation. See *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

TCP/IP Protocol Description: Define the following TCP/IP parameters for the workstation:

- Remote host name
- Port number

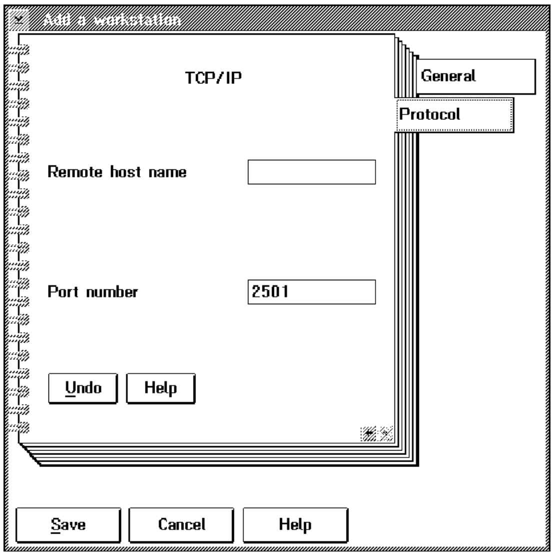

Figure 13. TCP/IP Protocol Page

1. In the Remote Host Name field, type *host name* or the *IP address* of the destination workstation. Use the host name only if you are sure that your workstation and IP address and the destination workstation and IP address are listed in HOSTS files on both workstations.

   Character guidelines:

   - It is 1–256 characters in length.
   - Upper- or lowercase letters (A-Z, a-z).
   - Digits (0–9).
   - All special characters except blanks.

2. In the Port Number field, type the *port number* of the destination workstation. For DCAF, the range is 1024–65534. The default is 2500 if you define a target. The default is 2501 if you define a LAN directory.

If you add more than one workstation to the directory, press the Save push button after each workstation description.

When you have completed the workstation descriptions, close the notebook. The added workstations appear in your workstation directory list when you close the notebook. Be sure that the communications are configured before you start a session with a new workstation. See *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

Opening a Workstation Description to View or Change It

To open a workstation to view or change all or part of the description of an existing workstation in your directory, perform the following steps:

1. From Session on the menu bar choose Open a Workstation Directory....

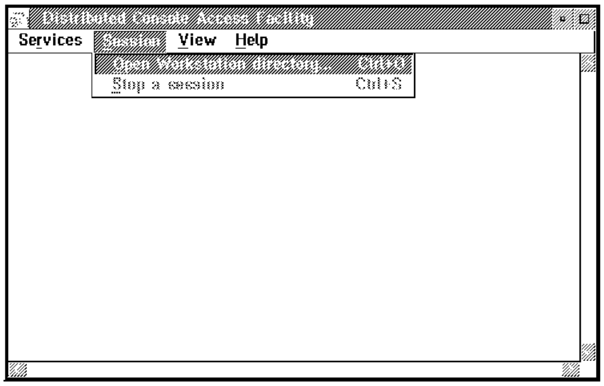

Figure 14. DCAF Controller Window with Session Pull-Down Menu

   The DCAF - Directory window (Figure 6 on page 16) appears.

2. In the DCAF - Directory window, select the workstation to open. To locate the workstation in the workstation directory list quickly, see "Locating a Workstation in the DCAF Directory" on page 25.
3. From Workstation on the menu bar, choose Open.... The Open Workstation notebook appears.
4. See "Adding a Workstation" on page 15, for a description of the parameters and fields.

   When you have completed viewing or modifying workstation descriptions, close the notebook. Any modified workstations appear in your workstation directory list when you close the notebook.

Ensure that the communications configuration reflects any changes you have made before you start a session. See the *Distributed Console Access Facility Installation and Configuration Guide*.

Copying an Existing Workstation

Copy a workstation when you want to create a workstation similar to an existing one. You can modify all the parameters when you copy a workstation.

To copy an existing workstation, perform the following steps:

1. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window (Figure 6 on page 16) appears.

2. In the DCAF - Directory window, select the workstation to copy. To locate the workstation in a list quickly, see "Locating a Workstation in the DCAF Directory" on page 25.
3. From Workstation on the menu bar, choose Copy.... The Copy Workstation notebook (Figure 7 on page 17) appears.
4. See "Adding a Workstation" on page 15, for a description of the parameters and fields.
5. To copy more than one workstation in the directory, press the Save push button after each workstation description.

   When you have completed copying the workstation descriptions, close the notebook. Any changes appear in your workstation directory list when you close the notebook.

Be sure to configure the communications before you start a session with the new workstation. See the *Distributed Console Access Facility Installation and Configuration Guide* to see how to configure the communications.

Deleting a Workstation

To delete a workstation from your directory, perform the following steps:

1. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window (Figure 6 on page 16) appears.
2. In the DCAF - Directory window, select the workstation to delete. To locate the workstation in a list quickly, see "Locating a Workstation in the DCAF Directory."
3. From Workstation on the menu bar, choose Delete. The message Are you sure you want to delete the selected item? appears. Press the Yes push button if you are sure.

The workstation is removed immediately from the list of workstations in your directory.

Locating a Workstation in the DCAF Directory

When there are many workstations in the DCAF directory, instead of scrolling through a long list of workstations, search for the workstation name from the list of workstations on the DCAF - Directory window. Perform the following steps:

1. From Workstation on the menu bar of the DCAF - Directory window (Figure 6 on page 16), choose Find.... The DCAF - Directory Search window (Figure 15) appears.

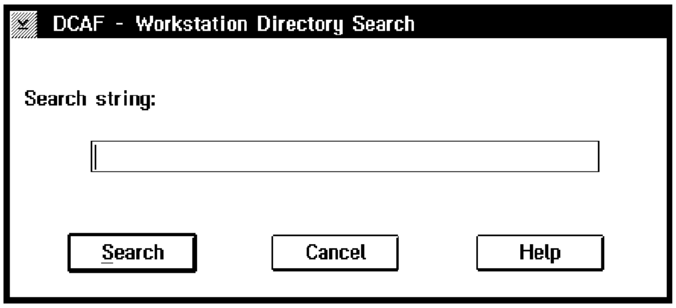

Figure 15. Directory Search Window

2. In the Search string, type a string or substring of characters from the workstation name. The maximum length is 62 characters. Press the Search push button. The first occurrence of the string appears, highlighted, at the top of the workstation list.
3. To search for each next occurrence, press Ctrl+F.

Defining or Changing the Security Administrator Description

Perform this task only if you connect to secure gateways or targets. This task enables your controller to send updates when you change your pass phrase to the security administrator. The security administrator updates your pass phrase in its database of security information and then distributes it across the secure network.

General Description

To define or change a security administrator description, perform the following steps:

1. Ensure that the controller is running (see "Starting the DCAF Controller" on page 15).
2. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window appears.

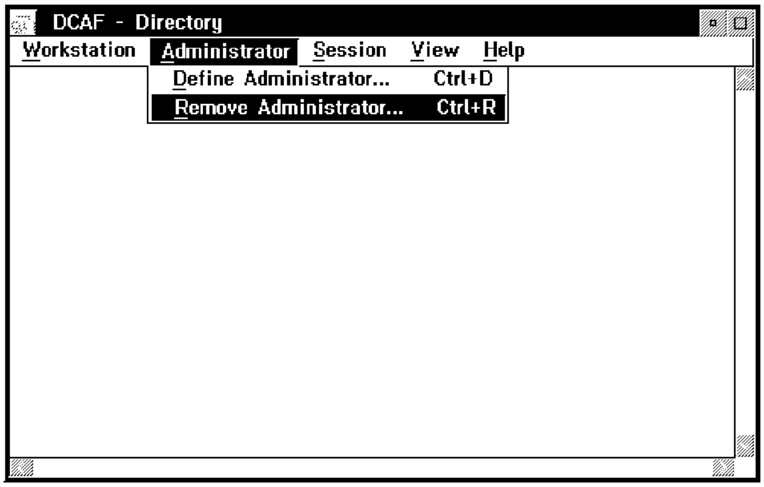

Figure 16. Defining or Changing the Administrator

3. From Administrator on the menu bar (Figure 16), choose Define Administrator....

   The Define Administrator notebook (Figure 17 on page 27) appears.

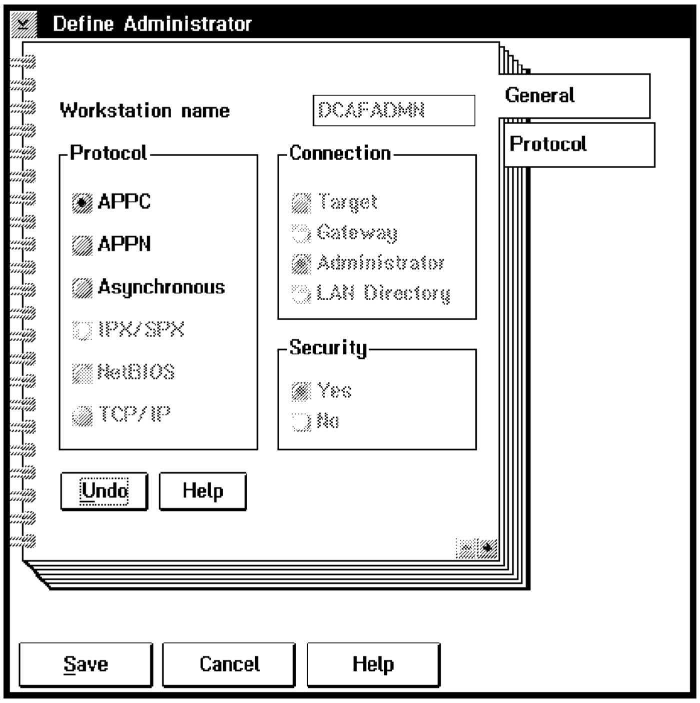

Figure 17. Define Administrator General Notebook

4. The Workstation name field is unavailable because there is one security administrator in the DCAF environment and its name must be DCAFADMN. From the Protocol list box, select the communications protocol that you use to connect to the workstation.
   - APPC
   - APPN
   - Asynchronous

You are ready to provide the protocol description.

Protocol Description

Provide a protocol description for the communication type that you use to connect to the security administrator. From the Define Administrator notebook, select the Protocol tab. If, on the General notebook page, you selected:

- APPC, the APPC page (Figure 8 on page 18) appears. Follow the instructions in "APPC Protocol Description" on page 18.
- APPN, the APPN page (Figure 9 on page 19) appears. Follow the instructions in "APPN Protocol Description" on page 19.
- Asynchronous, the Asynchronous page (Figure 10 on page 20) appears. Follow the instructions in "Asynchronous Protocol Description" on page 20.

Removing a Security Administrator

To remove a security administrator, perform the following steps:

1. Ensure that the controller is running (see "Starting the DCAF Controller" on page 15).
2. From Session on the menu bar of the Distributed Console Access Facility - Controller window, choose Open a Workstation Directory.... The DCAF - Directory window appears.

3. From Administrator on the menu bar (Figure 16 on page 26), choose Remove Administrator.... A message requesting confirmation to delete the security administrator appears.
4. Press the Yes push button. DCAF removes the security administrator.

Starting a Session

This section describes how to start a session in various ways. The first three provide progressively higher security. For a description of the varying levels of DCAF security, see "Levels of DCAF Security" on page 7.

- No password
- Password-only
- Secure
- Through a LAN directory

  The LAN directory enables you to access all the available LAN targets that reside on a specific LAN. The LAN directory keeps a running list of available targets. Access the LAN directory and then choose the target from its list of LAN targets.
- From the command line

  You can connect directly to the target with a command from the command line. This command works for IPX/SPX, NetBIOS, and TCP/IP connections only.

Before You Start

Before you start a session, ensure that you have already done the following:

- Installed the controller, target and, if necessary, LAN directory, gateway, or security components on the workstations. See the *Distributed Console Access Facility Installation and Configuration Guide* for installation instructions.
- Configured the communications for each workstation. See the *Distributed Console Access Facility Installation and Configuration Guide* for sample configurations.
- Added the workstation to which you are connecting to the DCAF directory. See "Adding a Workstation" on page 15 .
  - For a direct session with a target, add the target.
  - For a session on a LAN through a LAN directory, add the LAN directory, not the target The target is added to the LAN directory, not to the DCAF directory.
  - For a basic session through a gateway, add the gateway.
  - For a secure session, add the gateway and administrator.
- Started the controller and, if necessary, any other components. See "Starting the DCAF Controller" on page 15 to start the controller.
- Ensured that the target user has started the target. *Distributed Console Access Facility Target User's Guide* provides instructions to start the target.

No Password Sessions

To start a no password session, perform the following steps:

1. Ensure that the controller is running and that the workstation to which you are connecting is defined in the DCAF directory. If not, define it now (see "Adding a Workstation" on page 15).
2. From Session on the menu bar of the Distributed Console Access Facility - Controller window (Figure 14 on page 24), choose Open a Workstation Directory....

   The DCAF - Directory (Figure 18) window appears.

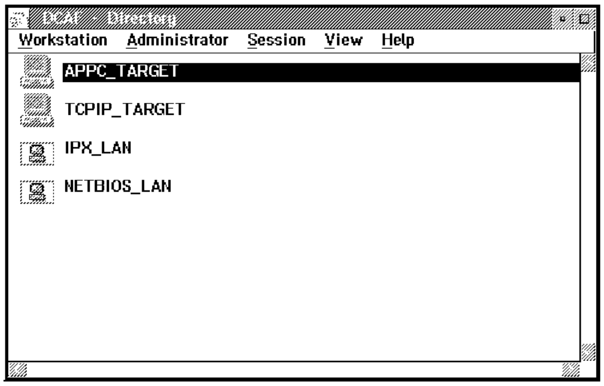

Figure 18. DCAF Directory Window

3. The workstations that are available for a session appear in the window. To locate the workstation in the DCAF directory quickly, see "Locating a Workstation in the DCAF Directory" on page 25. Select the one you want. From Session on the menu bar, choose Start a session.... The DCAF Target Password window (Figure 19) appears.
4. Press **OK**. The session starts. The workstation display appears on your screen. If you selected a target, you are ready to work on the workstation as if you were there.

   If you selected a gateway, the LAN Target Directory window appears. See "Sessions through the LAN Directory" on page 32, for instructions on starting a session from the LAN Target Directory window.

