OS/390

# LAN Server
# Installation Guide

GC28-1733-03

OS/390

# LAN Server
# Installation Guide

GC28-1733-03

**Note**

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

**Fourth Edition, March 1998**

This is a major revision of, and obsoletes, GC28-1733-02.

This edition applies to Version 2 Release 5 of OS/390 (5647-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

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

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

International Business Machines Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+914+432-9405
FAX (Other Countries):
Your International Access Code +1+914+432-9405

IBMLink (United States customers only): KGNVMC(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet e-mail: mhvrcfs@vnet.ibm.com
World Wide Web: http://www.s390.ibm.com/os390

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

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

# Contents

# Figures

# Tables

# 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 the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

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:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, New York 10594
USA

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
Mail Station P300
522 South Road
Poughkeepsie, NY 12601-5400
USA
Attention: Information Request

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

## Year 2000 Support for LAN Server

LAN Server, an element of OS/390, is certified as a Year 2000–ready operating system by the Information Technology Association of America (ITAA).

## Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

ADSTAR
Advanced Peer-to-Peer Networking
AIX
APPN
BookManager
ESCON
ES/9000
Extended Services
FFST/2
IBM
IBMLink
Micro Channel
Language Environment
Operating System/2
OS/2
OS/390
RACF
RS/6000
SAA
Systems Application Architecture
System/370
S/370
System/390
S/390
Ultimedia
VTAM

The following terms, denoted by a double asterisk (**) in this publication, are trademarks of other companies:

| | |
|---|---|
| Microsoft | Microsoft Corporation |
| Network File System | Sun Microsystems, Inc. |
| NFS | Sun Microsystems, Inc. |
| Sun | Sun Microsystems, Inc. |
| UNIX | X/Open Company Limited |

# About This Book

This book provides information for anyone who installs and sets up OS/390 LAN Server. OS/390 LAN Server allows workstation users to store and share their files on OS/390 systems. It also allows TSO/E administrators to back up and restore data sets to and from a backup server. OS/390 LAN Server is intended for organizations that want to use an OS/390 system as a file sharing system for OS/2 LAN Server networks, a TCP/IP network, or both.

## Who Should Read This Book

The primary audience consists of anyone who installs OS/390 LAN Server.

## What You Should Know before Reading This Book

You should be familiar with concepts and terms used in:

- OS/390* systems
- Local Area Networks (LANs) using file servers
- Transmission Control Protocol/Internet Protocol (TCP/IP) and Network File System** (NFS)
- IBM* Operating System/2* (OS/2)
- IBM OS/2 LAN Server (also referred to as WARP* Server)
- IBM Personal Computer Disk Operating System (DOS)*
- IBM ADSTAR Distributed Storage Manager* (ADSM)
- System/390 Open System Adapter Feature

## How This Book is Organized

This book is divided into the following sections:

- Chapter 1 -“Planning for Installation” describes the details that you should consider before installing OS/390 LAN Server, including both internal and external security.
- Chapter 2 -“Installing Host Code” describes how to install the code on OS/390.
- Chapter 3 -“O/2 LAN Server Front-End Processor Installation” describes how to install the OS/2 LAN Server OS/2 front-end processor.
- Chapter 4 -“NFS Front-End Processor Installation” describes how to install the NFS front-end processor.
- Chapter 5 - “NFS Server Installation Verification” provides a procedure for verifying the installation of the NFS server.
- Chapter 6 - “SNA Configuration Information” provides information about SNA connectivity.
- Two appendices provide information on how to run a CM/2 trace and sample files for SNA.

## Determining if a Publication is Current

As needed, IBM changes its information. For a given book, updates to the hardcopy and associated BookManager softcopy are usually available at the same time. Sometimes, however, the updates to hardcopy and softcopy are available at different times. Here's how to determine if you are looking at the most current copy of a book:

1. At the end of the order number, there is a dash followed by two digits, often called the dash level. A book with a higher dash level is more current than one with a lower dash level. For example, in the book order number GC28-1608-06, the dash level 06 means that the book is more current than previous levels, such as 05 or 04.
2. If a hardcopy book and a softcopy book have the same dash level, it is possible that the softcopy book is more current than the hardcopy book. Check the dates shown in the Summary of Changes. The softcopy book might have a more recently dated Summary of Changes than the hardcopy book.
3. To compare softcopy books, you can check the last two characters of the softcopy filename (also called the book name). The higher the number, the more recent the book. For example, IEA4E802 is more recent than IEA4E801. Also, next to the book titles in the CD-ROM booklet and the readme files, there is a change code (N, E, S, or T) that indicates whether a publication is new or changed, as follows:

   N=new
   E=softcopy enhancement
   S=service change
   T=technical change

# Summary of Changes

## Summary of Changes for GC28-1733-03, Version 2 Release 5

### Changed Information

Diskette labeling Information has been updated for Version 2 Release 5.

This edition includes terminology, maintenance, and editorial changes. Technical changes or additions to the text or illustrations are indicated by a vertical bar (|) in the left margin.

## Summary of Changes for GC28-1733-02 as Updated September, 1997

### New Information

Information supporting OS/2 LAN Server file level permissions has been added.

## Summary of Changes for GC28-1733-01, Version 2 Release 5

### New Information

The following is a list of the new information to be found in this release:

- A section on “Using OS/390 LAN Server with the Open Edition NFS Client” has been added.
- A section on “PCNFS Considerations” has been added.
- A section on “RACF* Control of Administrative Request to OS/390 LAN Server” has been added.
- A section on “Incremental Backup and Restore using LFSBR command” has been added.
- A section on “Backup and Restore using the Open Edition ADSM Client” has been added.
- A section on “Performance Tuning” has been added.

### Changed Information

The chapter on “Installing Host Code” has been updated.

# Chapter 1. Planning for Installation

This section provides the following planning information:

- Performance and administration considerations
- File naming and file writing information
- File access considerations
- Security information
- OS/390 resource accounting
- Incremental backup and restore information
- Overview of OS/390 LAN Server installation

## Performance Considerations

Performance of OS/390 LAN Server depends on a variety of processor and data communication load factors. Examples include:

- Connectivity option used for the OS/2 LAN Server to S/390* connection
- Number and type of file requests
- Load on the S/390 processor

When using OS/390 LAN Server for performance sensitive applications such as multimedia, it may be necessary to use the IBM PS/2 MMC or ESCON adapter cards.

## Compatibility with Prior Releases

- Compatibility between OS/390 LAN Server Release 1 and prior products

  In Release 1, the file extended attributes (EAs) have been relocated to enhance performance. Any files created after this release has been installed will use a new EA format. When a file that has the old EA format is updated, or has its extended attributes updated, it will be converted to the new EA format.

  When files are converted to the new format, the entire file must be rewritten to disk. If you have a lot of large files with extended attributes, it could be worthwhile to backup these files before installing the new version. Once the new version has been installed, these files could be restored to convert them to the new format. This would isolate users from the delay involved when old files are converted to the new format.

  Once Release 1 has been installed, it cannot be removed and replaced by an earlier product without first backing up the PWS data sets using the normal backup/restore procedure. Once the earlier version of the product is installed, these PWS datasets would have to be restored so that the EAs are restored to the old format. Since older versions do not support META or VIDEO data sets, those are not a problem.

  Since this version uses a different format for the EAs, files cannot be shared with other servers running a previous version of OS/390 LAN Server.

- Compatibility between OS/390 LAN Server Release 2 and Release 1

  No new functions were released for Release 2 . Therefore, there are no compatibility issues.

- Compatibility between OS/390 LAN Server Release 3 and Release 2

  For OS/390 Release 3, the LAN Server NFS and SNMP socket implementations were ported to Open Edition sockets. When using either the LAN Server NFS or SNMP features, Open Edition socket calls are issued. Open Edition requires that a Started Procedure must be defined in the OMVS segment before it is allowed to issue any Open Edition Service Calls. Therefore, starting with this release of LAN Server, if either the NFS or SNMP features are used, the LAN Server Started Procedure must be defined in the OMVS segment.

  With OS/390 Release 3, the CONFIG DD statement in the LAN Server Started Procedure is required.

- Compatibility between OS/390 LAN Server Release 4 and Release 3

  EXTENDED LDSs are not compatible with prior releases of OS/390 LAN Server. In the event that you must go back to a prior release, and you need to use the data that is on an EXTENDED LDS, you have two options:

  – COPY the data to a BASE LDS before going back to the prior level.

  – BACKUP the data before going back to the prior level, and then restore it to a BASE LDS later.

  **Note:** In both of these cases, the access control information that was in effect for the EXTENDED LDS is lost. The access controls will now be at the directory tree level, the same as it is for all other BASE LDSs.

- Compatibility between OS/390 LAN Server Release 5 and Release 4

  No new functions were released for Release 5 . Therefore, there are no compatibility issues.

## File Naming Considerations

OS/390 LAN Server supports file systems that have different file naming conventions. This section describes how OS/390 LAN Server handles this diversity in naming conventions.

## Characteristics of OS/2, DOS, and NFS File Names

There are many differences in the naming conventions supported by OS/2 and DOS workstations and NFS clients. These differences fall into three categories:

- Sets of valid file naming characters
- Length of file names
- Extent of support for mixed case file names

The OS/2 High Performance File System (HPFS), the DOS File Allocation Table (FAT) file system, and the NFS address file names are described as follows:

- OS/2 Version 1.2 introduced the High Performance File System (HPFS). Under HPFS, file and directory names may contain 1-255 characters. Subdirectory qualifiers in a path name must be separated from other subdirectories by a \ character. HPFS names can contain any characters except these symbols:

  `" : < > | \ / * ?`

While HPFS allows file names to contain both uppercase and lowercase characters, it ignores the case of the name while searching for files. This means that under HPFS, the file names *Abc* and *aBc* represent the same file.

OS/2 1.2 and later versions support both the HPFS and FAT file systems.

- DOS and pre-Version 1.2 releases of OS/2 use the File Allocation Table (FAT) file system. This file system supports only uppercase file names with a 1-8 character name and a 0-3 character extension, which is separated from the file name by a dot (.) character. This file naming format is sometimes called the 8.3 format. Directory names must also follow this 8.3 format. Directory qualifiers in a path are separated by the back slash (\) character. FAT names can contain any characters except blanks, ASCII characters less than X'20', and these symbols:

  `" < > | \ / * ? . : [ ] + = ; ,`

- NFS supports the largest set of valid file naming characters of the three environments. Basically, all ASCII characters may be used in NFS file names, although the use of certain characters (such as UNIX metacharacters) may cause problems with command interpretation at the workstation. File and directory names may be up to 255 characters long, and qualifiers in a path are separated by the slash (/) character. In addition to using the largest character set of the three environments, NFS also supports *and respects* mixed case names. This means that the file names *Abc* and *aBc* represent two different files to an NFS client.

The differences between naming conventions across the different OS/390 LAN Server workstation environments pose some interesting problems. It is important to be compatible with each environment to achieve the objective of transparency. However, because each environment has different capabilities, a rule that brings compatibility to one environment may actually be a restriction to another.

OS/390 LAN Server's approach to file name support is to be as flexible as possible without violating naming rules of the different environments.

## Handling Different Character Sets

In general, if a workstation user creates a file name with characters that are not allowed under another workstation user's file system, the second workstation user may be able to see the file name when listing the contents of the directory (using the DOS DIR command, for example), but may not be able to access or manipulate the file's contents.