Password-Only Sessions

To start a password-only session, perform the following steps:

1. Follow Steps 1 to 3 under "No Password Sessions."

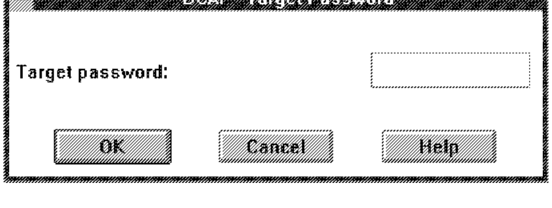

Figure 19. DCAF Target Password

2. On the DCAF Target Password, type the password for the workstation. It does not appear on the screen.

Character guidelines for the password:

- 4–8 characters in length
- Upper- or lowercase letters (A – Z, a – z)
- Digits (0–9)
- At least four alphanumeric characters
- Blanks after the last alphanumeric are ignored
- Not case sensitive

3. Press **OK**. The session starts. The workstation display appears on your screen. If you selected a target, you are ready to work on the workstation as if you were there.

Secure Sessions

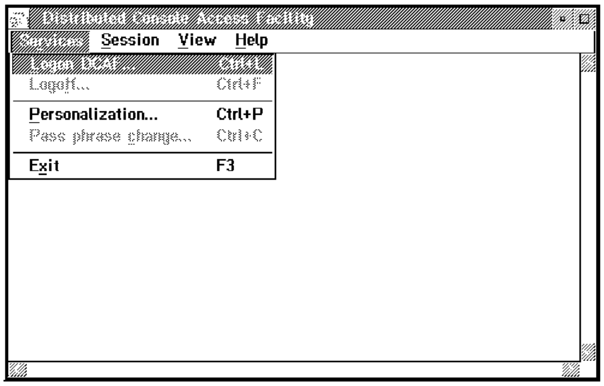

Figure 20. DCAF Controller with Services Pull-Down Menu

To start a secure session, perform the following steps:

1. Ensure that the controller is running and that the workstation to which you are connecting is defined in the DCAF directory. If not, define it now (see "Adding a Workstation" on page 15).

2. From Services on the menu bar of the Distributed Console Access Facility - Controller window (Figure 20), choose Logon DCAF....

   DCAF requires you to log on the first time you access the secure gateways and targets.

   The Logon DCAF window (Figure 21) appears.

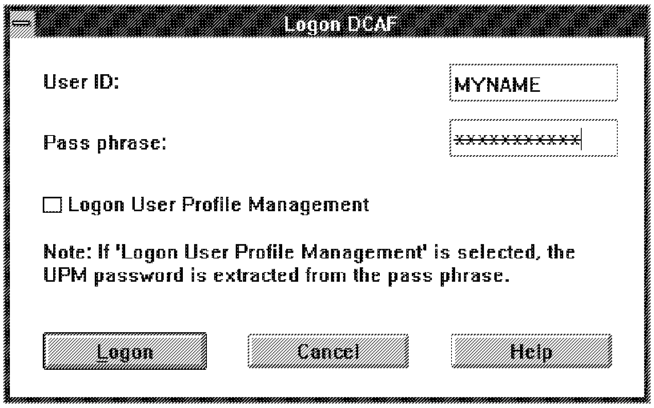

Figure 21. Logon DCAF

3. In the User ID field, type your DCAF user ID.
4. In the Pass phrase field, type your pass phrase.
5. Select the check box, to log on to the OS/2 User Profile Management at the same time.
6. Press the Logon push button. The Distributed Console Access Facility - Controller window reappears.
7. From Session on the menu bar, select Open Workstation Directory.... The DCAF - Directory (Figure 18 on page 29) window appears. The workstations that are available for a session appear in the window. To locate the workstation in a list quickly, see "Locating a Workstation in the DCAF Directory" on page 25. To access a LAN target directly, see "Sessions with a LAN Target via Fast Path."
8. Select the secure gateway that connects you to the secure target. From Session on the menu bar, choose Start a session....

   The DCAF LAN Target Directory window (Figure 23 on page 32) appears.
9. Select the secure target and choose Start a session... from Services on the menu bar. The session starts and the target display (Figure 32 on page 42) appears on your screen. You are ready to work on the target as if you were there.

Note: Ensure that you log off when you have completed working with the secure target. Otherwise, unauthorized users can access it if you leave your workstation unattended. See "Stopping the Session" on page 48.

Sessions with a LAN Target via Fast Path

If you know the exact name of the workstation (gateway or target) you can connect to it quickly by using a fast path. The fast path enables you to locate and connect to the target (or if you are connecting through a gateway, the gateway and then the target) without having to scroll through the list of workstations in the LAN directory. Perform the following steps:

1. From Session on the menu bar of the DCAF - Directory window (Figure 6 on page 16), choose Fastpath.... The DCAF - Workstation Directory Fast Path window (Figure 22) appears.

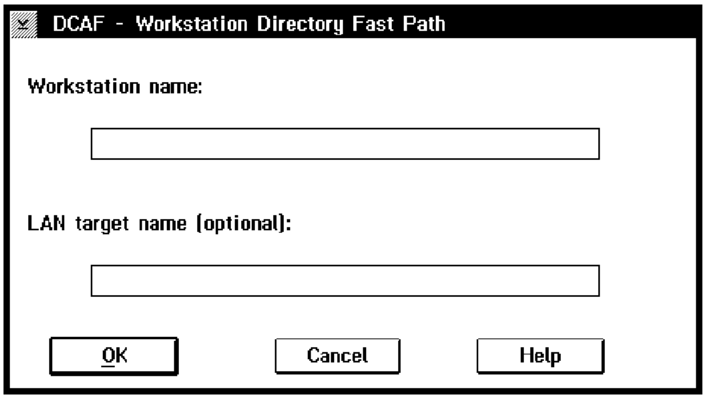

Figure 22. Workstation Directory Fast Path

2. In the DCAF - Workstation Directory Fast Path field, type the exact name of the gateway or target.

3. In the LAN target name field, type the exact name of the target only if you typed the name of a gateway in the previous field. This field is optional.
4. Press the **OK** push button. If you entered a target name, the session starts. If you entered a gateway name only, the DCAF LAN Target Directory window (Figure 23) appears. Continue the steps in "Sessions through the LAN Directory."

Sessions through the LAN Directory

The LAN directory enables you to access (via IPX/SPX, NetBIOS, or TCP/IP) all the available LAN targets that reside on a specific LAN. The LAN directory keeps a running list of available targets. For this kind of session, access the LAN directory and then choose the target from its list of LAN targets. In this way, it is not necessary to define every target in the DCAF directory. You can list them in the LAN directory.

To start a session through the LAN directory, perform the following steps:

1. Ensure that the controller is running and that the LAN directory is defined in the DCAF directory. If not, define it now (see "Adding a Workstation" on page 15).
2. From Session on the menu bar of the DCAF - Controller window, select Open Workstation Directory.... The DCAF - Directory (Figure 18 on page 29) window appears.
3. The LAN directory that is available appears in the window. To locate a specific LAN directory in a list quickly, see "Locating a Workstation in the DCAF Directory" on page 25.
4. Select the LAN directory and choose Start a session... from Session on the menu bar. The DCAF LAN Target Directory window (Figure 23) appears.

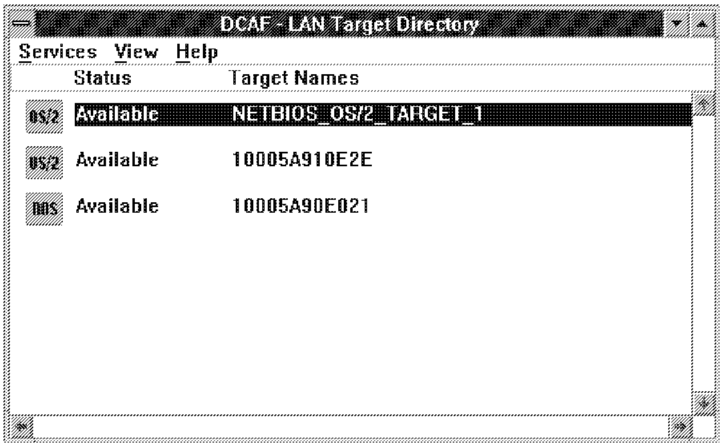

Figure 23. DCAF LAN Target Directory

5. Follow one of these procedures to connect to the LAN target:
   - If you know the exact name of the target, you can connect to it quickly by using a fast path. The fast path enables you to locate and connect to the target without having to scroll through the list of targets in the LAN target directory. To use the fast path, perform the following steps:

a. From Services on the menu bar of the DCAF - LAN Target Directory window (Figure 23), choose Fastpath.... The DCAF - LAN Target Fast Path window (Figure 24 on page 33) appears.

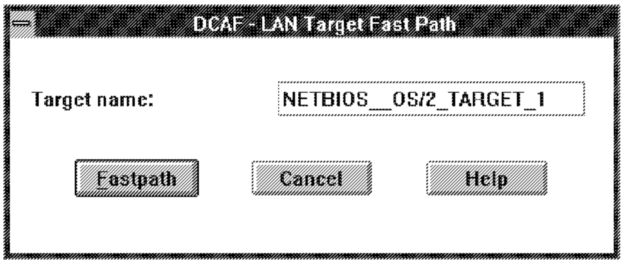

Figure 24. LAN Target Fast Path

b. In the Target name field, type the exact name of the target and press the Fastpath push button. The session starts.

- Scroll through the list of target names in the DCAF - LAN Target Directory window and select the target. Choose Start a session... from Services on the menu bar. The session starts and the target display (Figure 32 on page 42) appears on your screen.

Under the menu bar, Status shows the availability of the target. There are three statuses:

- Available: the target is running and ready for a session.
- Active: the target in a session with a controller
- Disabled: the target is not available for a session.

Updating the List of Available Targets in the LAN Directory

To see the current list of targets, choose Refresh from the Services pull-down menu. The status of the targets in the LAN Target Directory is updated.

To start a session with the LAN target:

1. Select the LAN target name.
2. From the Services pull-down menu, choose Start a session.... The secure session starts.

Changing the LAN Target Name

The targets appear under the Target Names column on the DCAF LAN Target Directory window. The target name is either a user-defined nickname or its LAN adapter address.

If you give a single LAN target a nickname, you can create a file that contains the nicknames of a list of targets. See “Creating a File of Target Nicknames” on page 50 for more information.

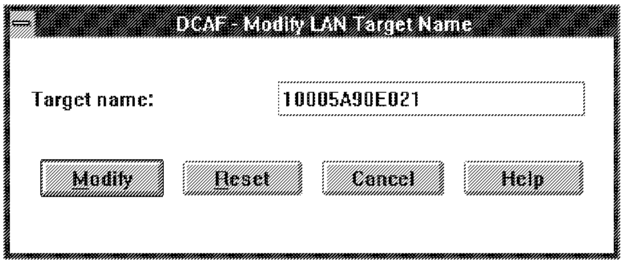

Figure 25. Modify LAN Target Name

To give a LAN target a nickname, perform the following steps:

1. Choose Modify a target name... from the Services pull-down menu. The Modify LAN Target Name window (Figure 25) appears.
2. Type the new name in the Target name field.

   Character guidelines for the target nickname:

   - 1–60 characters in length
   - Must not have blanks
   - Case sensitive
   - Must be unique
   - Cannot be a substring of another target nickname.
3. Press the **Modify** push button. The new name appears immediately in the LAN Target Directory.

Listing the NetBIOS Applications on the Target Workstation

DCAF can list the NetBIOS applications that are running on the LAN target workstation DCAF does this for targets connected via NetBIOS only.

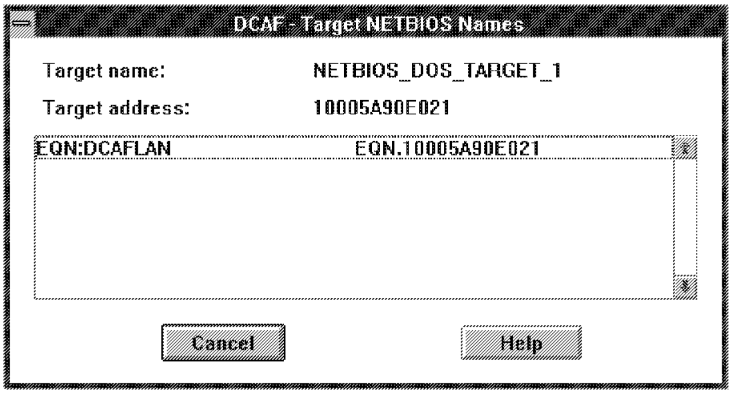

Figure 26. DCAF Target NetBIOS Names

To list the NetBIOS applications running on the target, choose List local names from the Services pull-down menu.

The DCAF Target NetBIOS Names window (Figure 26) appears. The target name and target LAN adapter address appear at the top of the window. The list box shows the active applications that are using NetBIOS on that workstation. Applications that begin with the letters 'EQN' belong to the DCAF.

Direct Sessions from the Command Line

You can connect directly to the target with a command from the command line without using the graphic interface. This command works for direct sessions with the target, not through the LAN directory or gateway, and it works for IPX/SPX, NetBIOS, and TCP/IP connections only.

To start a session from your command line, complete the following steps:

1. At an OS/2 command line, in the directory in which DCAF is installed, type **takeover** *protocol targetaddress*

   For example,

   IPX/SPX *NetworkAddress NodeAddress*

   NetBIOS *NetworkCallAddress AdapterNumber* (optional)

   TCP/IP *RemoteHostName PortNumber* (optional)

2. Press **Enter**. The session with the target starts.

Managing Sessions

This section describes how to manage sessions, including changing session states, switching your keystrokes between local and remote modes, transferring files, and moving among multiple sessions.

Changing the Session State

The session state is the current state of the session between the controller and the target workstation. The user of either workstation can change the session. While you are changing the session state, the target workstation user cannot alter that session. If both users change the session state simultaneously, precedence goes to the target workstation user. You will see a message and must wait until the target workstation user gives you control of the workstation or terminates the session.

A status indicator of the session state appears in the title bar of the session window or, when the session interface is minimized, under the controller icon.

The following table describes the various types of session states.

Table 1 (Page 1 of 2). Session States

Session States	Description
ACTIVE	A DCAF session has been established, and the controller user controls the keyboard input and monitors the display output of the target workstation. The target keyboard is locked; the keystrokes and mouse commands entered by the target user are not processed. If the hot key combination for the target is chosen at installation and enabled, then the target user can regain control by pressing the hot key combination to change the session state.

Table 1 (Page 2 of 2). Session States	
Session States	**Description**
BUSY	A DCAF session has been established, and the target workstation user has pressed the hot key combination and has regained control of the target workstation. The controller user must wait until the target workstation user chooses to put the DCAF session in another state.
FILE TRANSFER	A file transfer between a controller and a target workstation is in progress.
INITIATING	The controller is starting a DCAF session with a target workstation.
MONITORING	A DCAF session has been established, and the controller monitors (watches) the activity of the target workstation. The controller user sees everything on the target workstation display, but the target workstation user is in control of the keyboard and mouse input. If the hot key combination for the target workstation is chosen at installation and enabled, then the target workstation user can end the monitoring state by pressing the hot key combination to change the session state.
PENDING	A DCAF session is in the process of changing states. The OS/2 workstation user who requested the state change must wait until the pending state change is complete before issuing another request to change states.
SUSPENDED	The DCAF session in progress between the controller and the target workstation has been suspended. On the controller, the target workstation's last screen has been frozen. A suspended session does not require any session startup if you choose to change to another session state (for example, active or monitoring). A different controller cannot start a session with a target workstation in a suspended session state.
TERMINATING	The DCAF session is terminating (ending). This is for controller and OS/2 target workstations only.
For DOS Target Only	**Description**
CANNOT UNLOAD	The DOS target cannot unload from memory. A possible cause is a TSR (terminate stay resident) conflict. If a TSR application has been loaded after the DOS target, it should be unloaded before you attempt to unload the DOS target. This will also occur if you try to unload a TSR application from a virtual DOS machine.
ERROR	An error occurred in the DOS target. Refer to the DOS target message log file for more information.
LISTENING	The DOS target workstation is listening (waiting) for communications from a controller to establish a session. The DOS target workstation is in the listening session state when the DOS target has been enabled, when the session has been terminated, and if an error occurred in unloading the DOS target (it cannot be unloaded).
UNLOADED	The DOS target is unloaded from memory.
UNLOADING	The DOS target is being unloaded from memory.

Figure 27 shows an active DCAF session with an OS/2 target. The controller session window shows a view of the target workstation's display. The Desktop is open on the target workstation's display. The controller keystrokes are always in remote mode when the session starts.

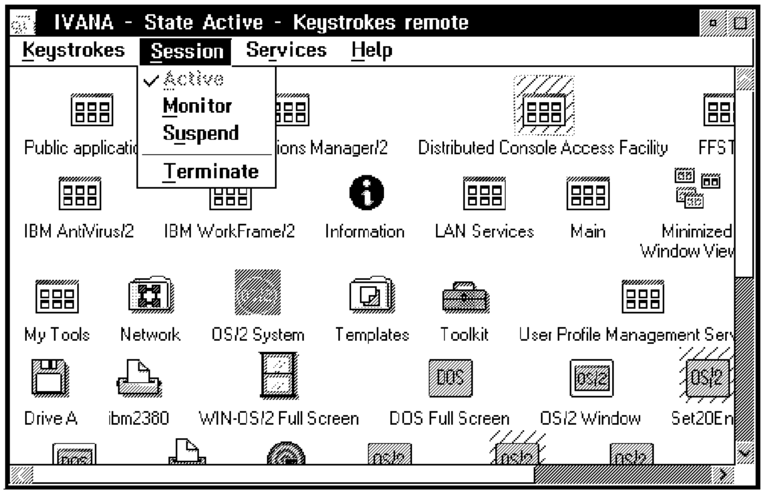

Figure 27. Controller Session Window with Session Pull-Down Menu

The workstation name, current session state, and the keystrokes mode is displayed on the title bar of the controller session window. Figure 27 shows the State as Active in the title bar.

To change the session state, do either of the following:

- Choose the Session pull-down menu, and then choose the action to change the session state.
- If you are in keystrokes local mode, press the shortcut key associated with the action to change the session.

Active	Ctrl+A
Monitor	Ctrl+M
Suspend	Ctrl+S
Terminate	Ctrl+T

Working on the Target

This section describes the actions you can take on the target from your workstation. They include using sending system shortcut keys, transferring files, shutting down the target, and starting an OS/2 command line.

Using Keystrokes during a Session

The keystrokes mode, displayed on the title bar of the session window, determines whether the controller user's keyboard input and mouse movements affect the controller or the target workstation. During an active session, you can change the keystrokes mode to local or remote.

In local mode,

- All your keyboard input and mouse movements affect the controller only. All keystrokes on the controller are processed by the controller.
- Only shortcut keys from the Keystrokes pull-down menu affect the target workstation. These shortcut keys simulate operating-system hot key combinations, such as Alt+Esc, Alt+Tab, Ctrl+Esc. On the DOS-only

workstation, the hot key combinations are not defined by the operating system so they work as they are defined by the application running on the target workstation during a session. Table 2 on page 38 shows how the shortcut keys work on OS/2 and Windows workstations.

Table 2. Shortcut Keys for the OS/2 or Windows Target

If you press...	Result
Ctrl+E	Simulates an Alt+Esc hot key pressed on the target workstation, causing the target workstation display to show the windows and full-screen sessions in an ordered rotation.
Ctrl+U	Simulates an Alt+Tab hot key pressed on the target workstation, causing the target workstation display to show the system menus for the windows and full screen sessions in an ordered rotation.
Ctrl+C	Simulates a Ctrl+Esc hot key pressed on the target workstation, causing the target workstation to display its task list.

In remote mode,

- All your keyboard input on the controller except the controller operating-system hot keys affects the target workstation. Operating-system hot key combinations always affect the controller only. These combinations Alt+Esc, Alt+Tab, Ctrl+Esc have the usual function.
- Mouse movements inside the target screen on the controller are sent to the target workstation. If you move your mouse outside the target screen, your mouse movements are processed on the controller. For example, if you choose an action from a pull-down menu over the target screen, the action will be processed on the OS/2 target workstation. If you choose an action from a pull-down menu over the controller window, the action will be processed on the controller.
- If a graphics application is running on the target workstation and you are moving the mouse pointer on the target with your keyboard arrow, you do not see the mouse pointer from the controller screen. You see the results of your actions on the target workstation, but you do not see the position of your keyboard arrow on the screen.
- You can send operating-system hot key combinations for the target workstation from the Keystrokes pull-down menu. See Figure 28 on page 39.

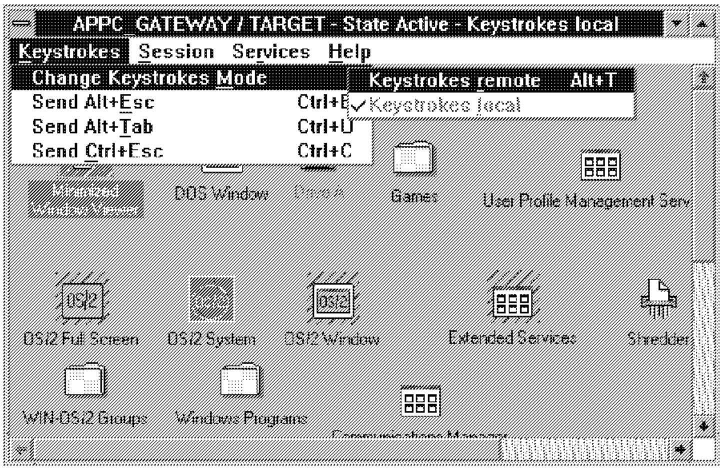

Figure 28. Controller Session Window with Keystrokes Pull-Down Menu

Figure 28 shows the controller window with a view of the target's display during an active session. The Desktop is open on the target workstation. The controller user is working in the keystrokes-local mode.

Examples:

- Changing the keystrokes mode

  Do one of the following:

  – Press the controller hot key (default Alt+T) to switch back and forth between local and remote mode.

  – Move your mouse onto the Keystrokes menu and choose Keystrokes remote or Keystrokes local from Change Keystrokes Mode. See Figure 28.

- Using hot key combinations

  To pull up the task list on the controller, press **Ctrl+Esc**. To pull up the task list on the target workstation, choose Send Ctrl+Esc from the Keystrokes pull-down menu.

- Scrolling windows

  In remote mode, when you use the scrolling keys, you scroll the active window on the target workstation.

  In local mode, when you use the scrolling keys, you scroll the active window on the controller.

Sending the Alt+Esc Command to the Target Workstation: Sending the Alt+Esc allows you to see the OS/2 target workstation's full screen or window sessions in ordered rotation. If you switch to a full screen session, then you are immediately in the full screen session of the target workstation.

To send the Alt+Esc to the target workstation, do either of the following:

- Choose Send Alt+Esc from the Keystrokes pull-down menu on the controller session window (see Figure 28).

- If you are in keystrokes local mode, press the **Ctrl+E** shortcut key.

Sending the Alt+Tab Command to the Target Workstation: Sending the Alt+Tab allows you to see the system menu for the OS/2 target workstation full screen or window sessions in ordered rotation. When you send the Alt+Tab command, the target workstation's system menu for the next window is displayed.

To send the Alt+Tab to the target workstation, do either of the following:

- Choose Send Alt+Tab from the Keystrokes pull-down menu on the controller session window (see Figure 28 on page 39).
- If you are in keystrokes local mode, press the **Ctrl+U** shortcut key.

Sending the Ctrl+Esc Command to the Target Workstation: During an active session, you can send the Ctrl+Esc command key.

Sending the Ctrl+Esc allows you to display the OS/2 task list on the OS/2 target workstation. After you display the task list, you can choose a task from the list. To send the Ctrl+Esc to the target workstation, do either of the following:

- Choose Send Ctrl+Esc from the Keystrokes pull-down menu on the controller session window (see Figure 28 on page 39).
- If you are in keystrokes local mode, press the **Ctrl+C** shortcut key.

Transferring Files

DCAF enables you to transfer files to or from the target workstation in the monitoring or active state. You can start a file transfer from the controller only.

Be sure that there is enough free disk space at the target workstation. It should be more than just equal to the size of the file being transferred. Factors affecting the required free disk space for a file transfer are:

- Using the high performance file system (HPFS), which requires more space than file allocation table (FAT)
- Using special options, such as Overwrite, which is shown on Figure 30 on page 41.

In such cases, follow these suggestions:

- If you do not select Overwrite or Compress, the free disk space at the destination must be at least equal to the size of the file being transferred.
- If you select Overwrite, the free disk space at the destination must be at least equal to the size of the file being transferred.
- If you select Compress or Overwrite and Compress, the free disk space at the destination must be at least equal to the size of the file being transferred plus the compressed file.

The source file name is the name of the file being sent. The destination file name is the name of the file at the destination location. The example in Figure 30 on page 41 shows the CONFIG.FIX file. The CONFIG.SYS file arrives at drive C of the target workstation. The file replaces (overwrites) the current CONFIG.SYS on the target.

To transfer files, perform the following steps:

1. Choose Start file transfer... from the Services pull-down menu on the display of the target window (see Figure 29 on page 41).

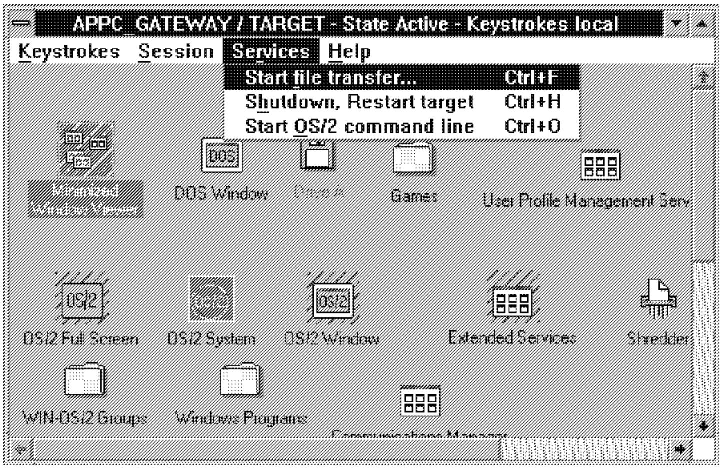

Figure 29. Controller Session Window with Services Pull-Down Menu

The File Transfer Utility window (Figure 30) appears.

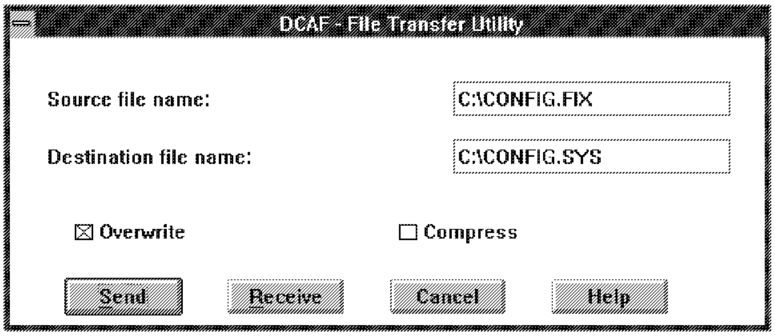

Figure 30. DCAF - File Transfer Utility

2. Type the path and file name of the source file. If the path is not specified, then the drive and directory where the DCAF is installed is used. The syntax for the file name follows High Performance File System (HPFS) and the File Allocation Table (FAT) file name conventions.
3. Type the path and file name of the destination file. If the file name is not specified, then the name of the source file will be used. If you type a path without a file name, be sure to type the final backslash. The file name requirements for the destination file name are the same as the requirements for the source file name.
   a. Select the Overwrite check box if you want to replace any destination file that already exists.
   b. Select the Compress check box to compress the file before it is sent. The file will be compressed for you before it is sent and decompressed after it is received. File compression is useful if you are sending files over a slow line. This is disabled if you are sending or receiving files with a DOS target workstation.
4. Press the **Send** push button to send the file from the controller to the target workstation. Press the **Receive** push button for the controller to receive the file from the target workstation.

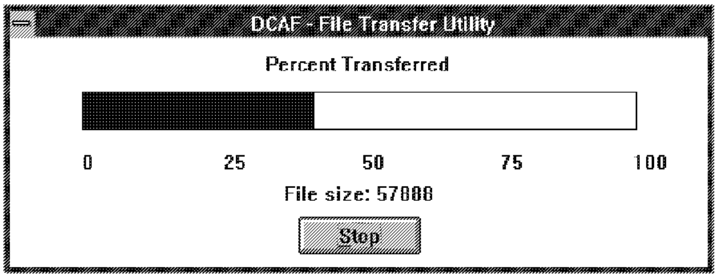

Figure 31. DCAF File Transfer Utility with Percent Transferred

While the file transfer is in progress, the percent-transferred indicator (Figure 31) appears indicating the percentage of the file that has been transferred. The status indicator on the controller and on the target workstation changes the session state to file transfer (while the file transfer is in progress). You can choose to interrupt the file transfer at any time by pressing the **Stop** push button. The target user can stop the file transfer by pressing the hot key combination, if it is enabled. This is valid for all targets except DOS-only workstations.

Restarting the Target Workstation

To shut down and restart the target workstation remotely, be sure that the session is in the active state. From Services on the menu bar of the display of the target window (see Figure 29 on page 41) choose Shutdown, Restart target. The target shuts down and then restarts.