This is most likely to happen when an OS/2 or DOS user attempts to view files created by NFS clients. However, because NFS imposes no rules on character sets, most every file name is valid to NFS clients.

Double-byte character set support is provided for file names and directories on workstation format data sets. Double-byte name support does not change any of the existing rules regarding valid character sets, length of name, or support for mixed class.

In addition to double-byte file names and directories, this support also allows users to specify double-byte characteristics in the *netname* and *os2path* parameters, or in the *exportname* and *nfspath* parameters.

If it is necessary to modify a double-byte conversion table, the user is responsible for the integrity of the data.

## Handling Limited Name Lengths

OS/390 LAN Server supports paths up to 1024 characters long with file or directory names up to 255 characters long.

The HPFS version of OS/2 allows file names to be up to 255 characters long. DOS and early OS/2 releases, on the other hand, are limited to the DOS 8.3 format. When accessing OS/390 LAN Server directories, DOS and pre-1.2 OS/2 requesters see only file names that conform to the 8.3 format. These requesters do not see any file names that are longer than the workstation's file system can handle.

## Handling Different File Name Cases

Different workstations handle file name casing differently. While some workstations fully or partially support mixed case names, others only support uppercase names. In general:

- NFS clients have the widest range of choices in terms of file names because NFS fully supports mixed case names. That is, NFS workstations respect the case of names when creating and retrieving files and directories. To be completely compatible with NFS conventions results in incompatibilities for OS/2 LAN Server users.
- DOS workstations only support uppercase file names. To be completely compatible with DOS clients results in limitations that may seem extreme to NFS clients.
- Users of OS/2 1.2 and later versions have somewhat better choices. While these workstations allow the creation of mixed case file names, the file name case is ignored when retrieving files or directories.
- Double-byte character set (DBCS) file names are supported.

To accommodate the differences between workstations that respect name cases versus those that do not, OS/390 LAN Server provides a FOLD directory format. The specification of FOLD is made on the SET ATTRIB administration command (see *OS/390 LAN Server Configuration Files and Commands* for details).

### FOLD Directories

**This is the only type of directory that OS/2 LAN Server users are allowed to access. Because of this, any data that is to be shared between OS/2 LAN Server and NFS users must be stored on FOLD directories.**

OS/390 LAN Server stores all file and path names in uppercase EBCDIC characters on FOLD directories. When *any OS/390 LAN Server client* attempts to create a file with lowercase letters (a-z) in the file name, OS/390 LAN Server translates those letters to uppercase before saving the file name. Likewise, when a user requests a search for a particular file name, the input path and file name is translated to uppercase before the search is conducted.

When an OS/2 LAN Server requester issues a DIR command against a FOLD directory, all names are displayed in uppercase, exactly as they are stored by OS/390 LAN Server. However, because OS/2 LAN Server requesters expect the case of the file names to be ignored, applications are not affected.

In contrast, when an NFS client issues an **ls** command against a FOLD directory, OS/390 LAN Server translates all of the file and directory names to lowercase before presenting them to the client. This translation is performed so that the *appearance* of OS/390 LAN Server folded directories is more consistent with what most NFS clients are accustomed to seeing. Because most NFS clients expect the case of file names to be respected, it is possible that some applications may produce unexpected results if they attempt to create or manipulate two files of the same name, but different cases (in which case, both file names will resolve to the same file). Additionally, commands that use wildcard characters at the NFS client must be specified with names that only contain lowercase characters. Because wildcard searches are performed by the NFS client (rather than by the server), searches that contain mixed case names will not match the lowercase names that are returned by OS/390 LAN Server. As a general rule, NFS clients should stick to lowercase-only names when accessing FOLD directories.

Different operating systems perform uppercasing differently for characters other than a-z; this includes non-English letters that contain accent marks. For example, one workstation may convert the ÿ character to a Y instead of Ÿ; a different workstation may not recognize ÿ as a letter with an uppercase counterpart and leave it unchanged.

### MIXED Directories (for NFS Clients Only)

OS/390 LAN Server stores file and path names in MIXED directories exactly as they are entered by the client. Because of this, a client may create two different files with the same name, but different cases (for example, 'Abc' and 'aBc'). Likewise, when searching for a file or path name, the case of the names are respected, so the search will only succeed if an exact match is found.

**MIXED directories provide full compatibility for NFS clients** because NFS clients expect name cases to be respected. However, because this type of behavior is incompatible with basic OS/2 file system rules, MIXED directories are not accessible to OS/2 LAN Server requesters. Only NFS clients may access MIXED directories. Because of this, **data that is to be shared between NFS and OS/2 LAN Server users may not reside in a MIXED directory**.

## Assigning File Naming Attributes

File naming attributes (FOLD and MIXED) may be specified at either the data set level or at the first level of subdirectories (subdirectories whose parent is the data set's root directory) on a special type of workstation format data set called an ANY data set.

## Setting Naming Attributes at the Data Set Level

The SET ATTRIB administration command specifies the naming attribute for a workstation format data set after the data set is formatted. The naming attribute can only be changed if no disk operations were performed on the data set since formatting, and in some cases, only when the data set is free of any network resource name definitions. Refer to *OS/390 LAN Server Configuration Files and Commands* for the rules pertaining to setting naming attributes on data sets.

If no naming attribute is explicitly assigned to a data set, the default is FOLD.

Once data sets are set up with naming attributes, you may use the QUERY LFSDSN command to determine the naming attributes of the different data sets that are known to OS/390 LAN Server.

If a data set is specified as having the FOLD attribute, then all data in that data set is stored by that naming attribute. If an installation is using OS/390 LAN Server as a server for only one file serving environment, then this is the method of choice.

Controlling naming attributes at the data set level is straightforward and requires a minimum of administrative overhead. In some cases however, it may be desirable to keep both FOLD and MIXED directories on the same data set. For these cases, the ANY naming attribute is provided.

## Setting Naming Attributes at the Directory Level: ANY Data Sets

If your installations supports both the OS/2 LAN Server and NFS environments, and you restrict naming attributes at the data set level, you may have difficulty allocating disk space. For example, if an installation has 3 GB of space available for storing workstation data and 10 different departments to which this space is to be allocated, the tendency may be to allocate each department its own data set.

If some or all of those departments support both OS/2 LAN Server and NFS users, each may need space on both FOLD and MIXED directories. Determining fair and equitable space allocation may become difficult and even impractical in this type of environment. By segmenting a large data set into several small data sets, you risk limiting some departments to less space than they actually need while other departments may end up with large amounts of unused space.

To avoid this problem, the installation may want to keep one or two large data sets in order to let their users' data expand as needed, and then charge for that space according to usage. ANY data sets facilitate this type of approach.

Data sets with the ANY naming attribute:

- May contain subdirectories with the FOLD naming attribute. These attributes are assigned on first level subdirectories (subdirectories whose parent is the root directory of the data set) when the directories are created with the CREATE DIRECTORY administration command.
- May not contain files in their root directory.
- May not be accessed at the root directory level by any end users. (OS/390 LAN Server will not allow netnames or export names to be defined on the root directory of an ANY data set.)

Similar to the behavior of FOLD and MIXED data sets, the naming attribute of a first level subdirectory on an ANY data set applies to all data contained within that subdirectory. This means that you cannot define a MIXED format subdirectory whose parent is a FOLD directory, nor can you define a FOLD format subdirectory whose parent is a MIXED directory.

Unlike data sets, the naming attribute of a subdirectory cannot be changed with the SET ATTRIB command, even if the subdirectory is empty. To change the naming attribute of a directory on an ANY data set, you must delete the directory through the DELETE DIRECTORY command, and then recreate the directory with the CREATE DIRECTORY command, specifying the desired naming attribute.

## File Writing Considerations

To ensure data integrity when rewriting an existing file, the data and directory is written to new DASD space before the old version is erased. Because of this technique, OS/390 LAN Server requires free DASD space greater that the size of the file being updated.

For example, if you copy a 250K byte file to a dataset on which the file already exists, you need 250K bytes of available DASD space. In addition, you must also have sufficient DASD space to rewrite the file directory. The amount of space that is needed for the directory depends on the number of workstation files in the directory.

## File Access Considerations

With OS/390 LAN Server, workstation users can access workstation format files stored on OS/390 DASD. However, OS/390 host users or applications cannot access these workstation format files. Workstation users cannot access host files, but a TSO/E OS/390 LAN Server administrator can copy data sets between workstation format files and OS/390 sequential files.

## Access to Workstation Format Files

Access to workstation format files depends on the environment in which you are working. OS/390 LAN Server uses different methods to control access depending on the environment.

### Access from an OS/2 LAN Server Environment

OS/2 LAN Server provides access control at the individual file level. This means that a user with access to a directory can access only the files for which the user was granted access.

OS/390 LAN Server permits controlling access to workstation files at the directory tree level if you are accessing a file on a BASE LDS. For files on an EXTENDED LDS, the access is at the file level.

### Access from an NFS Environment

Access to files stored under OS/390 LAN Server by NFS clients is controlled by records in the EXPORTS Configuration File. The EXPORTS Configuration File establishes a list of resources (OS/390 LAN Server directories) that can be mounted by NFS clients along with access restrictions that apply. The EXPORT command allows the administrator to update the exports list after the contents of the EXPORTS Configuration File is modified.

Use the QUERY EXPORT command to display a list of resources defined as exportable for NFS clients.

Once the directory is mounted, UNIX-style access controls apply:

- UNIX-style permissions are supported.
- UNIX permission uid and gid values are saved with the NFS data.
- The UNIX **chown** and **chgrp** commands can be used to modify the owner and group values. The **chmod** command can also be used to change permissions.

**Note:** OS/390 LAN Server does not attempt to administer the uid, gid, or permission values of the data it stores. It is up to the installation to control and manage the use of UNIX access control values as it sees fit.

## Cross-Environment Data Sharing

OS/2 LAN Server requesters and NFS clients can concurrently share workstation format data. This section addresses how OS/390 LAN Server handles data sharing between the different environments.

**Note:** Workstation format data shared between OS/2 LAN Server and NFS environments must be stored on FOLD format directories.

### Locking

OS/2 LAN Server protocols allow users to obtain several different types of explicit locks on files. Among these are *exclusive locks*, which prevent any other user from accessing the file until the lock is released. While the concept of exclusive locks is foreign to NFS protocols, the OS/390 LAN Server NFS server must still lock files internally for the duration of each user request to maintain data integrity. As in any application that uses locks, locking conflicts will occur.

In most cases, locking of files by OS/2 LAN Server users is transparent to NFS users. However, when an OS/2 LAN Server user obtains a lock for a long duration, NFS users may be unable to access the file until the lock is released. This will normally appear to the NFS client as an “access denied” error.

**Note:** The OS/390 LAN Server NFS server does not support the Network Lock Manager protocol (lockd or statd daemons).

### Differences in Data Formats

For text-oriented files (character data, rather than machine executable code), a slight incompatibility exists in the way that OS/2, DOS, and UNIX workstations handle the end-of-line condition. Many OS/2 and DOS applications normally mark the end of each line with a combination of the Carriage Return (CR) and Line Feed (LF) characters (this sequence will be referred to as the CR-LF combination hereafter). Most UNIX applications, on the other hand, use a single LF character. While the UNIX applications normally handle the OS/2-DOS format without a problem, some OS/2 and DOS applications may experience problems because of the missing CR characters in UNIX format files.

Because it is very difficult for a file server to reliably determine which files are text format and which are not, OS/390 LAN Server does not attempt to resolve these differences in data formats on workstation format data sets. Rather, the **unix2os2** and **os22unix** utility programs are supplied so that you can perform transformations as needed.