Starting an OS/2 Command Line Session

To start an OS/2 command line on the OS/2 target workstation, be sure that the session is in the active state. From Services on the menu bar of the display of the target window (see Figure 29 on page 41) choose Start OS/2 command line. An OS/2 command line starts on the target.

Using the Mouse during a Session

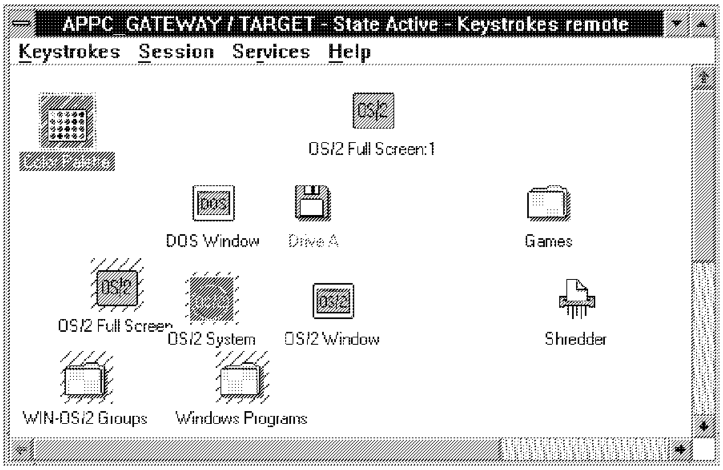

Figure 32. Controller Session Window

Figure 32 shows the controller session window with a view of the target workstation's display. The controller has an active DCAF session with an OS/2 target workstation. The Main group from the target workstation's Desktop has been selected with the mouse pointer by the controller user. The controller is in keystrokes remote mode.

During an active session, the mouse is a useful pointing device for making selections from the controller session menu bar or performing operations on the workstation's display. The keystrokes mode (local or remote) is for the controller workstation keyboard only and has no effect on the mouse.

When the session is active and the Presentation Manager* is the OS/2 active window on the OS/2 target workstation, then you can fully control the mouse pointer of the OS/2 target workstation in the controller session window. You cannot control the mouse pointers of the DOS or OS/2 full screen target workstation because they are not supported by the DCAF. If you start a DOS application on the DOS target workstation during an active session, then the mouse pointer is enabled again for the DOS target user. To correct this problem, temporarily change the session state to monitor and then change back to the active state.

To drive the mouse pointer means that your mouse pointer determines the position of the target mouse pointer, and your mouse clicks are effective on the target workstation. You can control the mouse pointer of the OS/2 target workstation if the following conditions are true:

- The controller session window is the active OS/2 window where the controller user is inputting mouse commands.
- The controller mouse pointer position lies within the controller session window.

When you are driving the OS/2 target mouse pointer, the graphical form of the pointer is determined by applications on the target workstation, and it is reflected in the controller session window. Pictorially, the mouse pointers may not be identical if the operating systems and display drivers of the target and of the controller are different. For example, when the target workstation is not displaying the system pointer (typical of a native Windows or OS/2-emulated Windows target), you see a private DCAF pointer on the controller. However, the mouse pointer displayed on the controller is functionally equivalent to the target workstation's mouse pointer.

Excessive movements of the mouse pointer during the active state in the controller session window can impede the performance of the current operation because the mouse pointer movements send information across the network.

In the active state, the OS/2 target mouse is disabled. In monitoring state, the target mouse pointer is never reflected in the controller session window. During the monitoring, busy, and suspended states, the mice for the controller and the target workstations function independently.

Using Different Keyboard Layouts during a Session

Typically, the keyboard layouts of the controller and target workstations match. When a DCAF session has been established and the keyboard layouts are different, the controller is warned with a message that the keyboard layouts do not match. You are asked, 'Do you want the controller keyboard to match this target's keyboard during the DCAF session?' If you choose to change the keyboard layout, then the keyboard layout changes to match the target workstation for the particular DCAF session only.

For example, the controller's keyboard layout is German and the target workstation's keyboard layout is French. The controller chooses to change the keyboard layout to match the target workstation's keyboard layout. This means that the keystrokes typed by the controller workstation user match the keystrokes of a French keyboard layout during the DCAF session between the controller and the French target workstation. If the controller switches to an OS/2 active window different from the DCAF session window, then the controller keyboard layout is the original one (the German keyboard layout). The controller must realize that a particular key on the controller's German keyboard may map to a different key on a French keyboard layout.

The hot key combination for the controller is affected when the keyboard layout changes. When you press the hot key combination (for example, Alt+T), it must correspond to the key combination for the new keyboard layout.

You are asked once at the beginning of the DCAF session to change the controller keyboard layout to match the target keyboard layout. You have one opportunity to request the DCAF support for mapping the keyboard layouts during that session. If later during the DCAF session you change the controller or target keyboard layout (for example, with the KEYB command from a command line), then the DCAF support for mapping the keyboard layouts is not available.

During a DCAF session between a controller and a DOS target workstation, the keyboard layout is changed to match the keyboard layout code (Table 3), but the default subcountry-code is used. If the default subcountry-code matches the subcountry-code of the DOS target workstation, then the keyboard layouts will match precisely. If the subcountry-codes do not match, then there will be a few discrepancies in the keyboard layouts.

If a keyboard layout is not supported by the DCAF 1.31, then you receive a message stating that it is not supported. See Table 3 for a list of supported keyboard layouts.

Table 3 (Page 1 of 2). Supported Keyboard Layouts

Country	**Keyboard Layout Code**
Belgium	BE
Canada	CF
Denmark	DK
Finland	SU
France	FR
Germany	GR
Italy	IT
Latin America	LA
Netherlands	NL
Norway	NO
Portugal	PO
Spain	SP
Sweden	SV
Switzerland	SF, SG
United Kingdom	UK
United States	US

Table 3 (Page 2 of 2). Supported Keyboard Layouts	
Country	**Keyboard Layout Code**
International English (Australian)	No specific code

Table 4 provides a list of unsupported keyboard layouts.

Table 4. Unsupported Keyboard Layouts	
Country	**Keyboard Layout Code**
Brazil	BR
Czech Republic (Czech)	CZ
Slovakia (Slovak)	SL
Hungary	HU
Yugoslavia	YU
Poland	PL
Arab Countries	No specific code

Using the Virtual DOS Machine on the OS/2 Target

DCAF supports the multiple virtual DOS machine (MVDM), that is, multiple DOS boxes in both a DOS full-screen and DOS window appearance. So, you can select, open, and work in one or more DOS boxes during a session.

Table 5. Using the Virtual DOS Machine on the OS/2 Target

When you run	This is the result
A graphic application on a DOS full-screen	The image cannot be transmitted to your workstation, and you see the message, 'The foreground application is in an unsupported mode and cannot be displayed.'
A graphic application in a DOS window	You see the image.
A text application on a DOS full-screen	You can view your screen and control the target keyboard.
The Personal Communications/3270 Emulation program	There is a conflict of resources and the DCAF does not support this program.

Switching between DOS and Windows Environments on the Windows Target

If you work in more than one environment (for example, in a Windows graphic environment and with an MS-DOS prompt) on the Windows target, ensure that the DOS target was started from a native DOS session before the Windows is started. Otherwise, the following happens:

- In Enhanced mode, the image cannot be transmitted to your controller, and the message, 'The foreground application is in an unsupported mode and cannot be displayed,' appears. To go back to the Windows environment, choose Send Alt+Esc from the Keystrokes pull-down menu.
- In Standard mode, the session goes down until you restart the session.

Some things you should know about the DCAF program and DOS sessions in Windows:

Table 6. Using the MS-DOS Prompt on the Windows Target

When you run	This is the result
A graphic application on a DOS full-screen	The image cannot be transmitted to your controller, and the message, 'The foreground application is in an unsupported mode and cannot be displayed' appears on your screen.
The Personal Communications/3270 Emulation program	There is a conflict of resources and the DCAF does not support this program.

Moving among Multiple Sessions

Moving among the DCAF sessions follows the general conventions for moving around the OS/2 PM (Presentation Manager) windows.

The controller main window displays each DCAF gateway or target session. The current sessions are listed by the appropriate icon (DCAF gateway or target) and workstation name.

To change to a different session, do either of the following:

- Choose the new session from the controller main window.
- Go to the OS/2 task list, and switch to the new session.

You can minimize or maximize the controller session windows and arrange them on the controller display. To return to the controller main window, go to the OS/2 task list and switch to the Distributed Console Access Facility (controller main window).

Managing Controller Options

The controller options include changing the pass phrase and logging your messages.

Changing the Pass Phrase

Pass phrases are required for secure sessions. You can request to change your own pass phrase. The request is sent automatically to the security administrator workstation. The security administrator has to be running in order to process your pass phrase change. If the security administrator is not enabled, you will receive a message that the security administrator is not running and that you should retry the operation at a later time. For more information see *Distributed Console Access Facility Installation and Configuration Guide*.

To change your pass phrase, define a security administrator on your controller. See "Defining or Changing the Security Administrator Description" on page 26 for instructions how to define it. The workstation name is DCAFADMN. See "Adding a Workstation" on page 15. Remember to define the security administrator workstation as the Partner Logical Unit (PLU) Profile in the Communications Manager on the controller.

If you have not already logged on, you must log on to the DCAF. For a description, see "Secure Sessions" on page 30. Then choose Pass Phrase Change... from the Services pull-down menu on the controller main window as shown in Figure 14 on page 24.

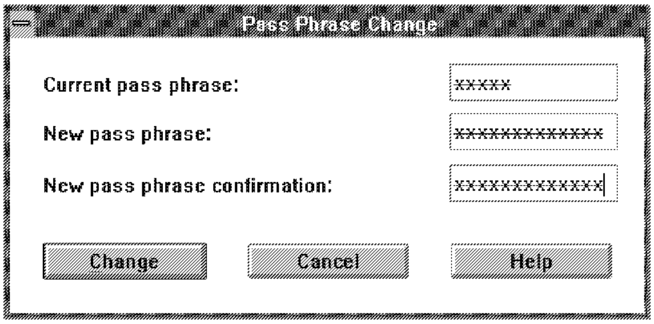

Figure 33. Pass Phrase Change

The Pass Phrase Change window (Figure 33) appears. To request a pass phrase change:

1. For Current pass phrase, type the pass phrase that matches the pass phrase that you typed when you logged on to the DCAF.
2. For New pass phrase, type your new pass phrase.

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

   - Upper- or lowercase letters (A-Z, a-z)
   - Digits (0-9)
   - Special characters: #, @, $ or blank.
3. Retype your new pass phrase in the New pass phrase confirmation field.
4. Press the **Change** push button.

You will receive notification if your request was processed and accepted as a valid request by the security administrator or if it was rejected as not valid. If it is not valid, you may have typed your user ID or pass phrase incorrectly when you logged on to the DCAF. Return to the logon, correct it, and retry the request.

If the request is accepted, the change is not immediate. The new pass phrase will be sent to all the security authenticators with the next file transfer from the security administrator.

To test if the change is complete, log off the controller by choosing Logoff... from the controller main window (see Figure 14 on page 24), and then log on with the new pass phrase and try to establish a session. If you receive a return code 4, then the pass phrase is incorrect. You can log on with the old pass phrase until the new pass phrase is sent to the security authenticators.

Logging Your Messages

To log the error and informational messages that you see, open Personalization and make sure that the Enable Message Log option is selected. The default message log file name is EQNCONT.LOG but you can customize it.

To view the message log file, check for it in the directory where DCAF is installed on your workstation and edit it.

Stopping DCAF

There are two steps to stopping DCAF: stopping the session and exiting the controller.

Stopping the Session

Stop all sessions in one of the following ways:

- From Session on the menu bar of the session window, choose Terminate (Figure 27 on page 37).
- On the Distributed Console Access Facility Controller window (Figure 14 on page 24), choose Stop a session.

Then for secure sessions, from Services on the menu bar of the Distributed Console Access Facility Controller window (Figure 14 on page 24), choose Logoff.... DCAF closes all access to secure sessions from your workstation.

Exiting the Controller

To exit the controller, from Services on the menu bar of the Distributed Console Access Facility Controller window (Figure 14 on page 24), choose Exit.

Chapter 4. Connecting to Targets on a LAN

The controller connects to targets on the same or another LAN through a LAN directory only or through a gateway and LAN directory.

Basic DCAF sessions with OS/2 or Windows targets via IPX/SPX, NetBIOS, or TCP/IP connect through a LAN directory. All secure sessions and all sessions with DOS targets connect through a gateway and LAN directory. See Figure 2 on page 4 for a scenario of targets on a LAN.

Connecting through a LAN Directory

The LAN directory keeps a list of targets that reside on its LAN. It presents targets that are ready for a session to the controller. Any kind of sessions with targets that are on a LAN require a LAN directory.

The LAN directory logs error and informational messages. The default message log file name is EQNLDDIR.LOG and is located in the directory in which DCAF is installed. You can personalize the log file name.

Starting and Stopping the LAN Directory

You can start the LAN directory automatically or manually. To start it automatically, see *Distributed Console Access Facility Installation and Configuration Guide*.

To start it manually, choose the DCAF LAN directory icon from the Distributed Console Access Facility folder on your desktop. The DCAF LAN Directory window (Figure 34) appears.

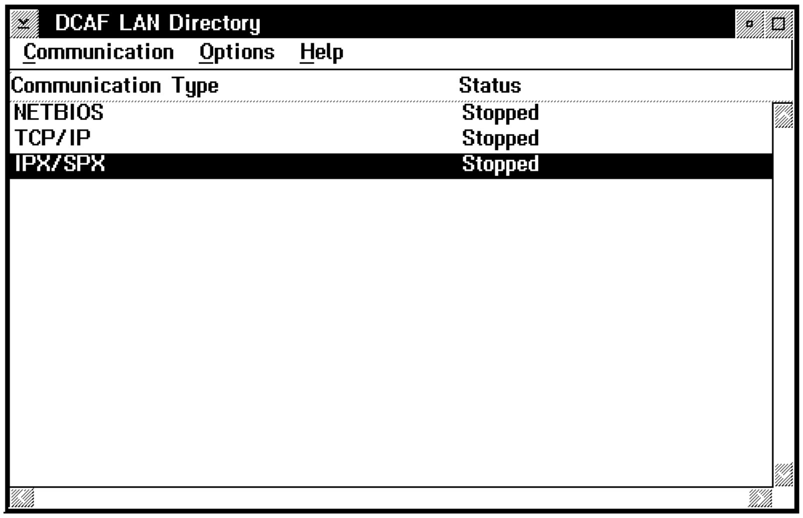

Figure 34. LAN Directory Window

To stop the LAN directory, choose Stop from Communication on the menu bar. The LAN directory directory stops.

© Copyright IBM Corp. 1990, 1995

Creating a File of Target Nicknames

To make it easier to identify targets on the LAN, use a nickname file in which you identify each target by using a nickname and a LAN identifier. When you start a session with a target, use the nickname to locate it in your directory of targets. Create your own nickname file for each communications protocol, or use the following example files included on DCAF diskette 3:

- EQNLDIPX.TXT for IPX/SPX
- EQNLDNET.TXT for NetBIOS
- EQNLDTCP.TXT for TCP/IP

To change the name of the nickname list file, choose Personalization... from Options on the menu bar. See *Distributed Console Access Facility Installation and Configuration Guide* for more details on personalizing the LAN directory.

IPX/SPX Nickname File

Create your own nickname list file with a text editor. For each target workstation, type on a new line your network address plus your node address, one or more blanks, and a nickname. The network address must be exactly 8 digits in length in any combination of hexadecimal numbers. The node address must be exactly 12 digits in length in any combination of hexadecimal numbers. The nickname can be 1–60 characters in length. See "IPX/SPX Protocol Description" on page 21 for character guidelines for both.

Figure 35 provides an example of an IPX/SPX nickname file.

```
0000000150005AAE90F8          Ipx_OS2_target_in_Atlanta
0000000250005A90AFF6          Lan_Target_IpxWin_Room_317
0000000150005A905F17          New_York_Ipx_workstation
0000000450005A900AAB          Bill_Ipx_Target_in_Raleigh
0000000150005A9011F9          Patricia_OS2_Ipx_Target_Rome
```

Figure 35. Example IPX/SPX Nickname File (EQNLDIPX.TXT)

Determining the Network and Node Address: The network address is the NetWare segment number that is defined to the NetWare server on the target's network during the server's installation. It identifies the network of which the target is a part to the controller.

To find the network address, do the following: Start the DCAF target and the IPX/SPX communication type (see *Distributed Console Access Facility Target User's Guide* for instructions). The target network and node addresses appear next to the started IPX/SPX communication type in the target window. The network address is the first eight digits in the hexadecimal value that appears next to the started IPX/SPX communication type in the target window.

You can find the target's node address in one of the following three ways:

- Start the DCAF target and the IPX/SPX communication type (see *Distributed Console Access Facility Target User's Guide* for instructions). The target network and node address appear next to the started IPX/SPX communication type in the target window. The node address is the last twelve digits in the hexadecimal value that appears next to the started IPX/SPX communication type in the target window.

- If the target workstation has LAPS, check the LANTRAN.LOG file in the IBMCOM directory for its universally administered address (UAA).
- Use the reference diskette to get the target's UAA.

TCP/IP Nickname File

You can convert the HOSTS file (if you use a HOSTS file) in the TCPIPETC directory and create a nickname file. Perform the following steps:

1. Copy the HOSTS file from the TCPIPETC directory to the directory in which the DCAF is installed.
2. Remove any comments in the file and make sure that each IP address has a unique alias associated with it.
3. Save and close the file.
4. Rename it with the same name as the nickname file that you assigned for the LAN directory (the default is EQNLDTCP.DAT). You have created a target nickname file for all TCP/IP connections with this LAN directory.

Otherwise, create your own nickname list file with a text editor. For each target workstation, type on a new line the IP address, one or more blanks, and a nickname. The IP address is a unique number that you (or your network administrator) assign to each workstation in the network. It is a string composed of four substrings of numbers, divided by a period (*nnn.nnn.nnn.nnn.*). The range for each substring is 0–255. The nickname can be 1–60 characters in length.

Figure 36 provides an example of a TCP/IP nickname file.

```
10.87.231.80          TcpIp_OS2_target_in_Atlanta
15.125.231.78         Lan_Target_Windows_Room_317
99.200.230.231        New_York_workstation_TcpIp
9.200.231.127         Bill_Target_in_Raleigh
17.156.200.111        Patricia_OS2_TcpIp_Target_Rome
```

Figure 36. Example TCP/IP Nickname File (EQNLDTCP.TXT)

NetBIOS Nickname File

You can convert existing nickname files, such as the LAN Manager names file, into a format that can be used by the DCAF. Figure 37 on page 52 provides a sample REXX program that converts a LAN Manager file for DCAF use.

```
/********************************************************/
/* Sample REXX Conversion File of                        */
/* LAN Manager File to Distributed Console Access        */
/* Facility nickname file                                */
/*                                                       */
/* This REXX command file takes as input a names file    */
/* exported from IBM LAN Manager.  It will reformat      */
/* the name, comment, and flag into a long descriptive   */
/* name acceptable by the Distributed Console Access     */
/* Facility program and create an output file that can   */
/* be used as input to the Distributed Console Access    */
/* Facility LAN Directory.                               */
/********************************************************/
infile = "lanmgr.out"       /* LAN Manager exported names */
outfile = "dcafdir.nam"     /* Distributed Console Access */
                            /* Facility nicknames file    */
do while lines(infile)      /* loop through input file    */
   line = linein(infile)    /* get a line from input file */
   if line = '' then iterate

   /* parse out the address, name, comment and flag       */
   /* from input                                           */
   parse value line with addr name . "" comment "" flag .

   /* strip leading and trailing blanks from the          */
   /* comment field                                        */
   comment = strip(comment, 'B')

   /* translate embedded blanks in comment to underscores */
   comment = translate(comment, '_', ' ')

   /* create a long descriptive name for the              */
   /* LAN Directory                                        */
   dcafname = name || '_' || comment || '_' || flag

   call lineout outfile, left(addr, 16) left(dcafname, 60)
end                         /* end of loop through file   */
return
```

Figure 37. Example of REXX Program that Converts Files into DCAF Nickname File

Otherwise, create your own nickname list file with a text editor. For each target workstation, type on a new line the LAN adapter address (exactly 12-characters in length), exactly ten blanks, and a nickname (1–60 characters). Figure 38 provides an example.

```
10005A100992          Teller_Paris
400001233210          Helpdesk_new_employees
10005A000111          Gateway_OS/2_Room_A2-401
400001230777          OS/2_H_Room_C3-512
```

Figure 38. Example NetBIOS Nickname List File

Determining the LAN Identifier Number (Adapter Address): You can find the target adapter address in one of the following ways:

- Start the target and LAN communication type. The OS/2 or Windows target window displays the LAN identifier. The DOS target window displays the LAN identifier when you press the hot key.
- If the target workstation has LAPS, check the LANTRAN.LOG file in the IBMCOM directory for its universally administered address (UAA).
- Use the reference diskette to find the target′s UAA.

Connecting through a Gateway

The gateway enables workstations to establish a session for the following connections:

- Secure sessions
- Sessions through an SNA backbone

Both cases require a LAN directory.

The gateway provides a constantly updated list of available targets with which you can start a session.

You can use any communications protocol to connect to the gateway. The gateway connects to the target via NetBIOS only.

A gateway can provide connections for up to 254 sessions simultaneously provided it has sufficient NetBIOS resources. See *Distributed Console Access Facility Installation and Configuration Guide* for information on configuring and personalizing the gateway.

Logging Messages

The gateway logs error and informational messages received during the sessions. The default message log file name is EQNGWAUD.LOG but you can personalize it. It is located in the directory in which DCAF is installed.

The log file provides an audit trail for secure and password-only sessions. For secure sessions, DCAF logs the user ID of the controller that connects to a secure target. For basic APPC/APPN sessions, DCAF logs the fully qualified PLU name of the controller.

You cannot change or erase the log file. When the log file reaches a maximum of 64000 bytes, DCAF converts it into a backup .LAB file and starts a new .LOG file of the same name. You can change or erase the .LAB file.

If there is more than one LAN directory on a logical LAN, personalize the LAN directory name on the gateway to make it unique on the LAN. The default LAN directory name is DCAFLAN. It is case sensitive.

Starting and Stopping the Gateway

The gateway starts automatically when you start the workstation. To start it automatically, see *Distributed Console Access Facility Installation and Configuration Guide*.

The gateway is running when you see the **DCAF Gateway initialization** icon in the icon view of the DCAF work folder. There is no user interface window for the gateway.

The gateway stops when you shut down the gateway workstation.

Part 3. Appendixes

© Copyright IBM Corp. 1990, 1995

Appendix A. Diagnosis

This appendix includes the most common problems users find when using DCAF and their solutions.

Table 7. Troubleshooting for DCAF

Problem	Solution
If you run the **Microsoft antivirus** program provided by Microsoft DOS 6.0 on a Windows target during an active or monitoring DCAF session, you may get an error when you start the antivirus program.	Start the antivirus program before you start the DCAF session.
When you run the Microsoft Windows **Display Test Application** on a Windows target, there may be a conflict or the DCAF session ends.	Avoid running this program during a DCAF session.
Your **mouse performance** is extremely slow during a session with any target running in DOS.	If you are using IBM LAN Support Program Version 1.30.1, you can improve mouse performance by including the following parameter in the DXMT0MOD.SYS statement: **PBA=0**.
When starting an APPC connection, you get an **APPC error**.	First, check physical network connections. Then check communication configurations.
You **shut down a DOS or Windows target** from the controller and an unexpected error occurs at the target.	Do the following: 1. Edit the CONFIG.SYS on the controller. 2. Change the three NetBIOS statements from: DEVICE=. . . to: DEVICEHIGH=. . . 3. Restart the workstation. 4. Restart the DCAF session.
You see a **blank screen** when starting a session with a downlevel target.	The target that you are trying to connect to has an earlier release of DCAF installed. The display driver that the target is using is not compatible with the one used by your workstation.
An **IPX session** with a Windows target remains in Initiating but never starts.	Targets running on Windows 3.11 do not support Novell NetWare Requester for DOS/Windows.

Checking the Message Log Files

For problem determination, see the DCAF message log files. Message log files are located in the same directory in which the DCAF component is installed. Table 8 shows a list of the default message log files.

Table 8 (Page 1 of 2). Message Log Files for the DCAF Components

DCAF Component	Message Log File
Controller	EQNCONT.LOG
OS/2 Target	EQNTG.LOG
DOS or Windows Target	EQNDDERR.LOG
LAN Directory	EQNLDDIR.LOG
DCAF Gateway	EQNGWAUD.LOG
Security Administrator	EQNADMN.LOG

© Copyright IBM Corp. 1990, 1995

Table 8 (Page 2 of 2). Message Log Files for the DCAF Components	
DCAF Component	**Message Log File**
Security Authenticator	EQNAUTH.LOG

How to Avoid Losing Personalization Options

If you install DCAF directly and later use the packager to install DCAF components on the same workstation, any original DCAF personalization options might be replaced by the personalization options in the DCAF package. This problem occurs most frequently when you install a security authenticator directly and later use the packager to install other components on the same workstation.

To avoid this problem, install the components in the following order:

1. Create a DCAF package with all the desired components.
2. Unpack the package at the workstation.
3. Restart the workstation.
4. Install the security authenticator from the DCAF diskettes.
5. Restart the workstation.

For the Controller

Some helpful information for using the controller follows:

If you notice that you do not see data from the target display on your screen, there may be applications that update the target screen continually running on the target. Because DCAF displays the most recent data from the target on your screen, previous screen data from the target may be overwritten by other data that arrives more quickly on your screen. You see only the most recent target screen.

During sessions, DOS target colors may change slightly when they arrive on your screen.

To See Windows Applications on the OS/2 Target Screen

To control a Windows application that is running on an OS/2 target, perform the following steps:

1. Open the Windows Program folder.
2. Start the Program Manager.
3. Start the Windows application that you want to use. Then you can see it from the controller.

Ctrl+Esc Does Not Work on the Windows Target

This symptom has various causes. When you send a Ctrl+Esc command to IPX/SPX Windows target and nothing happens, free some space in low memory. Make the following changes:

- Run as many applications as you can in high memory.

- In the CONFIG.SYS file, change the statement:

  DEVICE=path:directorySMRTDRV.EXE

  to

  REM DEVICE=path:directorySMRTDRV.EXE

- In the AUTOEXEC.BAT file, change the statement:

  path:directorySMRTDRV.EXE

  to

  REM path:directorySMRTDRV.EXE

When you press the hot key at the controller to make the keystrokes local and send a Ctrl+Esc command to any Windows target and nothing happens, do the following to fix the problem. Send an Alt+Tab or an Alt+Esc command to the target and then send a Ctrl+Esc. The command works on the target.

IPX/SPX Windows Target Does Not Have Enough Memory

If on the IPX/SPX Windows target you try to start the File Manager or other Windows applications and you receive a message stating that the workstation does not have enough memory, free some space in low memory. Make the following changes:

- Run as many applications as you can in high memory.

- In the CONFIG.SYS file, change the statement:

  DEVICE=path:directorySMRTDRV.EXE

  to

  REM DEVICE=path:directorySMRTDRV.EXE

- In the AUTOEXEC.BAT file, change the statement:

  path:directorySMRTDRV.EXE

  to

  REM path:directorySMRTDRV.EXE

Appendix B. Application Programming Interfaces (APIs)

This appendix provides General-Use Programming Interface and Associated Guidance Information. It is divided into three main sections:

- The EQNAPI.DLL APIs
- Calling EQNAPI.DLL APIs from a 32-Bit Application
- The EQNLR.DLL APIs

The APIs enable you to write programs that use some of the services that the DCAF provides. The programs using the DCAF APIs must be Presentation Manager applications.

The DCAF provides the following APIs in EQNAPI.DLL:

- DCAFOpen (session initialization)
- DCAFClose (session close)
- DCAFShowSession (make the DCAF session the top window)
- DCAFXfer (file transfer)

The DCAF provides the following APIs in EQNLR.DLL:

- LrOpenLR (open the workstation directory on the controller)
- LrCloseLR (close the workstation directory on the controller)
- DeleteWs (delete a workstation from the controller directory)
- ReadWs (view a workstation description in the controller directory)
- WriteWs (add or change a workstation in the controller directory)

This file contains all of the type definitions and constants that are required for application programmers to write applications using the DCAF APIs.

Reminder: You must start the DCAF controller before you start any applications using the APIs. Include the statement **START EQNMAIN** at the beginning of your application, or ensure that you open the DCAF Controller icon before running your application.

The EQNAPI.DLL APIs

These files can be found in the path and directory where the DCAF controller is installed. An include file, EQNDCAF.H, is provided on diskette number 3 for EQNAPI.DLL.

For EQNAPI.DLL, a sample API program, named APISMP.C, is supplied with the DCAF installation diskettes in the directory APISMP. A short description of the sample program appears at the beginning of the file. The command APISMP.CMD, also included, is used to compile and run the sample program.