### File Attributes

A single file or directory may have any combination of OS/2 and NFS attributes. When creating files and directories, both OS/2 LAN Server requesters and NFS clients assign appropriate attributes that pertain to their file serving environments. However, when this data is shared between OS/2 LAN Server and NFS users, some of these files may be assigned attributes from both environments. When a user accesses a file or directory, only the attributes that pertain to the file serving protocol of the request are returned. This means that:

- OS/390 LAN Server will not return any OS/2 attributes (including extended attributes) to an NFS client. This includes OS/2 NFS clients.
- OS/2 LAN Server requesters will never see NFS permission values.

File attributes remain with a file or directory as long as the file or directory is not erased or replaced (or until those attributes are explicitly changed).

For example, if an NFS client appends data to an existing file that contains OS/2 extended attributes, those attributes are not affected. However, if the NFS client replaces that file, the OS/2 attributes are lost. Likewise, if an OS/2 LAN Server requester replaces a file that has NFS permissions, those permissions are lost, and new permissions are assigned as they are for any other newly created file.

Additionally, if a user copies data from an OS/390 LAN Server directory, attributes that are foreign to the read request for the OS/390 LAN Server data are not copied to the newly created file or directory. For example, if an NFS client copies a file that contains OS/2 extended attributes from an OS/390 LAN Server server, the new file will only contain the file data and any NFS permissions from the source file. The extended attributes are not copied. *This includes OS/2 workstations that attempt to copy a file from an OS/390 LAN Server NFS server (through their NFS client) to a data set or server that supports extended attributes*.

Because of the inability of each file serving protocol to handle foreign attributes, be very careful about which files and directories are allowed to be shared in read/write mode between OS/2 LAN Server and NFS users.

## UNIX Links for OS/2 LAN Requesters

OS/390 LAN Server supports UNIX links for OS/2 LAN requesters as follows:

- Hard links appear to OS/2 LAN Server users as “normal” files.
- Symbolic links appear to OS/2 LAN Server users as 0-length files with the following OS/2 attributes:
  - Hidden
  - System
  - Read-only

## Cross-Environment Access Controls

There is a difference between the methods that OS/2 LAN Server and NFS user workstations use to provide access controls to data. Because of this, and because an objective of OS/390 LAN Server is to provide true workstation services natively on OS/390, differences also exist in the way OS/390 LAN Server provides access controls between the environments.

***Controlling Initial Access:*** Initial permissions for a given user to access a given directory are determined by:

- The NET USE command for OS/2 and DOS LAN requesters. Using the OLSACCS command, the OS/390 LAN Server administrator must tell OS/390 LAN Server that user X is allowed to enter a NET USE command for directory Y. For more information, refer to *OS/390 LAN Server Configuration Files and Commands*.
- The **mount** command for NFS clients. For more information, refer to *OS/390 LAN Server Configuration Files and Commands*.

The OS/390 LAN Server administrator uses the EXPORTS Configuration File to define which file systems are exported to which NFS clients, and the type of access for each client. For more information, refer to *OS/390 LAN Server Configuration Files and Commands*.

After a workstation user gains access to a given directory on an OS/390 LAN Server DASD, cross environment access controls are as follows:

***Creation of Data, Inheritance of Attributes:*** When files and directories are created on a workstation format data set, OS/390 LAN Server saves all attribute information supplied by the requester or client. However, when data is shared across environments, some attributes must be either inherited from the parent directory, or simply assumed if the needed parental attributes do not exist.

- When an OS/2 LAN Server requester creates a new file or directory, the UNIX permission values, owner uid, and group gid are inherited from the parent directory. If no such values exist, then they are set to zeros. OS/390 LAN Server uses default values when an NFS client accesses that file or directory, as described under "NFS Clients Reading OS/2 LAN Server-Created Data." The OS/390 LAN Server administrator can define UNIX permission values for a given directory (regardless of who created it) through the use of the SET ATTRIB administration command. For more information, refer to *OS/390 LAN Server Configuration Files and Commands*.
- When an NFS client creates a new file or directory, *no OS/2 attributes are saved*, as there are no OS/2 attributes for which such inheritance makes sense.

***NFS Clients Reading OS/2 LAN Server-Created Data:*** A file or directory created by an OS/2 LAN Server user may contain UNIX permission values. If these values are present, they will be used to control NFS user access to the file or directory. If this information does not exist, a dummy group ID (65535), owner uid (65535), and permission bits will be returned to the client. (OS/390 LAN Server considers NFS attributes to be nonexistent when the owner *uid* value is set to zero.) The client will be treated as a "public" user in terms of the returned permission bits. The default permission bits are set to:

- ------rwx if the OS/2 read-only attribute is *not* set for the file or directory, or
- ------r-x if the OS/2 read-only attribute *is* set

For example, suppose an NFS user issues a Unix-type **ls** command against an OS/2 LAN Server-created directory mounted as my/dir1. This directory contains one subdirectory and four files:

- No UNIX permission values exist for the my/dir1 directory.
- Two of the files, *some.goodies* and *notebooks*, contain UNIX permission values that were created by the OS/390 LAN Server administrator or by an NFS client.
- The remaining two files, (*whatta.great.file* and *read.fil*) and the directory *dir2*, do not have any UNIX permission values, but *read.fil* was assigned the OS/2 read-only attribute.
- The NFS user has read/write access to *my/dir1* as a result of the mount command used to access the directory.

Figure 1 on page 11 shows what the Unix-type **ls** command would display:

```
$ ls -l my/dir1

Permission  Links  Owner  Group   Size      Modified    Filename
----------  -----  -----  -----  -------  ------------  -----------------
D------rwx      2  65535  65535     8646  Aug  2 13:26  .
drwxrwxrwx      4    kjm  desgn     7546  Jul 31 16:37  ..
D------rwx      3  65535  65535       44  Jun 19 16:49  dir2
F------rwx      1  65535  65535     4399  May  3 09:17  whatta.great.file
Frwxr-x---      1    457     72    12512  May  8 10:03  some.goodies
F------r-x      1  65535  65535      832  Dec 21 17:22  read.fil
Frw-r--r--      1   1188    129     7364  Feb  7 19:01  notebooks
```

*Figure 1. Sample ls Command Output*

AIX* and UNIX users may find it convenient to define a user and group named "OLS" on their workstations. The OLS user uid and OLS group gid should both be defined as 65535. With these names defined, an **ls** command such as that in Figure 1 would show "OLS" in place of each 65535.

***OS/2 LAN Server Requesters Reading NFS-Created Data:*** OS/2 LAN Server users are not subject to any of the UNIX permissions because file-level permissions conflict with OS/390 LAN Server OS/2 LAN Server access controls. If an OS/2 LAN Server user is allowed access to a directory, then access to the entire contents of that directory is implied.

## Security Considerations

OS/390 LAN Server provides security through several different mechanisms:

- Authorization for OS/2 LAN Server front-end processors to connect to OS/390 LAN Server on the OS/390 system
- Authorization for OS/2 LAN Server front-end processors to access OS/390 LAN Server resources on the OS/390 system
- NFS front-end processors can connect only through a physical channel, so the physical connection provides security.
- Authorization of OS/390 LAN Server administrators
- User authentication of NFS clients using the host name from the Domain Name Server or the TCP/IP HOSTS file. In the OS/2 LAN Server environment, OS/390 LAN Server relies on the OS/2 LAN Server for its own user authentication.
- Authorization of individual users or groups of users to access a particular directory tree for both environments

OS/390 LAN Server allows an administrator to set up controls in several ways. By maintaining access for the OS/2 LAN Server and NFS environments, permissions for linear data sets and directories can be maintained according to the needs of the installation.

- OS/390 LAN Server maintains its own access control lists for the OS/2 LAN Server environment. These controls can be set for front-end processors, users, and groups of users.

- For the NFS environment, the EXPORTS Configuration File determines which file systems can be exported to which NFS clients and the type of access for each client. For external security, the external security manager will be checked, in addition to the EXPORTS Configuration File.

## Authentication and Access for OS/2 LAN Server Front-End Processors

In a typical installation, an administrator may set access controls so that each front-end processor can access specific linear data sets on the OS/390 system. The linear data sets may be accessible by only a single front-end processor or shared by many front-end processors. The administrator may keep these data sets completely separate, or place some of them where they can be accessed by more than one front-end processor, or even by NFS users.

When a front-end processor tries to connect to OS/390 LAN Server, its identity is checked against a list of authorized front-end processors. If the front-end processor is not authorized, it is denied a connection. If the front-end processor is authorized, a connection is established, and OS/390 LAN Server informs the front-end processor which resources it may share with its users.

## Authentication and Access for NFS Front-End Processors

For some ways of physically connecting front-end processors to OS/390 systems, such as a CLAW connection, front-end processors are *trusted* because the physical connection is believed to be secure. An S/390* channel attachment is this type of connection. This is true for all NFS front-end processors. An example of such a connection is using a System/370* channel attachment.

For these connections, the front-end processors must be kept in a physically secure location. This location prevents unauthorized persons from physically using the front-end processors. The cabling system makes it very difficult for someone to attach an unauthorized front-end processor to the trusted physical connection. Individual workstations on the LAN need not be in physically secure locations.

## Authorization of OS/390 LAN Server Administrators

OS/390 LAN Server maintains a list of authorized VTAM* application IDs that are allowed to connect to the server to perform administration commands. The AUTHORIZ configuration record and the AUTHORIZ command help define this list. Administrators added to the AUTHORIZ list have access to linear datasets, even if profiles are defined preventing this access.

Through parameters on the LFSCMD or LFSBR command, TSO/E users can specify the VTAM application ID and application ID PASSWORD, if required, used to communicate with OS/390 LAN Server. However, it is the responsibility of each installation to ensure the appropriate security is in place to control which TSO/E users are allowed to use a particular VTAM application ID.

If a TSO/E user is allowed to use a VTAM application ID, the LFSCMD or LFSBR command can be used to establish communications with OS/390 LAN Server using this application name. By checking the authorized list, OS/390 LAN Server verifies that the application name used by the TSO/E administrator is a name authorized to connect to the server. If the application name is not authorized, the OS/390 LAN Server server ends communications, and therefore, does not allow administration commands to be processed.

## Using OS/390 LAN Server with the Open Edition NFS Client

The following conditions are required to enable using OS/390 LAN Server with the Open Edition NFS Client:

- Open Edition must have a Hierarchical File System (HFS).
- The Open Edition NFS client must be up and running.
- TCP/IP must be up and running.
- The USER ID that will be used for the *mount* and *unmount* commands must be defined as a Super User to Open Edition.
- The OS/390 LAN Server started procedure must be RACF defined and be in the OMVS segment.

With the above conditions in place, Open Edition applications can access OS/390 LAN Server data using NFS protocols.

The following steps are required to mount an OS/390 LAN Server exported resource under HFS:

- Define the OS/390 LAN Server exported resource to the Exports member of SBFSCNFG.
- Define a mountpoint in the Open Edition Shell.
- Mount the exported resource under HFS.

**Note:** There is no mount command in the Open Edition Shell utility. The mount must be issued using TSO (ISPF option 6).