DCAFOpen: Session Initiation API

This API allows an application program to initiate a DCAF session by passing, in a control block, the required session information for a specific DCAF gateway and/or target workstation. If the API was started unsuccessfully (that is, the DCAF main program is not active), a return code equal to 1 will be returned to the calling process and no message will be posted to the calling process. If the API was started successfully, but the session was unsuccessfully started, a nonzero return code will be returned to the calling process as a posted message. If a session was started successfully, a DCAF session handle and a

© Copyright IBM Corp. 1990, 1995

return code equal to zero will be returned to the calling process as a posted message. The returned handle must be used by the application to close the DCAF session at a later time. This handle is also a required parameter for all the other DCAF APIs. The DCAFOpen requires that the DCAF product on the controller be running and that the user be logged on if the requested session is with a secure target workstation. The call syntax is as follows:

DCAFOpen (hCaller, open_structure_ptr)

where:

Hcaller (HWND) - input
HWND (window handle) of the window that requests the API service

open_structure_ptr (POPEN_STRUCTURE) - input
Pointer to a structure containing session information

rc (BOOL) - return
Return code descriptions are:

1 error occurred
0 no error occurred

Message posted by DCAF to the caller at the end of the call:

DCAF_STARTSESSIONRESPONSE

Parameters

param1

hDcaf (USHORT)
DCAF session handle
result (USHORT)
return code

param2

addr (POPEN_STRUCTURE)
pointer to open_structure

Session Information structure:

typedef **struct _OPEN_STRUCTURE**

CHAR **link_rec_name** (61 bytes) /* workstation name */

CHAR **lan_target_name** (60 bytes) /* target name */

CHAR **target_pw** (8 bytes) /* target password */

CHAR **gateway_pw** (8 bytes) /* gateway password */

-OPEN_STRUCTURE;

typedef **OPEN_STRUCTURE** far * **POPEN_STRUCTURE**; /* structure pointer */

DCAFClose: Session Close API

This API allows an application program to request that a DCAF session be closed. The DCAF session must have been started via the DCAFOpen, prior to the invocation of this API.

If the API was started unsuccessfully, a return code equal to 1 will be returned to the calling process, and no message will be posted to the calling process. If the API call is successful, then a return code equal to zero will be returned to the calling process, and a message will be posted.

In the case where the API is successfully started, but started with an incorrect **hDcaf** parameter, the return code will be zero, but no message will be posted. It is important to receive the posted message to ensure that the API call is successful.

The application must pass, as a parameter, the session handle returned by DCAF when the session was first started. The call syntax is as follows:

DCAFClose (hDcaf)

where:
hDcaf (USHORT) - input
DCAF session handle

rc (BOOL) - return
Return code descriptions are:

1 error occurred
0 no error occurred

Message posted by DCAF to the caller at the end of the call:

DCAF_ENDSESSIONRESPONSE

Parameters

param1

hDcaf (USHORT)
DCAF session handle
result (USHORT)
return code

param2

empty

DCAFShowSession: Make the DCAF Session Top Window

This API allows an application program to request that a previously started DCAF session be brought to the foreground and made the top window. The DCAF session must have been started via the DCAFOpen, prior to the invocation of this API.

If the API was started unsuccessfully, a return code equal to 1 will be returned to the calling process, and no message will be posted to the calling process. If the

API call is successful, then a return code equal to zero will be returned to the calling process, and a message will be posted.

In the case where the API is successfully started, but started with an incorrect **hDcaf** parameter, the return code will be zero, but no message will be posted. It is important to receive the posted message to ensure that the API call is successful.

Receiving the posted message may be useful for applications that serve as a user shell. With this call, the application can display the DCAF Session window again even though it may have released the focus to another window. The application must pass, as a parameter, the session handle returned by DCAF when the session was first started. The call syntax is as follows:

DCAFShowSession (hDcaf)

where:

hDcaf (USHORT) - input
DCAF session handle

rc (BOOL) - return
Return code descriptions are:

1 error occurred
0 no error occurred

Message posted by DCAF to the caller at the end of the call:

DCAF_SHOWSESSIONRESPONSE

Parameters

param1

hDcaf (USHORT)
DCAF session handle
result (USHORT)
return code

param2

empty

DCAFXfer: File Transfer API

This API allows an application program to initiate a file transfer via DCAF. The DCAF session must have been started via the DCAFOpen, prior to the invocation of this API.

If the API was started unsuccessfully, a return code equal to 1 will be returned to the calling process, and no message will be posted to the calling process. If the API call is successful, then a return code equal to zero will be returned to the calling process, and a message will be posted.

In the case where the API is successfully started, but started with an incorrect **hDcaf** parameter, the return code will be zero, but no message will be posted. It is important to receive the posted message to ensure that the API call is successful.

The application must pass as parameters, the session handle, file specification and transfer flag. The transfer flag parameter of this API is used to indicate whether to start or stop the file transfer. The **status** element of the **file_transfer_entry_ptr** parameter must be set to 1 to receive the **DCAF_TRANSTATUS** posted message. The call syntax is as follows:

DCAFXFer (hDcaf, cmd, file_transfer_entry_ptr)

where:

hDcaf (USHORT) - input
DCAF session handle

cmd (BOOL) - input
Transfer action flag; start or stop a file transfer:

0 Start file transfer

1 Stop file transfer

file_transfer_entry_ptr (PXFERENTRY) - input
Pointer to the structure containing file transfer information

rc (BOOL) - return
Return code descriptions are:

1 error occurred
0 no error occurred

Messages posted by DCAF to the caller at the end of the call:

DCAF_STARTTRANRESPONSE
DCAF_STOPTRANRESPONSE

Parameters

param1

hDcaf (USHORT)
DCAF session handle
result (USHORT)
return code

param2

empty

DCAF_TRANSTATUS

Parameters

param1

hDcaf (USHORT)
DCAF session handle
percent (SHORT)

percent of file transferred expressed as a whole number between 0 and 100, inclusive

param2

empty

File Transfer Information structure:

```
define MAX_LEN   256               /* bytes */

typedef struct _XFERENTRY

   BOOL receive     /* controller send-receive switch:
                                     1=receive, 0=send */

   BOOL overwrite   /* overwrite switch:
                                  1="Yes", 0="No" */

   BOOL nocompress /* compression switch:
                                  0="Compression", 1="No Compression" */

   BOOL status      /* send to the user application percent
                                  of transferred file:
                                  1="Yes", 0="No" */

   CHAR sourcefile MAX_LEN    /* source path and file name */

   CHAR destfile MAX_LEN      /* destination path and file name */

- XFERENTRY;

typedef XFERENTRY FAR * PXFERENTRY; /* structure pointer  */
```

Calling EQNAPI.DLL APIs from a 32-Bit Application

The EQNAPI.DLL APIs were written in 16-bit code. Therefore, some problems may occur if you call them from a 32-bit application.

The following sections provide the changes that you should make in the EQNDCAF.H file to get the APIs to work in a 32-bit environment.

Changes to DCAFOpen

Make the following changes to the Session Information (_OPEN_STRUCTURE) structure:

Table 9. Changes to the OPEN_STRUCTURE

For 16-bit Version	For 32-bit Version
typedef struct _OPEN_STRUCTURE	typedef _Packed struct _OPEN_STRUCTURE

Changes to DCAFXfer

Make the following changes to the File Transfer Information (_XFERENTRY) structure:

Table 10. Changes to the _XFERENTRY

For 16-bit Version	For 32-bit Version
typedef struct _XFERENTRY	typedef _Packed struct _XFERENTRY
BOOL receive; BOOL overwrite; BOOL nocompress; BOOL status;	BOOL16 receive; BOOL16 overwrite; BOOL16 nocompress; BOOL16 status;

Changes to the DCAF API Prototypes

Make the following changes to the DCAF API prototypes on lines 54 through 57:

Table 11. Changes to the DCAF API Prototypes

For 16-bit Version	For 32-bit Version
BOOL FAR PASCAL DCAFOpen(HWND, POPEN_STRUCTURE); BOOL FAR PASCAL DCAFClose(USHORT); BOOL FAR PASCAL DCAFShowSession(USHORT); BOOL FAR PASCAL DCAFXfer(USHORT, BOOL, PXFERENTRY);	pragma linkage(DCAFOpen, far16 pascal) pragma linkage(DCAFClose, far16 pascal) pragma linkage(DCAFShowSession, far16 pascal) pragma linkage(DCAFXfer, far16 pascal) SHORT DCAFOpen(HWND, POPEN_STRUCTURE); SHORT DCAFClose(USHORT); SHORT DCAFShowSession(USHORT); SHORT DCAFXfer(USHORT, BOOL, PXFERENTRY);

The EQNLR.DLL APIs

For EQNLR.DLL a sample API program, consisting of the following files, is included in the DCAF installation diskettes.

- LRSMP.C. Sample source code.
- LRSMP.DEF. A sample definition file.
- LRSMP.H. A sample header.
- LRSMP.L. A sample link file.
- LRSMP.MAK. A sample make file.

To build the LRSMP sample program, perform the following steps.

Note: You must use a 32-bit compiler, such as the IBM C-Set/2 compiler, and the IBM Developer's Toolkit for OS/2 Version 2.1.

1. Copy all the LRSMP.* files from DCAF diskette 3 to your working directory.
2. Copy EQNLR.DLL from the directory in which DCAF is installed to your working directory.
3. Type **nmake /f lrsmp.mak**.

Any errors generated when you run these APIs are logged in the EQNLR.LOG file.

LrOpenLR: Open the Workstation Directory

This API allows an application program to open the workstation directory on the controller.

Note: The EQNLR.INI file, which keeps record of the workstations in the DCAF directory can be corrupted. It is recommended that you always make a backup copy of the EQNLR.INI file after you have established a stable list of workstations in the DCAF directory. If the API is successful, the handle of the EQNLR.INI file is returned to the calling program. If an error occurs, NULL is returned to he calling program. The call syntax is as follows:

hini LrOpenLR (HAB hab, BOOL bFlag)

where:
hab (HAB) - input
Anchor block handle of the calling program.

bFlag (BOOL) - input
The parameter may be one of the following:
CREATE 0
OPEN 1

LrCloseLR: Close the Workstation Directory

This API allows an application program to close the workstation directory on the controller. If the API is successful, TRUE is returned to the calling program. If an error occurs, FALSE is returned to the calling program.

The call syntax is as follows:

BOOL LrCloseLR (hini)

where:
hini (HINI) - input
HINI (handle) of the profile EQNLR.INI

rc (BOOL) - return
The return value is TRUE if the function is successful, FALSE if an error occurs.

DeleteWs: Delete a Workstation from the Directory

This API allows an application program to delete a workstation from the controller directory. If the API was started unsuccessfully, a return code equal to 1 will be returned to the calling process will be posted to the calling process. If the API is successful, the workstation is removed from the workstation directory and a TRUE value is returned. Otherwise, the workstation is not removed and a FALSE value is returned. The call syntax is as follows:

BOOL DeleteWs (hini, pLRKey Name)

where:
hini (HINI) - input
HINI (handle) of the profile EQNLR.INI

pLRKey Name (PBYTE) - input
Pointer to the workstation name string

rc (BOOL) - return
Return code descriptions are:

FALSE if an error occurs.
TRUE if the function is successful.

ReadWs: View a Workstation in the Directory

This API allows an application program to read a workstation description in the controller directory. If the API is successful, the values of the workstation are returned in pLRBuffer and TRUE is returned to the calling process. Otherwise, a FALSE value is returned to the calling process. Start the controller before you run the ReadWs API. The call syntax is as follows:

ReadWs (hini, pLRKey Name, pLRBuffer)

where:

hini (HINI) - input
HINI (handle) of the profile EQNLR.INI

pLRKey Name (PBYTE) - input
Pointer to the workstation name string

pLRBuffer (PSFDAT_RECORD) - output
Pointer to the buffer that receives the data for the given workstation name.

rc (BOOL) - return
Return code descriptions are:

FALSE if an error occurs.
TRUE if the function is successful.

SFDAT_RECORD structure:

```
typedef struct _SFDAT_RECORD{
 CHAR sfdat_name[SFLRN_MAX62];        /* workstation name */
 CHAR sfdat_type[2];         /* workstation type*/
 union _REC_SIZE{
  CHAR sfdat_rest[SFMAX_REC_SIZE];
 } sfflags;

 struct        {    /*Overlay first two bytes 02,03 types*/
    BYTE sfdat_icon_flag; /* connection   */
    BYTE sfdat_secure_flag; /* security   */
    CHAR sfappc_lu_alias[8]; /* local LU name */
    CHAR sfappc_partner_lu_alias[8];/*partner LU name*/
    CHAR sfappc_mode_name[8]   /* mode of allocation */
    CHAR sfappc_tp_name[64]   /* transaction program name */
 } sfappc_record;

 struct        {    /* APPC DCAF data type 01 */
    CHAR sfappc10_lu_alias[8]; /* local LU name */
    CHAR sfappc10_partner_lu_alias[8]; /* partner LU name */
    CHAR sfappc10_mode_name[8]; /* mode of allocation *
 } sfappc10_record;

 struct        {    /* ACDI async specific DCAF type 02 */
    BYTE sfacdi_icon_flag;     /* connection */
```

```
      BYTE sfacdi_secure_flag; /* security */
      CHAR sfacdi_device_name[8]; /* character device name */
      USHORT sfacdi_line_speed; /* BitRate (bps) of line*/
      USHORT sfacdi_call_retries; /* num of call retries  *
      USHORT sfacdi_retry_delay; /* delay between call retries */
      CHAR sfacdi_telephone_num[250]; /*telephone number */
      BYTE sfacdi_connect_type;   /* connection type 0-4*/
      BYTE sffiller;
   } sfacdi_record;

   struct       {   /* ACDI async specific DCAF type 00 */
      CHAR sfacdi10_device_name[8]; /* character device name */
      USHORT sfacdi10_line_speed; /* BitRate (bps) of line*
      USHORT sfacdi10_call_retries; /* num of call retries
      USHORT sfacdi10_retry_delay; /*delay between call retries */
      CHAR sfacdi10_telephone_num[250];/*telephone number */
      BYTE sffiller10;  } sfacdi10_record;

   struct         {   /* NETBIOS specific data type 04 */
      BYTE sfncb_icon_flag; /* connection */
      BYTE sfncb_secure_flag; /* security */
      CHAR sfncb_name[12];/* network control block name */
      CHAR sfncb_callname[12];/*network ctrl.blk.call name */
      BYTE sfncb_adapter_flag; /* byte for adapter */
   } sfncb_record;

   struct         {     /* TCP/IP specific data type 05    */
      BYTE sftcp_icon_flag; /* byte for connection*/
      BYTE sftcp_secure_flag; /* secure/non secure flag  */
      CHAR sftcp_callname[256]; /*remote host name */
      USHORT sftcp_socket; /* remote port number */
   } sftcp_record;

   struct         {     /* IPX/SPX specific data type 06    */
      BYTE sfipx_icon_flag; /* byte for connection */
      BYTE sfipx_secure_flag; /* secure/non secure flag  */
      CHAR sfipx_nwaddr[8]; /*remote network address */
      USHORT sfipx_socket; /* remote socket number */
   } sfipx_record;

   struct         {     /* APPN specific data type 07    */
      BYTE sfappn_icon_flag; /* byte for connection   */
      BYTE sfappn_secure_flag; /* secure/non secure flag  /
      CHAR sfappn_lucp_[8]; /* lu/cp alias */
      CHAR sfappn_mode_name[8];  /* mode name */
      CHAR sfappn_mode_name[17];  /* fully qualified plu name */
   } sfappn record;
  } REC_SIZE;
 } SFDAT_RECORD;
typedef SFDAT_RECORD FAR *PSFDAT_RECORD; /* pointer to SFDAT_RECORD structure*/
```

Table 12 provides a description of the entries in the SFDAT_RECORD structure.