The following is an example of the mount command:

```
mount filesystem(lfslx) type(nfs) mode(rdwr) mountpoint('/u/lfslx')
parm('s3172e:gbla,xlat(y)')
```

where

- filesystem
  - lfslx - is any arbitrary name, but it must be unique within HFS. It is recommended that it be the same as the Open Edition mountpoint.
- mountpoint
  - /u/lfslx - is the empty directory in the Open Edition Shell, to be used as the mountpoint for the remote file system.
- parm
  - s3172e - is the LFS NFS server (IP address for the TCP/IP hostname).
  - gbla - is the exported dataset from LAN Server (note there is no '/').
  - xlat(y) - is data translation between ASCII and EBCDIC. LFS(CFR) and AIX filesystems are ASCII, while OS/390 Open Edition is EBCDIC.

To unmount the LAN Server resource, issue the following command:

```
unmount filesystem(lfslx) immediate
```

## Access Controls for NFS LAN End Users

An administrator can also set access controls for end users and for groups of users. For example, LAN users in a particular group might be the only users permitted to access certain data sets.

OS/390 LAN Server provides three types of user-access controls:

- LOCAL, which is provided through the OLSACCS command and the EXPORTS Configuration File
- EXTERNAL without PCNFS, which uses an external security manager such as RACF
- EXTERNAL with PCNFS, which uses an external security manager such as RACF, plus the PCNFS Authentication Protocol

### LOCAL and EXTERNAL Security for Export Names

For the NFS environment, permission to mount a given file system is granted based on the export list, set up by the administrator in the EXPORTS Configuration File. Once a file system is mounted, OS/390 LAN Server supports UNIX-style permissions as maintained by the client workstations. These permissions can be controlled by either workstation users, or by the OS/390 LAN Server administrator, or even by NFS users.

The OS/390 LAN Server file server supports three types of security for controlling user access to given export names:

- LOCAL, which is provided through the exports list in EXPORTS Configuration File to control user access at mount time. In this case, no external security manager is consulted.
- EXTERNAL without PCNFS, which uses the external security manager through the RACROUTE macro. The NFS client's TCP/IP host name and the fully qualified path name are used to determine whether the appropriate access authorities exist.
- EXTERNAL with PCNFS, which uses the PCNFS Authentication Protocol. In this case, when an NFS client issues a mount, the NFS client is prompted for a USER ID and a PASSWORD. The USER ID and PASSWORD are verified by an external security manager through the RACROUTE macro. If the client's USER ID and PASSWORD are valid, a second RACROUTE macro is issued using the NFS client's TCP/IP host name and the fully qualified path name to determine whether the appropriate access authorities exist.

Once a client is allowed to mount a file system, UNIX style permissions are enforced on all files and directories below the mount point.

### LOCAL Access Control for NFS

Since LOCAL security implies standard UNIX style export list processing, users are referred to the AIX or UNIX documentation for a complete description.

**Note:** There is no support for PCNFS authentication (OS/390 LAN Server/ESA does not provide a PCNFS daemon).

## EXTERNAL Access Control Using External Security Managers for NFS Access

If you want to use an external security manager for resource access control by specifying SECURITY EXTERNAL in the NFSLFS Configuration File, then the *-access, -ro,* or *-rw* entry in the EXPORTS Configuration File is ignored. Instead, the appropriate external security manager commands must be used to define resources and the NFS client access controls. However, the export list is still used to map *exportnames* to fully qualified path names and to define the anonymous user ID values for the file system.

If SECURITY EXTERNAL is specified in the NFSLFS Configuration File, then, during startup processing, the OS/390 file server verifies that the external security manager is available and that the OS/390 file server resource class, LFSCLASS, was defined and activated. This is done by passing the TCP/IP host name to the RACROUTE macro.

If the external security manager is not available, or if the OS/390 file server resource class was not defined and activated, an error message is issued and OS/390 file server startup processing ends.

If the external security is available and the OS/390 file server resource class is defined, then the OS/390 file server uses the RACROUTE facility to route access control requests to the external security manager. As a result, if you use an external security manager for resource access control, there are certain restrictions made by the RACROUTE facility that must be considered:

- The OS/390 file server uses VSAM linear data sets to emulate a workstation file system, complete with hierarchical directories and long file names. This means that a single VSAM data set can contain a directory hierarchy and many workstation files in each directory.
- In order for NFS users to connect to various points in the directory hierarchy, the OS/390 file server maps symbolic (export) names to specific directories through the export list entries in the EXPORTS Configuration File.
- The points in the directory are specified using a combination NFSLFS Configuration File of the VSAM data set name, and, optionally, a directory path in the form:

  ```
  dsname:/path.../directory
  ```

  This is the notation used by the OS/390 file server to represent a file sharing resource.
- NFS clients request access to the OS/390 LAN Server NFS server file sharing resource by issuing a *mount* command and specifying the export name that they want to access.
- When the NFS server receives the mount request, it maps the export name to the file sharing resource name, and determines whether or not the NFS client is allowed to access the file sharing resource.

If SECURITY EXTERNAL is not specified in the NFSLFS Configuration File, the OS/390 file server performs access control checking based on the *-access, -ro,* or *-rw* entries in the export list.

If SECURITY EXTERNAL is specified in the NFSLFS Configuration File and PCNFS OFF is specified in the CONFIG Configuration File, the OS/390 file server

uses the following information to build a RACROUTE AUTHOR request to send to the external security manager:

- The first eight characters of the NFS client's TCP/IP host name, left justified, and either truncated or padded with blanks on the right, if necessary
- The OS/390 file sharing resource name, up to 246 characters, to which the requested export name maps

If SECURITY EXTERNAL is specified in the NFSLFS Configuration File and PCNFS ON or PCNFS LIST is specified in the CONFIG Configuration File, the OS/390 file server uses the following information to build a RACROUTE VERIFY request to send to the external security manager:

- The eight characters of the USER ID, left justified, and either truncated or padded with blanks on the right, if necessary
- The eight characters of the NFS client's password, left justified, and either truncated or padded with blanks on the right, if necessary

If the RACROUTE VERIFY request is verified as correct, the OS/390 file server uses the following information to build a RACROUTE AUTHOR request to send to the external security manager:

- The first eight characters of the NFS client's TCP/IP host name, left justified, and either truncated or padded with blanks on the right, if necessary
- The OS/390 file sharing resource name, up to 246 characters, to which the requested export name maps

**Note:** If the external security manager is not available to perform access control checking at the time an NFS client attempts to access the OS/390 file server resource, a “Network Access Denied” message displays.

This method of access control has the following implications:

- External security manager access controls are based on client identifiers of up to eight characters, so only the first eight characters of the host name, or up to the first period (whichever is shorter), are used by the external security manager. Those first eight characters for two different NFS client host names can be identical, as in the case of WILLIAMTHOMAS and WILLIAMTAYLOR, and both of those users are resolved to WILLIAMT by the external security manager.
- Since external security manager names are limited to 246 characters, all file sharing resources cannot exceed 246 characters in length. If SECURITY EXTERNAL is specified in NFSLFS Configuration File, then any export list entries in EXPORTS Configuration File or EXPORT commands specifying longer file sharing resource names will display an error message that the resource name is too long. For EXPORT administrator requests, the command ends with no action.
- The characters used to specify an OS/390 file sharing resource must follow the VSAM data set naming conventions, NFS file/directory naming conventions, and RACROUTE resource class naming conventions, appropriately.

Before the OS/390 file server can use the external security manager for access control checking, the system administrator must:

- Define a new resource class named LFSCLASS, using the ICHERCDE macro defined with:

  - The maximum class name length of MAXLNTH=246
  - The minimum character restrictions of OTHER=ANY
  - A unique ID number of ID=nnn
- Use SETROPTS to activate LFSCLASS: SETROPTS CLASSACT(LFSCLASS)
- Define resource profile names to protect the OS/390 file sharing resources; that is, the appropriate external security manager commands must be issued to create groups, identify the file sharing resource names, and define the user/group access permissions to the file sharing resources.

## PCNFS Considerations

PCNFS is a protocol used to authenticate PC users to an NFS server. With PCNFS, an NFS client must provide a user ID and password when issuing a MOUNT command. This password scheme allows auditing of user activity based on user ID and provides some level of data security on the server.

The authentication capabilities of PCNFS, therefore, enable you to monitor system resources more effectively and increases the choices for access control.

PCNFS has the same security concerns as other network functions that are built on Remote Procedure Calls. For password checking, the encryption employed is trivial. This checking is intended to deter only those users who are casually scanning network traffic. Therefore, it is recommended that you define an alternate USER ID and PASSWORD that is only used for accessing file sharing resources. Then you will need to PERMIT that USER ID to the LFSCLASS. The NFSLFS Configuration File is not dynamically updatable. To add records, you must stop OS/390 LAN Server. If you are going to add users, you might consider creating additional records with IP addresses that are not currently being used so that they are available when the users need to be added.

If you decide to use PCNFS authentication, you **must** specify NFS ON, and either PCNFS ON or PCNFS LIST, in the CONFIG Configuration File.

Specify PCNFS LIST if you have clients running on systems that do not support the PCNFS Authentication Protocol. A NOPCNFSAUTH record must be specified in the NFSLFS Configuration File for each of these clients. Authentication of these clients will be done using the External method without PCNFS, i.e., the client's TCP/IP host will be passed the RACROUTE macro.

Some login protocols recognize a set of *trusted* clients, allowing these clients to access resources without requiring password verification. This *trusted* concept does not apply to PCNFS authentication. If a client (trusted or non-trusted) is running on a system that supports PCNFS Authentication Protocol, they **must** supply a USER ID and PASSWORD. Conversely, clients (trusted or non-trusted) running on systems that do not support the PCNFS Authentication Protocol, do not have to supply a USER ID and PASSWORD. **However**, as noted above, a NOPCNFSAUTH record **must** be specified for these clients.

## Access Controls for OS/2 LAN Server End Users

The access controls for OS/2 LAN Server end users are as follows:

- Local access control using the ACCESS command
- Local access control using OLSACCS
- External access control using an external security manager

The following topics give a brief overview of the access controls for OS/2 LAN Server end users. For more detailed information, see *OS/390 LAN Server Guide*.

### Local Access Control using the ACCESS Command

For EXTENDED LDSs, OS/390 LAN Server provides local access control through the ACCESS command. The default for EXTENDED LDSs is no access. The OS/390 LAN Server Administrator uses the ACCESS command to set OS/2 LAN Server permissions against host directories, subdirectories, and files. For more information on the ACCESS command, see *OS/390 LAN Server Configuration Files and Commands*.

### LOCAL Access Control Using OLSACCS

For BASE LDSs, OS/390 LAN Server provides local access control through the OLSACCS and related administration command. This support does not require an external security manager application, and allows authorized administrators to:

- Define the OS/390 LAN Server resources for which access can be controlled
- Create groups of LAN users
- Define which LAN users and groups have access to certain OS/390 LAN Server resources

If you attempt to enter local access control commands with RACF or another external security manager, you will receive an error message stating that the commands cannot be used. For more information on the OLSACCS commands, see *OS/390 LAN Server Configuration Files and Commands*.

### EXTERNAL Access Control Using an External Security Manager

External security managers (ESMs), such as RACF, can also be used to control user access to OS/390 LAN Server. If your installation wants to use an external security manager for resource access control, you must specify SECURITY EXTERNAL in the OS2LFS Configuration File, or specify the EXTERNAL keyword on the SHARE statement in the OS2LFS Configuration File to override the SECURITY LOCAL.

When external security is specified, the OS/390 LAN Server server verifies during startup processing that the external security manager is available and that the OS/390 LAN Server resource class, LFSCLASS, was defined and activated. This is accomplished by using the RACROUTE interface to enter the following request:

```
RACROUTE REQUEST=STAT,CLASS=LFSCLASS
```

If the external security manager is unavailable, or if the OS/390 LAN Server server resource class was not defined and activated, then an error message is issued and OS/390 LAN Server startup processing ends.

When using an external security manager such as RACF, there are some limitations; for example:

- User IDs must be eight characters or less.
- User IDs must be unique over the LAN.
- User PASSWORDS must be eight characters or less.
- Resource (directory path) names must be less than 246 characters.
- Character set limitations may apply.

A typical resource name that OS/390 LAN Server gives to an External Security Manager contains two parts: a data set name and a workstation directory name, with a colon between the names. The workstation directory contains a backslash before every directory name. Since a maximum of only 246 characters are supported, this name may be truncated. When using local OS/390 LAN Server security, the name is not truncated.

A sample resource name is:

*samp.dsname:\dir1\dirsub*

If you are using RACF, you need to use *generic profile processing* for LFSCLASS which lets you have profiles containing asterisks (*) that act as wildcards. To do this, enter this RACF command from TSO/E:

```
setropts generic(lfsclass) refresh
```

Then you need to define profiles to protect the OS/390 LAN Server data. The entity name passed by OS/390 LAN Server using the RACROUTE interface is of the form:

```
mvs.dataset.name:\dir1\subdir
```

Depending on the capabilities of your External Security Manager, you may not be able to define a profile using the PC backslashes or other high performance file system (HPFS) characters. In this case, you can only define a generic profile that protects at the *data set level*, such as:

```
rdefine lfsclass (mvs.dataset.name:*) uacc(none)
```

Next, you need to permit user IDs to that class; for example:

```
PERMIT mvs.dataset.name:* ACCESS(READ) ID(ARNIE) CLASS(LFSCLASS)
```

**Note:** For each LAN user ID that you are adding, you need a TSO/E user ID of the same name, something RACF can check, either a user ID or a started task.

RACF access options of ALTER, UPDATE, and CONTROL, all map back to LAN access of WRITE.

In Table 1 on page 20 and Table 2 on page 20, differences between external and local security are shown.

| *Table 1. External Versus Local Security Characteristics for OS/2 LAN Server* | |
|---|---|
| **External Security** | **Local Security** |
| Up to 8-character user ID | Up to 20-character user ID |
| All LAN user IDs must be unique | *user ID.FEP* must be unique |
| Up to 246-character profile names | Up to 1200-character profile names |
| May not handle all HPFS characters in profile | Handles all HPFS characters |
| Defining profiles is the same as current host protection. | Profiles are defined using OS/390 LAN Server notation. |

| *Table 2. External Versus Local Security Characteristics for NFS* | |
|---|---|
| **External Security** | **Local Security** |
| First 8 characters of fully-qualified TCP/IP host name | Fully-qualified TCP/IP host name |
| First 8 characters of TCP/IP host names must be unique | TCP/IP host names must be unique |
| With PCNFS active, the eight character or less USER ID | N/A |
| With PCNFS active, the eight character or less PASSWORD | N/A |
| Up to 246-character profile names | Up to 1200-character profile names |
| May not handle all valid UNIX naming characters | Handles all UNIX naming characters |
| Defining profiles is the same as current host protection. | Profiles are defined using OS/390 LAN Server notation. |

## RACF Control of Administrative Request to OS/390 LAN Server

Previously, OS/390 LAN Server allowed the customer to control the TSO/E users who could issue LFSCMD subcommands using the OS/390 LAN Server subcommand and configuration record AUTHORIZ. When a user had permission to issue a subcommand, they could issue any OS/390 LAN Server subcommand. The new support allows the customer to control which user can issue which LFSCMD subcommand from either TSO/E or through the administrative command API. This support is provided using the OS/390 Security Server RACF element, or an equivalent non IBM product. To provide this control, the customer must do the following:

- Activate the RACF class LFSCLASS.
  - It is also recommended that generic classes be turned on using the SETROPTS command as follows:

    ```
    SETROPTS CLASSACT(LFSCLASS) GENERIC(LFSCLASS)
    ```

- Define the appropriate RACF profiles in the LFSCLASS; these profiles have the form of:

  ```
  IBMLSCMD.ADMIN.subcommand_name.OS/390 LAN Server_procname
  ```

  where:
  - IBMLSCMD.ADMIN is fixed.

  - subcommand_name is the first word of the LFSCMD subcommand that is to be protected. For example:
    - **ERASE** or **LIST**, **LFSBR** if the OS/390 LAN Server command **LFSBR** is to be protected.
    - **SET** if the OS/390 LAN Server command **SET ATTRIB** is to be protected.
    - **QUERY** if the OS/390 LAN Server command **QUERY** is to be protected.
  - OS/390 LAN Server_procname is the name of the procedure which starts OS/390 LAN Server.
- Permit the appropriate users or groups to the RACF profile with access of at least **READ**.
- Specify SECURITY EXTERNAL in the CONFIG Configuration File.

**Implementation note**

When OS/390 LAN Server receives an administrative request, it issues a RACROUTE AUTH for the user who originated the request. The entity to be checked will be constructed by concatenating the fixed string IBMLSCMD.ADMIN to the first word of the administrative request. Next, the dot "procname" will be concatenated to the existing string. The authority requested will be **READ**.

If the RACF class LFSCLASS is inactive and SECURITY is LOCAL, then anyone who had been granted access by the OS/390 LAN Server LFSCMD subcommand or configuration record **AUTHORIZ** will have access to all administrative requests. The procedure name which starts OS/390 LAN Server is part of the profile to allow the customer to provide a different level of security for each instance of OS/390 LAN Server on a processor, within a sysplex, or within a complex of RACF Remote Sharing Facility nodes. If this capability is not required by the customer and LFSCLASS supports generic profiles, then this type of profile should be created. An example of the RACF commands to create the generic profiles to allow any RACF id to issue the OS/390 LAN Server LFSCMD subcommand **LIST**, and to restrict all other subcommands is:

```
RDEFINE LFSCLASS IBMLSCMD.ADMIN.** UACC(NONE)
RDEFINE LFSCLASS IBMLSCMD.ADMIN.LIST.** UACC(READ)
```

The standard RACF rules are used to determine which RACF profile determines access. In addition to the standard RACF rules for determining access, the standard rules for logging request will be used. See *RACF Auditor's Guide SC23-3727* for details.

This support does not replace the existing OS/390 LAN Server AUTHORIZ support. It provides additional granularity to the support provided by AUTHORIZ. The current OS/390 LAN Server AUTHORIZ name support determines who can connect to LAN Server to issue commands. This support provides a way of controlling which commands can be issued after the connection has been made. Therefore, a user ID must be in both the AUTHORIZ name list and the appropriate RACF group which is authorized to the appropriate RACF profiles.

For more information on defining and activating RACF groups, refer to the RACF Command Language Reference manual. In particular, see the following commands:

- ADDGROUP

- CONNECT
- SETROPTS

**Note:** A single RACF profile can be created to grant all members of the group that can correspond to the AUTHORIZ list, the authority to issue all commands.

The following is an example of the necessary RACF commands to create the profiles and groups so that ids on the current AUTHORIZ list can issue all the commands.

```
profile created by RDEFINE   LFSCLASS IBMLSCMD.ADMIN.** UACC(NONE)
add group          ADDGROUP  LFSADM
grant access       PERMIT    IBMLSCMD.ADMIN.** ACCESS(READ) CLASS(LFSCLASS)
add ids to group   CONNECT   user ID GROUP(LFSADM)
until all members of the
authorize list have been added
```

When using an External Security Manager, all LAN Server Administrative commands issued from the console will be allowed. If protection of all commands or specific commands is needed, one of the following may be used:

1. Use the MVSCONS command to prevent all LAN Server commands from being issued from the console. It is suggested that MVSCONS STOPONLY be specified to allow LAN Server to be stopped normally from the console.
2. Specify LOGON REQUIRED in PARMLIB. This forces the console to be logged on before any commands can be issued from it. LAN Server Administrative commands will be allowed if the user ID logged onto the console has authority to issue them.
3. Specify LOGON AUTO and a console name (NAME parameter) in PARMLIB, and define a user ID which is the same as this console name. When the system IPLs, this user ID is automatically logged onto the console. LAN Server Administrative commands will be allowed if the user ID logged onto the console has authority to issue them. This user ID cannot be logged off, but another user ID can be logged on over top of it. This approach may be used when it is necessary to use an id which has greater or lesser authority.

## LFSCLASS versus SECURITY

The following table describes what will occur for each combination of LFSCLASS being active or inactive, and SECURITY being LOCAL or EXTERNAL:

| | **SECURITY LOCAL** | **SECURITY EXTERNAL** |
|---|---|---|
| LFSCLASS active | The External Security Manager is used to verify authority for commands. | The External Security Manager is used to verify authority for commands. |
| LFSCLASS inactive | Local access controls (AUTHORIZ list) are used to verify access to commands. | Error message BFSMMA0100I is issued, and the LAN Server procedure ends. (See NOTE below.) |

**Note:** If OS/390 LAN Server is already up and running with SECURITY EXTERNAL and LFSCLASS active, and someone then makes LFSCLASS

inactive, the SECURITY is treated as LOCAL. No error messages are issued.

## OS/390 Resource Accounting

The OS/390 LAN Server server writes accounting records to keep track of LAN user access to OS/390 LAN Server resources. The OS/390 LAN Server server creates accounting records for events such as logging on and logging off, and writes the records to a standard OS/390 System Management Facilities (SMF) data set.

## Incremental Backup and Restore using the LFSBR Command

OS/390 LAN Server provides a built-in ADSM client that uses WDSF protocols for backing up and restoring OS/390 LAN Server data. Incremental backups and restores for OS/390 LAN Server are done by the OS/390 LAN Server administrator. Workstation users need not be concerned with backing up or restoring OS/390 LAN Server data.

The incremental backup function assists in protecting OS/390 LAN Server data sets by storing a copy of the data set on the Backup server. The restore function allows the OS/390 LAN Server administrator to recall files from the Backup server and replace them on OS/390 LAN Server. Front-end processors need not be operational for the OS/390 LAN Server administrator to back up or restore data sets.

The LFSBR...INCREMENTAL backup request can be used to:

- Incrementally back up OS/390 LAN Server data sets to the Backup server
- Back up workstation format files
- Specify a directory path for the incremental backup of workstation formatted data sets

**Note:** The incremental backup and restore functions of OS/390 LAN Server use the FORMATDS label of each VSAM linear data set (LDS) defined to the OS/390 LAN Server server as part of the volume label when backing up or restoring the data set to the OS/390 LAN Server backup server. Therefore, it is highly recommended that you use a unique label for each VSAM LDS, regardless of whether the data set will be used as a FOLD, MIXED, or ANY data set. This avoids the chance that two or more data sets will be backed up to (or restored from) the same filespace within the backup server.

The first time LFSBR...INCREMENTAL backup is requested for an OS/390 LAN Server data set, the entire OS/390 LAN Server data set will be backed up. After the first incremental backup request has been completed, an LFSBR...INCREMENTAL request will back up only new files and files that have changed since the last incremental backup.