Table 12 (Page 1 of 3). Description of the SFDAT Structure			
Field Name	**Type**	**Accepted Values**	**Description**
sfdat_name	CHAR (62)	1–62 characters in length, (A – Z, a – z, 0–9), embedded blanks are not valid.	Workstation name
sfdat_type	CHAR (2)	Asynchronous="02" APPC="03" NetBIOS="04" TCP/IP="05" IPX/SPX="06" APPN ="07"	Communication protocol type
sfdat_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sfdat_secure_flag	BYTE	Secure target 1 Nonsecure Target 0	Security
sfappc_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sfappc_secure_flag	BYTE	Secure target=1 Nonsecure Target=0	Security
sfappc_lu_alias	CHAR (8)	1–8 characters in length, any combination of characters, except left, right parenthesis, comma, semicolon, blanks and cannot start with @. You can leave it blank if you want to use the CP name.	Local LU name
sfappc_partner_lu_alias	CHAR (8)	same as sfappc_lu_alias	Partner LU name
sfappc_mode_name	CHAR (8)	same as sfappc_lu_alias	Mode name for DCAF in your network
sfappc_tp_name	CHAR (64)		Reserved
sfacdi_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sfacdi_secure_flag	BYTE	Secure target=1 Nonsecure Target=0	Security
sfacdi_device_name	CHAR (8)	"COM1", "COM2", "COM3"	Communication port number of the workstation
sfacdi_line_speed	USHORT	1200, 2400, 4800, 9600, 19200, 38400, 48000, 56000, 57800, 64000	Modem transmission rate in bits per seconds
sfacdi_call_retries	USHORT	0–20	Number of times you want DCAF to redial the telephone number
sfacdi_retry_delay	USHORT	1–1200	Pause in between retries (in seconds)
sfacdi_telephone_num	CHAR (250)	Max of 250 characters	Modem telephone number of the workstation
sfacdi_connect_type	BYTE	MANUAL=0 AUTO=2	Kind of dialing
sffiller		Reserved	

Table 12 (Page 2 of 3). Description of the SFDAT Structure			
Field Name	**Type**	**Accepted Values**	**Description**
sfncb_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sfncb_secure_flag	BYTE	Secure target=1 Nonsecure target=0	Security
sfncb_name		Reserved	
sfncb_callname	CHAR (12)	Exactly 12 characters in length, (A – F,a – f,0–9), special characters	Network call address if you are defining a target, LAN directory name if you are defining a LAN Directory
sfncb_adapter_flag	BYTE	0– 3	Adapter number of the workstation
sftcp_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sftcp_secure_flag	BYTE	Secure target=1 Nonsecure target=0	Security
sftcp_call_name	CHAR (256)	1–256 characters in length (A – Z,a – z,0–9), all special characters except blanks	Host name of the workstation
sftcp_socket	USHORT	1024-65534	Port number of the workstation
sfipx_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sfipx_secure_flag	BYTE	Secure target=1 Nonsecure Target=0	Security
sfipx_nwaddr	CHAR (8)	Exactly 8 characters in length, (A – F,a – f,0–9). The range is 00000000 – FFFFFFFE	Network address of the workstation
sfipx_nodeaddr	CHAR (12)	Exactly 12 characters in length, (A – F,a – f,0–9). The range is 000000000000 to FFFFFFFFFFFF	Node address of the workstation
sfipx_socket		Reserved	
sfappn_icon_flag	BYTE	TARGET=0 GATEWAY=1 ADMINISTRATOR=2 LAN Directory=3	Connection
sfappn_secure_flag	BYTE	Secure target=1 Nonsecure Target=0	Security
sfappn_lucp_alias	CHAR (8)	1–8 characters in length, any combination of characters, except left, right parenthesis, comma, semicolon, blanks and cannot start with @. You can leave it blank if you want to use the CP name.	Controller LU name
sfappn_mode_name	CHAR (8)	Same as the sfappn_lucp_alias	Mode name for DCAF in your network

Table 12 (Page 3 of 3). Description of the SFDAT Structure			
Field Name	**Type**	**Accepted Values**	**Description**
sfappn_fqplu_name	CHAR (17)	Same as the sfappn_lucp_alias	Controller node ID and destination workstation LU name

WriteWs: Add or Change a Workstation in the Directory

This API allows an application program to open a workstation description in order to add a new workstation or change an existing one in the controller directory. To add a workstation, fill out the SFDAT_RECORD structure and call the WriteWs API. To call the WriteWs API, pass the handle HINI that is returned by the OpenWs API and pass the pointer to the SFDAT_RECORD structure.

Note: Do not use this API to define the a security administrator. You must define it from the notebook (see "Defining or Changing the Security Administrator Description" on page 26).

If there are errors in the workstation definition, they are logged in the EQNLR.LOG file. If a workstation definition is incorrect, the workstation is not added to the EQNLR.INI file. The call syntax is as follows:

WriteWs (hini, pLRBuffer)

where:

hini (HINI) - input
HINI (handle) of the profile EQNLR.INI

pLRBuffer (PSFDAT_RECORD) - input
Pointer to the buffer that receives the data for the given workstation name.

rc (UNSHORT) - return
Return code descriptions are:

FALSE if an error occurs.
TRUE if the function is successful.

Uses the same structure as the ReadWs API.

Appendix C. Using DCAF to Run Your Own Applications on a Target Workstation

By creating your own application and compiling it with DCAF, you can use DCAF to run your application on a target workstation *before* the session starts. For example, you can do a security check from the target before a controller gets access to it, or you can enable the target user to accept or reject incoming sessions initiated by the controller.

DCAF diskette 3 contains, in directory A:EXIT, a sample application that enables the target user to accept or reject the session. The sample files include a source file that shows how to get your application to communicate with DCAF and a compiled executable file that displays a message to accept or reject the session. You can use the following sample files to write an application adapted to your network′s needs.

Sample Files for OS/2 Targets

You can use the following sample files to write an application for the OS/2 target.

- STRTEXIT.C
- STRTEXIT.DEF
- STRTEXIT.EXE
- STRTEXIT.L
- STRTEXIT.MAK

The following excerpt from STRTEXIT.C shows the conditions that you must use to start or prevent the session, depending on how the user responds to the message. End the routine with DosExit. Use return code **0** to start the session and return code **1** to prevent the session.

```
rcode = WinMessageBox(HWND_DESKTOP,
              hwnd,
              ″There is an incoming session. Do you want to continue?″,
              ″Distributed Console Access Facility″,
               (USHORT) 0,
               (ULONG) (MB_YESNO | MB_ICONHAND));
 if (rcode == MBID_YES)
   {
     RETURN_CODE = 0;
     DosExit(EXIT_PROCESS,RETURN_CODE);
   }
 else
   {
     RETURN_CODE = 1;
     DosExit(EXIT_PROCESS,RETURN_CODE);
   }
```

When you complete your OS/2 application, compile it with a 32-bit compiler, such as the IBM C-Set/2 compiler, and the IBM Developer′s Toolkit for OS/2 Version 2.1.

© Copyright IBM Corp. 1990, 1995

Sample Files for Windows Targets

You can use the following sample files to write an application for the Windows target.

- WSTRTEXI.C
- WSTRTEXI.DEF
- WSTRTEXI.EXE
- WSTRTEXI.MAK

The following excerpt from WSTRTEXI.C shows the conditions that you must use to start or prevent the session, depending on how the user responds to the message. To start the session, send the following message to the target: UI_ACCEPT_OPEN. To prevent the session, send the following message to the target: UI_REJECT_OPEN.

```
        rc =  MessageBox(hwnd,
                         "There is an incoming session. Do you
                         want to continue?",
                         "Distributed Console Access Facility",
                         MB_YESNO | MB_ICONHAND);

        if (rc == IDYES)
    {
              PostMessage(hWnd, UI_ACCEPT_OPEN, wMsg, 0L);
    }

        if (rc == IDNO)
    {
              PostMessage(hWnd, UI_REJECT_OPEN, wMsg, 0L);
    }
```

When you complete your Windows application, compile it with the Microsoft C/C++ Compiler Version 7.0

Glossary of Terms and Abbreviations

This glossary defines important DCAF terms and abbreviations. It includes information from the *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994. Definitions from the *American National Dictionary for Information Processing* are identified by an asterisk (*). Definitions from draft proposals and working papers under development by the International Standards Organization, Technical Committee 97, Subcommittee 1 are identified by the symbol **(TC97)**. Definitions from the *CCITT Sixth Plenary Assembly Orange Book, Terms and Definitions* and working documents published by the Consultative Committee on International Telegraph and Telephone of the International Telecommunication Union, Geneva, 1980 are preceded by the symbol **(CCITT/ITU)**. Definitions from published sections of the *ISO Vocabulary of Data Processing*, developed by the International Standards Organization, Technical Committee 97, Subcommittee 1 and from published sections of the *ISO Vocabulary of Office Machines*, developed by subcommittees of ISO Technical Committee 95, are preceded by the symbol **(ISO)**.

For abbreviations, the definition usually consists only of the words represented by the letters; for complete definitions, see the entries for the words.

Reference Words Used in the Entries

The following reference words are used in this glossary:

Contrast with. Refers to a term that has an opposed or substantively different meaning.

See. Refers to multiple-word terms that have the same last word.

See also. Refers to related terms that have similar (but not synonymous) meanings.

A

ACDI. Asynchronous Communications Device Interface.

active. In the DCAF program, the session state in which the controller has control of the target workstation. The target workstation keyboard is locked. That is, any keystrokes or mouse commands entered by the target workstation user will not be processed by applications running on the target workstation.

active window. The window with which a user is currently interacting. This is the window that receives keyboard and mouse input from the user. Contrast with *inactive window*.

administrator. See *security administrator*.

Advanced Peer-to-Peer Networking* (APPN). An extension to SNA featuring (a) greater distributed network control that avoids critical hierarchical dependencies, thereby isolating the effects of single points of failure; (b) dynamic exchange of network topology information to foster ease of connection, reconfiguration, and adaptive route selection; (c) dynamic definition of network resources; and (d) automated resource registration and directory lookup. APPN extends the LU 6.2 peer orientation for end-user services to network control and supports multiple LU types, including LU 2, LU 3, and LU 6.2.

advanced program-to-program communications (APPC).. An implementation of the SNA/SDLC LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

APPC. Advanced program-to-program communications.

application. A collection of software components that is used to perform specific types of work on a computer. For example, the DCAF program is a software application that is used to provide remote console services.

APPN. Advanced Peer-to-Peer Networking.

Asynchronous Communications Device Interface (ACDI). The programming interface that provides support for those who want to use the serial ports for asynchronous communications in a multitasking environment. ACDI interacts with the serial ports through the base operating system and ensures that interrupts are handled and data is buffered for applications as required.

authentication. (1) A process that is used to verify the integrity of transmitted data, especially a message. (2) In computer security, a process that is used to verify the user of an information system or protected resources. (3) A process that checks the integrity of an entity. (4) See also *password*.

authenticator. See *security authenticator*.

B

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges are connected. (3) In the DCAF, the SNA backbone connects the OS/2 controller

© Copyright IBM Corp. 1990, 1995

workstation with the OS/2 target or DCAF gateway workstations by means of an LU 6.2.

backtab. To move the cursor to the beginning of the previous entry field or the previous selection field. Contrast with *Tab*.

busy. The DCAF session state when the target workstation user is changing session states, and the controller user must wait before attempting to change the session state.

button. (1) A mechanism on a pointing device, such as a mouse, that is used to request or initiate an action. See *mouse button*. (2) A graphical device that identifies a choice. See *radio button* and *push button*. (3) A graphical mechanism in a window that, when selected, results in an action. For example, a list button produces a list of choices. See *list button*, *maximize button*, *minimize button*, and *restore button*.

C

choice. Any item that a user can select.

Close. A choice that removes a window and all its associated windows from the screen.

command. A request for system action.

command area. The area on the panel that contains the command entry field. See also *command entry field*.

command entry field. An entry field in which a user types commands. See also *command area*.

component. In the DCAF program, it is a specialized part of the program that can function independently of the other components. For example, a workstation operating on DOS may have only the target for DOS component installed. The DCAF components include the controller, OS/2 target, DOS target, DCAF gateway, LAN directory, Security Administrator, Security Authenticator, and the Packager.

configuration. (1) (TC97) The arrangement of a computer system or network as defined by the nature, number, and the chief characteristics of its functional units. The term may refer to a hardware or a software configuration. (2) The devices and programs that make up a system, subsystem, or network. (3) In the DCAF program, the arrangement of components and workstations in the network. Also, the collective set of item definitions that describe such a configuration. (4) See *system configuration.*

connection type. When personalizing the asynchronous communications parameters for an OS/2 target, the connection type is represented by a number from 0 to 4. The default, type 3, is for automatic data answering.

controller. In the DCAF, the workstation that can monitor or take over and operate the keyboard and display of another workstation. Contrast with *target workstation*.

CP name. A network-qualified name of a control point (CP), consisting of a network ID qualifier identifying the network (or name space) to which the CP's node belongs, and a unique name within the scope of that network ID identifying the CP. Each APPN or LEN node has one CP name, assigned to it at system-definition time.

D

DCAF. Distributed Console Access Facility.

DCAF gateway workstation. For the DCAF, a LAN-attached workstation that provides communication functions between a controller and a target workstation on a LAN. See also *gateway* and *LAN gateway*.

Disk Operating System (DOS). Software for the PC that controls the execution of programs. Its full name is the IBM Personal Computer Disk Operating System.

display. (1) To present information for viewing, usually on a terminal screen or a hardcopy device. (2) A device or medium on which information is presented, such as a terminal screen.