The LFSBR...RESTORE request can be used to:

- Restore an entire OS/390 LAN Server data set that has been backed up to the Backup server

- Restore specific subdirectories or files that have been backed up to the Backup server
- Restore single or multiple files with similar file names (using wildcard characters)
- Restore files to a different data set or subdirectory than the one from which they were backed up
- Restore multiple inactive versions of files that have been backed up to the Backup server

For specific information about using the LFSBR command, see *OS/390 LAN Server Configuration Files and Commands*.

## Backup and Restore using the Open Edition ADSM Client

The built-in ADSM client that OS/390 LAN Server provides for backing up and restoring OS/390 LAN Server data supports only a limited subset of the functions available with a full ADSM client. Therefore, OS/390 LAN Server also supports Backup/Restore using the Open Edition ADSM client. Some of the functions that are available on the Open Edition ADSM client, but not on the built-in ADSM client, are as follows:

- Selective backup of individual files
- Timed backup of files
- The ability to select from which backup copy you want to restore

Using this method, all backup/restore commands are issued from the Open Edition ADSM Client. The Open Edition ADSM Client uses NFS protocols to retrieve or send data to OS/390 LAN Server depending on whether a backup or a restore is being performed.

To implement this method to Backup/Restore OS/390 LAN Server data, you must have the OS/390 LAN Server TCP/IP NFS Support active. Additionally:

- The Open Edition ADSM Client must be installed.
- The Open Edition NFS Client must be installed.
- The OS/390 LAN Server file system must be mounted as a remote file system to Open Edition.

## Overview of Installing OS/390 LAN Server

The following section gives you an overview of the tasks needed to install the OS/390 host code and a front-end processor. In an NFS environment, the use of a front-end processor is optional.

## Installing the OS/390 host system:

1. Receive OS/390 LAN Server (or, OS/390 LAN Server NLS feature) to move the OS/390 LAN Server material from the distribution tape into SMPTLIBS.
2. Install job streams from SMPTLIBS to copy JCL members from the SMPTLIBS into a temporary data set.

3. Allocate target and distribution data sets to provide the distribution and target libraries to perform an SMP/E apply.
4. Define DDDEFs to SMP/E to add the appropriate DDDEF entries to the target and DLIB zones into which OS/390 LAN Server is installed.
5. Apply OS/390 LAN Server with CHECK processing to check for SYSMOD errors.
6. Apply OS/390 LAN Server to update the target libraries.
7. Accept OS/390 LAN Server with CHECK processing to complete the final phase of the host installation.
8. Apply OS/390 LAN Server to update the distribution libraries.

## Installing the LAN Front-End Processor:

Install and configure the front-end processor drivers to perform the initial installation of the front-end processor code and the initial configuration of your front-end processor as a server machine.

1. Complete the appropriate front-end processor (OS/2 page “OS/2 LAN Server Front-End Processor Installation Worksheet” on page 40 or NFS page “NFS Front-End Processor Installation Worksheet” on page 90) installation worksheet to enter the values for your configuration.
2. At the prompt,
   - For an OS/2 front-end processor, enter *drive:**BFSINST* and follow the prompts on the panels for installing and configuring the front-end processor drivers.
   - For an NFS front-end processor, enter *drive:**BFSNINST* and follow the prompts on the panels for installing and configuring the front-end Processor drivers.
3. Verify the OS/390 LAN Server host software installation.
4. Verify the OS/2 environment if you are installing an OS/2 front-end processor.
5. Verify the NFS environment if you are installing an NFS front-end processor.
6. End the verification session.

When installation is complete, the following actions are optional:

- Modify the front-end processor driver configuration to allow configuration changes for your server machine (if OS/390 LAN Server front-end processor driver code is already installed on your system).
- Replace existing front-end processor drivers with a new version of the front-end processor driver code.
- Remove front-end processor drivers from the workstation so the front-end processor will no longer function as a server for the OS/390 LAN Server.
- Create a front-end processor installation diskette to use for another machine.
- Copy the front-end processor installation code to the hard disk of the front-end processor.
- Create or use response files to ease the front-end processor driver code installation task.

**Note:** No new OS/390 LAN Server code is required on any end-user's workstation. However, two utility programs are provided for workstation users to use in environments that share data between their OS/2 LAN Server and NFS users. These programs, **os22unix** and **unix2os2**, are shipped on the host installation tape.

## Installing on the Host

A sample configuration file for an OS/390 LAN Server server is shipped on the product tape that is loaded onto the OS/390 LAN Server system. This file can be used as a model for the configuration entries for all of your OS/390 LAN Server servers. A configuration file is a member of a partitioned data set, and is identified by a CONFIG Configuration File in the JCL.

OS/390 LAN Server requires one mandatory and one optional configuration file for product installation.

Linear data sets must also be provided for the actual storage of workstation data. The number and size of these data sets is determined by the system administrator.

Use the OS/390 LAN Server TSO/E command FORMATDS to initially allocate and format an LDS for actual storage of workstation data.

**Note:** The backup and restore functions of OS/390 LAN Server use the FORMATDS label of each VSAM linear data set (LDS) defined to the OS/390 LAN Server server as part of the filespace name when backing up or restoring the data set to the OS/390 LAN Server backup server. Therefore, it is recommended that you use a unique label for each VSAM LDS, regardless of whether the data set will be used as a FOLD, MIXED, or ANY data set. This avoids the chance that two or more data sets will be backed up to (or restored from) the same filespace within the backup server.

### TCP/IP Environment

One or more OS/390 LAN Server servers can be defined on a given OS/390 system. However, each OS/390 LAN Server server providing NFS services must be connected to a separate TCP/IP address space. For example, if you want two OS/390 LAN Server NFS servers on an OS/390 system, you need two TCP/IP address spaces, each with one OS/390 LAN Server NFS server connected to it. This approach may also be used to connect other OS/390-based NFS servers on the same OS/390 system.

If an NFS server that is connected to a TCP/IP address space is being replaced by an OS/390 LAN Server NFS server, then the currently running server must be shut down.

### CLAW Connectivity

When using CLAW connectivity, the number of page frames that OS/390 LAN Server attempts to lock in storage is determined by the RPAGES and WPAGES operands of the LINK record in the CONFIG Configuration File. Each of these values can range from 16 to 63. The CLAW communications driver is unsuccessful if it cannot lock the total number of pages specified by the sum of the RPAGES and WPAGES operands plus 2 pages.

# Chapter 2. Installing Host CODE

## Overview

See *OS/390 Planning for Installation Release 4* for the hardware and software requirements for OS/390 LAN Server.

See the OS/390 Program Directory for additional installation information.

This is an overview of the steps required to install OS/390 LAN Server and a brief explanation of what you are doing in each step. For the purpose of this overview, it is assumed that a SMP/E install of the OS/390 LAN Server code has already been completed. Following the overview, is a detailed step by step procedure explaining how to accomplish the install. The steps required to install OS/390 LAN Server are as follows:

- **Update PROCLIB.**

  In this step, you are defining the started procedure in PROCLIB for OS/390 LAN Server.

- **Update PARMLIB.**

  In this step, you are performing the APF authorizations for the started procedure defined in the PROCLIB. You are updating the PROGxx member with the data set name that contains the OS/390 LAN Server executable code. LNKLSTxx must be updated if you are not using STEPLIB in the JCL started proc. You may also have to define OS/390 Open Edition authorization for the started procedure defined above.

- **Define VTAM Logon Mode.**

  In this step, you are updating the VTAM mode table in VTAMLIB to include OS/390 LAN Server in that table.

- **Define VTAM application names.**

  In this step, you are updating your VTAMLST to include the VTAM application IDs for OS/390 LAN Server.

- **Define the TSO/E user(s) that will administer the OS/390 LAN Server server.**

  There are three steps required to define the TSO/E user(s). The three steps are:

  – Update the logon PROC of the user.
  – Place an authorize record in the CONFIG member of the Configuration data set.
  – Set up the VTAM application ID for the user.

- **Allocate and initialize the linear data set(s) for OS/390 LAN Server.**

  In this step, you will create the VSAM linear data set(s) and format them using FORMATDS. This formatting of the data set enables OS/390 LAN Server to use the data set(s).

- **Define resource access control.**

In this step, you will define the security method used to:

- Specify access control for data
- Specify access control for started procedures
- Specify access control for Administrator commands
- Specify access control for NFS client user IDs and passwords

- **Define connection method.**

  In this step, you will define one or more connection method(s) used to connect the users to OS/390 LAN Server. The connection methods are:

  - TCP/IP connection
  - VTAM LU6.2 connection
  - OS/2 front-end processor CLAW connection
  - NFS front-end processor CLAW connection

- **Install Front-End Processor.**

  In this step, you will set up the front-end processor(s) with the OS/390 LAN Server front-end processor code.

- **Tailor OS/390 LAN Server.**

  In this step, you will tailor the Configuration data set on the Host to match your installations requirements. You will also tailor the CONFIG files and INI files on the front-end processor.

- **Define OS/390 LAN Server transaction names to the OS/390 Workload Manager.**

  In this step, you will define the Workload Management policy for the OS/390 LAN Server tasks.

- **Start OS/390 LAN Server Front-End Processor(s).**

  In this step, you will start the OS/390 LAN Server front-end processor code that was installed on the front-end processor(s).

- **Start OS/390 LAN Server Host Server.**

  In this step, you will start the PROC that was placed in the PROCLIB on your system.

At this point, your installation is complete. It is now time to logon users and have them use OS/390 LAN Server.

## Detailed Installation Steps

**Please note**

If you are migrating from an earlier release of this product, you may want to refer to the following data sets before continuing. You can easily create similar data sets for use with the new release. Copy your existing data sets that contain the appropriate information to new data sets that you can then modify to use with the new release.

- Access control information - refer to the ACCSCTL DD statement or to the default data set BFS.LFS.ACCSCTL.
- OS2LFS configuration information - refer to the OS2LFS DD statement or to the default data set BFS.SBFSCNFG(OS2LFS).
- CONFIG configuration information - refer to the CONFIG DD statement or to the default data set BFS.SBFSCNFG(CONFIG).
- Installation logon procedures and run procedures - refer to your system administrator for these procedures.

1. **Update PROCLIB.**

   Copy the following to SYS1.PROCLIB (or other PROCLIB, as appropriate for your installation) to member name RUNLFS:

   ```
   BFS.SBFSSAMP(BFSXXRUN)
   ```

   Customize the region size parameter to an appropriate value for your installation. OS/390 LAN Server uses the maximum amount of virtual storage (region size) allowed by the installation since it is a memory-intensive task. A REGION=0K allows the task to obtain the installation maximum value specified at JES initialization.

   **Note:** If your installation does specify REGION=0K, the result is unpredictable. You may want to ask your local IS system administrator for more information about your installation's maximum region size.

   In addition to the region size, the SYSTRACE data definition is defined with FREE=CLOSE and may be customized by the installation. FREE=CLOSE allows the OS/390 LAN Server trace data to be deallocated when tracing is turned off. For example, if an installation wants to use a data set for trace data, the FREE=CLOSE option is not appropriate. For more information on the use of FREE=CLOSE, see *OS/390 MVS JCL Reference*.

   **Note**

   The STEPLIB data definition may have to be updated to include the Language Environment* for OS/390 and the OS/390 LAN Server load libraries. The default data set names are commented out in the BFSXXRUN member. Also, these load libraries must be APF authorized when used with OS/390 LAN Server, since it is APF authorized.

2. **Update PARMLIB.**

   You must add the following statement to either the IEAAPFxx or PROGxx member, including `volser`:

   ```
   BFS.SBFSLMOD volser
   ```

   In addition, you must add:

```
BFS.SBFSLMOD
```

to one of the following:

- To member LNKLSTxx

  Or,

- To the STEPLIB statement SYS1.PROCLIB(RUNLFS). See step 5 on page 31.

  To start the OS/390 file server during OS/390 system initialization, add the following statement to the COMMNDxx member of the SYS1.PARMLIB data set:

```
COM='START RUNLFS'     where RUNLFS is the name of the proc you
                       created in the Update Proclib step above.
```

**Note: If you have chosen to use the member, PROGxx, it is not necessary to re-ipl your system.**

3. **Define VTAM Logon Mode.**

   In this step, you are updating the VTAM mode table in VTAMLIB to include OS/390 LAN Server in that table.

   Run the JCL in member BFSXXTAB that is located in BFS.SBFSSAMP.

   For further information, see “Sample VTAM Logon Mode Definition File for LU6.2 Applications” on page 158.

4. **Define VTAM application names.**

   Add BFS.SBFSSAMP(BFSXXAPL) to SYS1.VTAMLST as member BFSAPPLS. The VTAM application names specified for the front-end processor application name, the administration application name, and the TSO/E user application name in BFSAPPLS, must match the parameters specified in BFS.SBFSCNFG(CONFIG).

   The command to activate the VTAM major node for only the duration of a specific system IPL is:

```
V NET,ACT,ID=BFSAPPLS
```

   If you want to activate the VTAM major node automatically on each IPL, add BFSAPPLS to member ATCCONxx of the SYS1.VTAMLST data set.

   The following is an example of the SYS1.VTAMLST for OS/390 LAN Server:

```
************************************************************
*                                                          *
* VTAM APPLICATION NAMES FOR OS/390 LAN Server                    *
*                                                          *
************************************************************
BFSAPPL  VBUILD TYPE=APPL            APPLICATION MAJOR NODE
*
* FEP COMMUNICATION APPLICATION NAME
LFSFEP APPL APPC=YES,        ALLOW APPC COMMUNICATIONS     *
            SECACPT=CONV,    CONVERSATION SECURITY ALLOWED *
            DSESLIM=4,       SESSION LIMIT                 *
            PARSESS=YES,     ALLOW PARALLEL SESSIONS       *
            MODETAB=BFSTAB,  LOGON MODE TABLE FOR APPL     *
            DLOGMOD=BFSLMOD  LOGON MODE FOR APPL
*
* ADMINISTRATION COMMUNICATION APPLICATION NAME
LFSADM APPL APPC=YES,        ALLOW APPC COMMUNICATIONS     *
            SECACPT=CONV,    CONVERSATION SECURITY ALLOWED *
            DSESLIM=2,       SESSION LIMIT                 *
            PARSESS=YES,     ALLOW PARALLEL SESSIONS       *
            MODETAB=BFSTAB,  LOGON MODE TABLE FOR APPL     *
            DLOGMOD=BFSLMOD  LOGON MODE FOR APPL
*
* TSO/E USER (ADMINISTRATOR) COMMUNICATION
* APPLICATION NAME(S)
*
LFSADM1 APPL EAS=2,          ESTIMATED CONCURRENT SESSIONS *
             SECACPT=CONV,   CONVERSATION SECURITY ALLOWED *
             APPC=YES,       ALLOW APPC COMMUNICATIONS     *
             DSESLIM=2,      SESSION LIMIT                 *
             PARSESS=YES,    ALLOW PARALLEL SESSIONS       *
             MODETAB=BFSTAB, LOGON MODE TABLE FOR APPL     *
             DLOGMOD=BFSLMOD, LOGON MODE FOR APPL          *
             AUTOSES=2,      CONTENTION WINNER INFORMATION *
             AUTH=TSO        TSO/VTAM TIME-SHARING PROGRAM
*
* ...
*
```

5. **Define the TSO/E user(s) that will administer the OS/390 LAN Server server.**

   TSO/E users who plan to administer the OS/390 LAN Server server must have access to the OS/390 LAN Server load modules and the Language Environment for OS/390 run time libraries.

   If you did not update SYS1.PARMLIB as described in Step 2 on page 29, data set BFS.SBFSLMOD must be in the user's TSO/E search order to allow access to LFS. Do this by adding the data set to the logon procedure in SYS1.PROCLIB (or other PROCLIB, as appropriate for your installation).

   The following data definitions must be added to the logon procedure or through the TSO ALLOCATE command:

   - BFS.SBFSTLIB must be added to the ISPTLIB data definitions.
   - BFS.SBFSPLIB must be added to the ISPPLIB data definitions.
   - BFS.SBFSPROC must be added to the SYSEXEC data definitions.

- BFS.SBFSMSGS(AMENG) must be added as the BFSLANG data definition.

**Note:** You must logoff and log back on again to pick up these changes.

6. **Allocate and initialize the linear data set(s) for OS/390 LAN Server.**

   a. **If System Managed Storage (SMS) is active**, use the FORMATDS command to dynamically allocate and initialize the VSAM linear data set. This is a stand-alone command entered from a TSO/E user ID. Formatting a large linear data set can take several minutes. The FORMATDS command attempts to dynamically allocate a linear data set using OS/390 callable services. The following is the command format for FORMATDS:

      ```
      formatds dsname label size
      ```

      **dsname** Specifies the name of a VSAM linear data set used as a workstation data repository.

      **label** Specifies the label of the disk image. The label can be from 1 to 6-alphanumeric characters and is used to construct the volume label seen by workstations. Lowercase characters are converted to uppercase.

      **size** Specifies the size of the disk image. This parameter can be specified in one of the following formats. If the specified size is less than 256 4K pages (1M), an error message is issued. Size is limited by VSAM to a maximum of 4GB.

      **Please note**

      Since the allocation of linear data sets by VSAM occurs on cylinder boundaries, the maximum size can be slightly smaller than 4GB. The actual difference depends on your DASD type. For example, a triple density 3380 DASD with a 2 cylinder VTOC would support a maximum LDS size of 1.5GB.

      ```
      (2653 cyl. * 150 pages per cyl * 4096 Bytes per page)
      ---------------------------------------------------- = 1.51 GB
                           1,073,741,824
      ```

      **Note:** In each of the following descriptions, *nnn* can be specified as a positive whole number (10 or 20, for example), or a positive decimal number greater than 1.0 (1.5 or 4.5, for example). Positive decimal numbers less than 1.0 (0.5 or 0.7, for example) do not work.

      *nnn* Specifies the size of the data set where *nnn* is in 4K blocks.

      *nnnK* Specifies the number of kilobytes (1024-bytes) for the disk image. This number is rounded up to the nearest 4KB boundary, if necessary.

      *nnnM* Specifies the number of megabytes (1024*1024-bytes) for the disk image. This number is rounded up to the nearest 4KB boundary, if necessary.

*nnnG* Specifies the number of gigabytes (1024*1024*1024-bytes) for the disk image. This number is rounded up to the nearest 4KB boundary, if necessary.

Here is an example of the FORMATDS command:

```
formatds data.set1 onemeg 1m
```

In this example, the data set name DATA.SET1 is the same as in an LFSDSN record located in BFS.SBFSCNFG(CONFIG) and a SHARE record located in BFS.SBFSCNFG(OS2LFS). The label of the data set is ONEMEG. The size of the data set is one megabyte (1024*1024-bytes).

b. **If System Managed Storage (SMS) is NOT active**, a linear data set must be allocated in a separate step before entering a FORMATDS command. See BFS.SBFSSAMP(BFSXXBAT) for a sample JCL to allocate the data set. Then use the FORMATDS command in Step 6 on page 32 to format the data set. If *nnn* does not match the RECORDS *nnn* in the JCL to allocate a new linear data set, an error may result.

7. **Define resource access control.**

Create a sequential data set for group, user and resource access control definitions before starting OS/390 LAN Server. A sample is shipped as a member of BFS.SBFSSAMP(BFSXXACS). This member can be copied to the sequential data set named BFS.LFS.ACCSCTL that is allocated during installation.

If external security is used for a resource, take the appropriate steps to define your resources and LAN user IDs to your external security manager. You may want to consult your local IS security administrator for more information about your installation's external security manager.

a. If using an OS/2 front-end processor with LOCAL security:

- BASE LDSs

  The default access control file grants all users access to all base formatted data sets. Access controls for BASE LDSs can be changed by the OS/390 LAN Server Administrator using the OLSACCS command.

- EXTENDED LDSs

  The default access for EXTENDED LDSs is no access. Access controls for EXTENDED LDSs can be changed by the OS/390 LAN Server Administrator using the ACCESS command.

b. If using an NFS Front-End Processor:

If you chose to use SECURITY LOCAL (the default) in configuration data set BFS.SBFSCNFG(NFSLFS), then create a sequential data set for group and resource access control definitions before starting OS/390 LAN Server. A sample is shipped as a member of BFS.SBFSSAMP(BFSXXACS). This member can be copied to the sequential data set named BFS.LFS.ACCSCTL that is created during installation. The default access control file grants all users access to all resources. This can be changed later with administrator commands.

If you plan to use PCNFS Authentication, you must specify NFS ON, and either PCNFS ON or PCNFS LIST in the CONFIG Configuration File. If you

specify PCNFS LIST, you must specify a NOPCNFSAUTH record in the NFSLFS configuration file for each user that is running on a system that is not capable of using the PCNFS Authentication Protocol.

8. **Define connection method.**

   a. Using a TCP/IP connection.

      1) TCP/IP must be up and running on the Host.

         a) In the TCP/IP profile, port 2049 must be commented out.

         b) Portmapper must be up and running.

         c) The TCP/IP process must be OMVS defined.

      2) Open Edition must be up and running.

      3) The NFS client must be up and running.

      4) Update the CONFIG Configuration File as follows:

         - The NFS record must specify ON.
         - The NFSID record must specify the symbolic name of the host NFS server to which the NFS front-end processor will connect.
         - If present, the TCPIP record must be deleted or commented out.
         - The NOTCPIP option of the NFSID record must be removed.

   b. Using a VTAM SNA LU6.2 connection.

      1) On the Host side:

         a) Update/Create the VTAM Logon mode definition file. Refer to “Sample VTAM Logon Mode Definition File for LU6.2 Applications” on page 158 for an example of this file.

         b) Update BFS.SBFSCNFG(CONFIG) to include:

            - OLSID your_fep

         c) Your_fep must also be defined in the BFSAPPLS member in SYS1.VTAMLST. Refer to “Sample VTAM APPC VTAMLST - SNA Application Name” on page 158 for an example of this file.

         d) Setup the VTAM Switch Major Node definition file.

         e) Setup the VTAM Major Node definition file.

            **Note:** Refer to your VTAM documentation for assistance in setting up the above two steps.

      2) On the front-end processor side:

         - Refer to “Configuring CM/2” on page 145 and perform the steps necessary for your account.

   c. Using an OS/2 front-end processor CLAW connection.

      When you are making an OS/2 front-end processor CLAW connection, you must modify the BFS.SBFSCNFG(CONFIG) file.

      1) Update the LINK statement in the CONFIG file for the CLAW connection between the host and the front-end processor (FEP).

         The LINK statement is in the form **LINK even_device_address fepname CLAW**. The even_device_address is a 4-character

hexadecimal number. The FEPNAME is up to an 8-character name identifying the front-end processor. The default FEPNAME is FEPUSER.

2) Refer to the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40.

   Write the *FEPNAME* in the FEP Name row of the worksheet. Then write the last two digits of the *even device address* in the Channel Address row of the worksheet.