Distributed Console Access Facility (DCAF). (1) This program product provides a remote console function that allows a user at one programmable workstation to remotely control the keyboard input and monitor the display output of another programmable workstation. The DCAF program does not affect the application programs that are running on the workstation that is being controlled. (2) An icon that represents the Distributed Console Access Facility.

DOS. Disk Operating System.

E

Enter. An action that submits information to the computer for processing. Enter tells the computer to perform actions on whatever has been selected.

enter. To submit all selected choices and entry-field information to the computer for processing; for example, to type information on a keyboard and press the Enter key.

entry. An input operation on a workstation.

entry field. An area in which a user types information. Its boundaries are usually indicated. See also *selection field.*

Exit. An action that ends the active application and removes, from the screen, all windows associated with the application.

F

fast path. A method of doing something more directly and quickly than the regular way. For example, pressing a function key is a faster path than typing a command.

field. An identifiable area on a screen. See *entry field*, *command entry field*, and *selection field*.

G

gateway. A functional unit that connects two computer networks of different network architectures.

Note: A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures.

See also *DCAF gateway workstation* and *LAN gateway*.

gateway workstation. See *DCAF gateway workstation*.

H

Help. A push button that provides information about the item the cursor is on or about the entire window.

hot key combination. A combination of two keys that, when pressed simultaneously for a period of time, can be used to cause a specific action. At the DCAF target workstation, the hot key combination can be used to manipulate the session status. During the installation or packaging of the target component, the hot key can be enabled or disabled and the key combination can be defined. At the controller, the hot key can be used to manipulate the keystroke mode. See also *keystrokes local* and *keystrokes remote*.

I

icon. A graphical representation of an object, consisting of an image, image background, and a label.

inactive window. A window with which a user is not currently interacting. The window cannot receive input from the keyboard or mouse. Contrast with *active window*.

initiate. (1) In SNA, a request sent from a logical unit (LU) to a system services control point (SSCP) requesting that an LU-LU session be established. (2) In the DCAF, a target workstation's request to start a session. The target workstation must send a request to initiate a session to the controller before a session can be established. A target workstation can be initiated by the target workstation user or by an autostart command.

installation. The procedure of personalizing and copying the components of the DCAF product onto the workstations where they will be processed.

K

KEK. The DCAF key-encrypting key encrypts and decrypts all keys that are distributed in the network for the DCAF when this key is configured for secure DCAF sessions.

keystrokes local. A DCAF keystroke mode that occurs on the controller workstation when the keystrokes and mouse commands will be processed at the controller workstation. Contrast with *keystrokes remote*.

keystrokes remote. A DCAF keystroke mode that occurs on the controller workstation when the keystrokes and mouse commands will be transmitted to the target workstation and processed at the target workstation. Contrast with *keystrokes local*.

L

LAA. Locally administered address.

LAN. Local Area Network.

LAN directory. This DCAF component supplies the controller component with the names of the enabled DCAF target workstations, on the NetBIOS LAN, that are registered with the name of this LAN directory. Each NetBIOS LAN with DCAF has a specific DCAF LAN directory name. The name of the LAN directory is used by the DCAF components to make the logical connection between the DCAF components on the LAN.

LAN directory nickname list. For the DCAF, this file contains the list of user-defined nicknames and the associated UAA or LAA for the target workstations on the LAN. See *LAN Target Directory*.

LAN gateway. A functional unit that connects a local area network with another network using different protocols. See also *gateway* and *DCAF gateway workstation*.

LAN target. A DCAF term that is used when referring to a DCAF target workstation that is on a NetBIOS LAN. See *LAN Target Directory*.

LAN Target Directory. A DCAF window that can be displayed on the controller after the user has chosen a DCAF gateway or LAN directory from the DCAF directory. The window displays the LAN adapter addresses or the descriptive names for the target workstations that are registered with the same LAN directory as the chosen DCAF gateway.

link. In SNA, the combination of the link connection and the link stations that join network nodes. A link connection is the physical medium of transmission. A link, however, is both logical and physical.

list button. A button, labeled with a underscored down arrow, that produces a list of valid choices that can be selected for that field. See *button*.

local area network (LAN). (1) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. See also *token ring*. (2) A network in which communications are limited to a moderately sized geographic area such as a single office building, warehouse, or campus, and which do not generally extend across public rights-of-way. Contrast with *wide area network*.

locally administered. A DCAF security authenticator workstation is locally administered when it is installed on the same workstation as the DCAF security administrator component. When locally administered, the security data files can be transferred (locally) from the DCAF security administrator to the DCAF security authenticator without the need for a secure session to transfer the files. Contrast with *remotely administered*.

locally administered address (LAA). In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

local node name. In a network, name of a point, accessed directly without use of a telecommunication line, at which one or more functional units connect channels or data circuits. (I)

M

master key. The master key is used by the CCA services to encrypt and decrypt many data-encrypting keys and key-encrypting keys that are stored in a key data set.

maximize button. A button on the rightmost corner of the title bar of a window that has not been maximized that, when selected, enlarges the window to its largest possible size. See *button*. Contrast with *minimize button*. See also *restore button*.

menu. A list of choices that gives users access to actions that can be applied to an object.

menu bar. The area near the top of a window, below the title bar and above the rest of the window, that contains choices that provide access to other menus.

message. Information not requested by a user but displayed or logged by an application in response to an expected or unexpected event.

minimize button. A button, located next to the rightmost button in a title bar, that, when selected, reduces the window to its smallest possible size. See *button*. Contrast with *maximize button*. See also *restore button*.

mode name. The name used by the initiator of a session to designate the characteristics desired for the session, such as traffic pacing values, message-length limits, sync point and cryptography options, and the class of service within the transport network.

monitoring. In the DCAF program, the session state in which the controller workstation user sees everything on the target workstation display, but the target workstation user controls the keyboard and mouse.

mouse. A device that a user moves on a flat surface to position a pointer on the screen. It allows a user to select a choice or function to be performed or to perform operations on the screen, such as dragging or drawing lines from one position to another.

mouse button. A mechanism on a mouse that a user presses to select choices or initiate actions.

N

NetBIOS. Network Basic Input/Output System. An operating system interface for application programs used on IBM programmable workstations that are attached to the IBM Token-Ring Network.

network. An arrangement of nodes and connecting branches.

network address. (1) An identifier for a node, station, or unit of equipment in a network. (2) In a subarea network, an address, consisting of subarea and element fields, that identifies a link, link station, physical unit, logical unit, or system services control point. Subarea nodes use network addresses; peripheral nodes use local addresses or local-form session identifiers (LFSIDs). The boundary function in the subarea node to which a peripheral node is attached transforms local addresses or LFSIDs to network addresses and vice versa.

node address. In a network, the unique code assigned to the point at which one or more functional units connect channels or data circuits. (I)

O

online. Stored in a computer and accessible from a workstation.

OS/2. An operating system that runs on a personal computer with an 80286 processor or larger (for example, an IBM Personal System/2 model 80).

P

packager. A DCAF component that creates installation packages from of the other DCAF components. These packages can later be installed on workstations. The components can be personalized during the creation of the package. The security authenticator and administrator components cannot be packaged.

panel. A particular arrangement of information that is presented in a window or pop-up. If some of the information is not visible because of the size of the panel, a user can scroll to see the information.

pass phrase. For a secure DCAF environment, each controller user has a pass phrase of 4 to 80 characters. The pass phrase may contain uppercase and lowercase letters, the digits 0 to 9, and the special characters #, @, $, and blanks.

password. A unique string of characters known to a computer system and to a user, who must specify the character string to gain access to a system and to the information stored within it.

password-only session. In the DCAF environment, a password-only session requires the controller user to type the correct password for the target or DCAF gateway workstation before a session is established. A nonsecure session is established when the user presses Enter without typing a password. Both these sessions do not require authentication. Contrast with *secure session*. See *session*.

personalization. Many of the features of the DCAF components are options that can be customized. During installation, the options for the DCAF components can be selected. Some of the options may be selected or changed, or both, after installation.

port number. In TCP/IP, a 16-bit number used to communicate between TCP and a higher-level protocol or application. Some protocols, such as the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP), use the same port number in all TCP/IP implementations.

programmable workstation. A workstation that has some degree of processing capability and that allows a user to change its functions.

Program Manager. An application that is central to the Windows operating system. It starts whenever you start Windows and continues to run as long as you are working with Windows. You can use Program Manager to start other applications and organize applications and files into groups that make sense to you. It is the default shell for Windows.

prompt. A symbol or action that requests an entry or selection from the user.

protocol. (1) (TC97) The set of semantic and syntactic rules governing the operation of functional units of a communication system that must be followed if communication is to be achieved. (2) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. (3) The DCAF program can use NetBIOS, SNA, and switched asynchronous protocols.

pull-down menu. A list of choices extending from a selected menu-bar choice that gives access to actions.

push button. A rectangle with text inside. Push buttons are used in windows for actions that occur immediately when the push button is selected.

R

radio button. A circle with text beside it. Radio buttons are combined to show a user a fixed set of choices from which only one can be selected. The circle is partially filled when a choice is selected.

Refresh. An action that updates the information that is being displayed.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunications line. (2) In Advanced Program-to-Program Communications (APPC), indicates that the partner logical unit (PLU) or transaction program is not at the local node.

remote console function. The function that allows one workstation to control another.

remote host. Any host on a network except the one at which a particular operator is working.

remotely administered. A DCAF security authenticator workstation is remotely administered when it is not installed on the same workstation as the DCAF security administrator component. When remotely administered, the security data files must be transferred via a secure DCAF session. It is necessary that a secure OS/2 target component be installed on the security authenticator workstation. Contrast with *locally administered*.

restore button. A button that appears in the rightmost corner of the title bar after a window has been maximized. When the restore button is selected, the window returns to the size it was before it was maximized. See *button*. See also *maximize button* and *minimize button*.

Restructured Extended Executor (REXX). A programming language. A REXX program can be used to call OS/2 or DOS commands.

REXX. Restructured Extended Executor.

S

screen. The physical surface of a display device upon which information is shown to a user. Contrast with *panel*.

scroll. To move a display image vertically or horizontally to view data that is not otherwise visible in a display screen or window.

search. The process of looking for a particular item.

secure session. In the DCAF environment, a secure session is a DCAF session that has been authenticated by the DCAF security authenticator. Contrast with *password-only session*. See *session*.

security administrator. The DCAF security administrator component centralizes the maintenance of the databases for the controller users, the target access tables, the secure target workstation information, and the security authenticators. This component updates the file EQNADMN.LOG with error and informational messages for the security file transfers.

security authenticator. The DCAF security authenticator verifies and authorizes the secure DCAF sessions between the controller and target components. The file EQNAUTH.LOG is used to log error and informational messages such as authentication requests. See also *locally administered* and *remotely administered*.

select. The process of explicitly identifying one or more objects to which a subsequent action will apply.

selection field. A set of related choices. See also *entry field*.

Send. (1) A choice in the Keystrokes pull-down menu that a user can select to send certain command key sequences to a target workstation. (2) A push button on the DCAF-File Transfer Utility window that causes a file to be sent to a target workstation.

server. On a local area network, a data station that provides facilities to other data stations; for example, a file server, a print server, a mail server, or an authentication server.

session. In the DCAF, the period of communications activity between DCAF components. See *password-only session*, *secure session*, and *session state*.

session state. The status of the DCAF session. The session state can be active, monitoring, busy, or suspended. Whether the controller or target workstations can change the session state depends on their configuration.

shortcut key. A key or combination of keys that a user can press to perform an action that is available from a menu; for example Alt+F4 = Close.

SNA. Systems Network Architecture.

status. The measure of the condition of a session. See *session state*.

suspended. In the DCAF program, the session state in which the controller does not control or monitor the target workstation. The controller does not receive display updates from the target, or in any way control the target workstation. Either the controller or the target workstation user can resume the session.

system configuration. A process that specifies the devices and programs that form a particular data processing system.

T

tab. A typing action that moves the cursor to the beginning of the next entry field or the next selection field if no choice is selected. If the next selection field contains a selected choice, the cursor moves to that choice. Contrast with *backtab*.

target workstation. In the DCAF, the workstation whose keyboard and display will be monitored or taken over by the controller. Contrast with *controller*.

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol. A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

title bar. The area at the top of each window that contains the window title and system-menu icon. When appropriate, it also contains the minimize, maximize, and restore icons.

token ring. A network with a ring topology that passes tokens from one attaching device to another. For example, the IBM Token-Ring Network.

U

UAA. Universally administered address.

universally administered address (UAA). In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

user. Anyone who requires the services of a computing system.

user interface. The actions or items that allow a user to interact with and perform operations on a computer.

Using help. A help choice that gives a user information about how the help function works.

W

wide area network. A network that provides data communication capability in geographic areas larger than those serviced by local area networks. Wide area networks may extend across public rights-of-way. Contrast with *local area network*.

window. An area of the screen with visible boundaries within which information is displayed. A window can be smaller than or the same size as the screen. Windows can appear to overlap on the screen.

workstation. A programmable or nonprogrammable device that allows a user to do work. A workstation allows a user to transmit or receive information from a computer.

workstation definition. The description or profile of a workstation as defined in the DCAF directory on controllers. The definitions provide general and protocol descriptions of any workstation to which the controllers connect.

Index

© Copyright IBM Corp. 1990, 1995

B

C

D

E

I

K

L

O

P

R

S

T

U

V

W

X

Communicating Your Comments to IBM

Distributed Console Access Facility
User's Guide
Version 1.31

Publication No. SH19-4069-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

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

If you prefer to send comments by mail, use the reader's comment form (RCF) at the back of this book. If you wish, you can give the RCF to the local branch office or IBM representative for postage-paid mailing.

If you prefer to send comments by FAX, use this number, which is in Italy:

39+6+596+62845

If you prefer to send comments electronically, use this network ID:

ROMERCF at VNET.IBM.COM

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies

Help us help you!

Distributed Console Access Facility
User's Guide
Version 1.31

Publication No. SH19-4069-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	__	__

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	__	__
Complete	__	__
Easy to find	__	__
Easy to understand	__	__
Well organized	__	__
Applicable to your task	__	__

Specific Comments or Problems:

Please tell us how we can improve this book:

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name

Address

Company or Organization

Phone No.

Help us help you!
SH19-4069-01

Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

PLACE
POSTAGE
STAMP
HERE

End-User Technologies
Rome Networking Software Laboratory
IBM SEMEA S.p.A.
P.le G. Pastore, 6
00144 Rome
Italy

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line

Part Number: 34H0764
Program Number: 5622-212

Printed in Denmark by IBM Danmark A/S

34H0764

SH19-4069-01