**Please note**

This is the second place where you are asked to specify the FEPNAME. The host side and the PC side must identify the front-end processor by the same name, or communications between the two sides will not occur. You must specify the same FEP Name in both places. The default FEP Name is **FEPUSER**. The two places to specify FEPNAME are:

1. The **CONFIG** file **LINK** statement.
2. The **SET CONFIGURATION** panel of the front-end processor installation on the PC **FEP Name** field.

**For CLAW Connections - Please Note**

There are two places where you are asked to specify the line addresses for the CLAW connections. The host side and the PC side must identify the CLAW line address by the same number(s), or communications between the two sides will not occur. The two places to specify the line addresses for the CLAW connections are:

1. The **LINK** statement in the **CONFIG** file.
2. The **SET CONFIGURATION** panel of the front-end processor installation on the PC **Channel Address** field uses the **last two digits of the even odd pair line address**.

d. Using an NFS front-end processor CLAW connection.

When you are making an NFS front-end processor CLAW connection, you must modify the BFS.SBFSCNFG(CONFIG) file.

1) Update the LINK statement in the CONFIG file for the CLAW connection between the host and the front-end processor.

   The LINK statement is in the form **LINK even_device_address fepname CLAW**. The even_device_address is a 4-character hexadecimal number. The FEPNAME is up to an 8-character name identifying the front-end processor. The default FEPNAME is FEPUSER.

2) Refer to NFS Front-End Processor Installation Worksheet, Table 9 on page 90.

Write the *FEPNAME* in the FEP Name row of the worksheet. Then write the last two digits of the *even device address* in the Channel Address row of the worksheet.

**Please note**

This is the second place where you are asked to specify the FEPNAME. The host side and the PC side must identify the front-end processor by the same name, or communications between the two sides will not occur. You must specify the same FEP Name in both places. The default FEP Name is **FEPUSER**. The two places to specify FEPNAME are:

1. The **CONFIG** file **LINK** statement.
2. The **SET CONFIGURATION** panel of the front-end processor installation on the PC **FEP Name** field.

**For CLAW Connections - Please Note**

There are two places where you are asked to specify the line addresses for the CLAW connections. The host side and the PC side must identify the CLAW line address by the same number(s), or communications between the two sides will not occur. The two places to specify the line addresses for the CLAW connections are:

1. The **LINK** statement in the **CONFIG** file.
2. The **SET CONFIGURATION** panel of the front-end processor installation on the PC **Channel Address** field uses the **last two digits of the even odd pair line address**.

9. **Install Front-end Processor.**
   - If you are not installing a front-end processor, omit this step.
   - Refer to Chapter 3, “OS/2 LAN Server Front-End Processor Installation” on page 39 for OS/2 front-end processor installs.
   - Refer to Chapter 4, “NFS Front-End Processor Installation” on page 89 for NFS front-end processor installs.
10. **Tailor OS/390 LAN Server.**

    Following is a list of some of the modifications that you may want to make:

    - Modify the OS/390 LAN Server Configuration Data Set.

      OS/390 LAN Server Configuration Data Set BFS.SBFSCNFG(CONFIG) defines configuration parameters to use when the OS/390 file server is started. The records in this data set may be up to 1200 characters long with no continuation.

      Examples of what you may need to modify are:

      – The OLSID and ADMINID of the OS/390 LAN Server administration processor and SMB processor, if you changed the VTAM APPLIDs in Step 4 on page 30
      – The name and size of an audit data set, if any

  - The single byte character set (SBCS) translation table to use
  - The TSO/E user APPLIDs that are authorized to connect to the server for administration in Step 4 on page 30
  - The options regarding the use of channel connections, if any
  - The maximum number of concurrent users of the server
  - The file sharing data sets accessed by the server
  - The translation table to use when using uppercase network path names
  - The BFSBR options file to use when using Backup/Restore commands
  - The ADSM Server information to use when using the ADSM Server
  - The COMAPI record, if you want to define the socket a program uses to issue LAN Server commands

- Modify the OS/390 LAN Server OS/2 LAN Server Configuration Data Set.

  The OS/2 LAN Server Configuration Data Set (BFS.SBFSCNFG(OS2LFS)) contains configuration parameters for the host side of the connection between the OS/390 file server and its OS/2 LAN Server front-end processors. The records in this data set may be up to 1200 characters long with no continuation.

  Examples of what you may need to modify are:

  - The type of security mechanism used for LAN user access control
  - The names of the OS/2 LAN Server machines acting as front-end processor(s)
  - The OS/390 data sets that can be accessed by each front-end processor
  - If accounting information is recorded for OS/2 LAN Server client activity
  - The maximum size of communication buffers

- Modify the OS/390 file server Profile.

  The OS/390 file server Profile (BFS.SBFSEXEC(PROFILE)) Data Set can contain a list of administration requests entered during server initialization. Any valid OS/390 file server administration request can be specified in this data set, but only one request can be specified on each record of the data set. In addition, only the first 1200 characters of each record are examined.

- Modify the BFSBR Options File.

  The Backup/Restore options file (BFS.SBFSCNFG(BFSBR)) defines the options that the OS/390 LAN Server and the backup servers use to back up and restore data sets when the LFSBR command is entered. The options file is not required. If you do not want to use such a file to store the LFSBR command defaults, you may enter the operands of your choice each time you enter the LFSBR command. There are several records in the options file that need to be tailored to suit your backup and restore requirements.

  Examples of what you may need to modify are:

  - The administrative user ID and node where backup/restore status log files are sent.
  - The server name of the backup server where the files will be backed up.
  - The user ID and node of the backup server.
  - The log mode of the backup server.
  - The name of the backup node to back up data sets to.
  - A password used to access the backup server.

For further customization, see the *OS/390 LAN Server Guide*.

11. **Define OS/390 LAN Server transaction names to the OS/390 Workload Manager.**

    If you do not wish to manage the four individual workloads within the OS/390 LAN Server address space, then you must either:

    a. Delete the enclaves statement in the configuration file referenced by the CONFIG DD statement of the OS/390 LAN Server started procedure, or

    b. Specify ENCLAVES NO in the configuration file referenced by the CONFIG DD statement of the OS/390 LAN Server started procedure.

    If you are not managing any of the four workloads within the OS/390 LAN Server address space, then each of the four types of work will all be managed based upon the controls defined for the OS/390 LAN Server address space.

    If you do wish to manage the workloads within the OS/390 LAN Server address space, then you must set the enclaves record in the configuration file referenced by the CONFIG DD statement of the OS/390 LAN Server started procedure to say YES (ie. ENCLAVES YES). See "Managing Workloads" in the *OS/390 LAN Server Guide* for instructions on setting up the necessary Workload Manager controls.

    **Note:** Changing the treatment of the workloads does not change the total throughput of OS/390 LAN Server, but it does change the effective throughput of each workload. Giving a particular workload better treatment will increase the effective throughput of that workload.

12. **Start OS/390 LAN Server Front-End Processor(s).**

    Issue the command START BFSSERV on the front-end processor. This will start the OS/390 LAN Server code on the front-end processor and get it ready for use.

13. **Start OS/390 LAN Server Host Server.**

    Issue the START command for the *procname* that your account has set up to start OS/390 LAN Server.

# Chapter 3. OS/2 LAN Server Front-End Processor Installation

## Introduction

The OS/2 LAN Server front-end processor drivers are found on the 3.5" Installation Diskette provided. This diskette consists of the file system drivers and related files that are installed within each OS/2 LAN SERVER machine that will communicate with OS/390 LAN Server. (Once installed, the OS/2 LAN SERVER machine is referred to as an OS/2 LAN Server front-end processor.) The diskettes that can be used for the install are listed below.

For the English version:

- If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

  OS/390 LAN Server: English
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (1 of 2)

  OS/390 LAN Server: English
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (2 of 2)

For the Japanese version:

- If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

  OS/390 LAN Server: Japanese
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (1 of 2)

  OS/390 LAN Server: Japanese
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (2 of 2)

**Note:**

You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia* on the front-end processor before installing OS/390 LAN Server front-end processor code.

# OS/2 LAN Server Front-End Processor Installation Worksheet

*Table 3 (Page 1 of 3). OS/2 LAN Server Front-End Processor Installation Worksheet*

| Information Needed | Your Value | Description |
|---|---|---|
| **For All Connection Types** | | |
| Installation Source | | This is the location of the OS/390 LAN Server source code. If you are installing from the Installation Diskette, it will be ***A:***. |
| Installation Target | | This is the target location where you want the front-end processor driver code to be installed on your server or network. Give the drive and path. If you specify a directory that does not currently exist, the directory will be created for you. If you specify a subdirectory that does not currently exist, the subdirectory will be created for you if the directory itself already exists. That is, the system can create only one new directory layer automatically. The default is: **C:\BFS.** |
| OS/2 LAN Server Path | | This is the path to the OS/2 LAN Server code, of which the IBMLAN.INI file is a part. Fill in the value of the OS/2 LAN Server drive and root directory. The default directory for the OS/2 LAN Server code is **\IBMLAN**. |
| BFS Log File Name | | This record specifies the name of the file to be used to collect log and trace data. The path specified must already exist. The default is **installation target path\BFS.LOG**. |
| Front-End Processor Name | | This is the name the front-end processor will use to connect with host programs. The entry in this field must exactly match the front-end processor record in the OS2LFS file for OS/390. For PWSCS connections, the front-end processor name must match the USERID value in the ACPI.INI file. The default is **front-end processor USER**. |
| OLSID | | This specifies the SMB processor within the File Services server. The entry in this field must exactly match the OLSID record in the CONFIG file for OS/390. If there is no OLSID record, use the default name of **LFS front-end processor**. |
| Connection Type | | This indicates the type of connection between your host server and the front-end processor. The choices are **CM/2**, **CLAW-MMC** and **CLAW-NSCA**. |
| Retry Wait Time | | This indicates the number of seconds the front-end processor should wait before it tries again to establish a connection with the host, when such a connection has been unsuccessful or lost. The values may range from 1 to 3600 seconds. The default is **60** seconds. |
| Heap Size | | This indicates the size of the heap region, an area of free storage from which an application can dynamically allocate blocks of storage. The range for this value is 100KB to 2048KB. This value defaults to 512KB. |

| *Table 3 (Page 2 of 3). OS/2 LAN Server Front-End Processor Installation Worksheet* | | |
|---|---|---|
| **Information Needed** | **Your Value** | **Description** |
| Caching | | This indicates whether memory caching is active or inactive on the front-end processor. Select '***ON***' to make caching active, or '***OFF***' to make caching inactive. If you set caching ON, specify the memory cache size as an integer value between 256 and 16384. The defaults are **ON** and **256**. |
| DB Threshold | | This indicates a file size above which an alternate caching scheme will be used. This field is only relevant for CLAW connections. For CM/2 connections, the values in the DB Threshold field are ignored. Select '***ON***' to activate the DB Threshold, or '***OFF***' to make the DB Threshold inactive. If you set DB Threshold 'ON', specify the DB Threshold file size in an integer value between 120 and 65535. The default for this value is 1004KB. |
| Message Timeout | | This indicates whether messages should be displayed on the front- end processor, and if so, for how long. Select '***ON***' to display messages, or '***OFF***' to log messages without displaying them. If you set Message Timeout 'ON', specify the number of seconds for them to display as an integer value between 0 and 60. The defaults are **ON** and **15** seconds. |
| **For CLAW-MMC Connections Only** | | |
| MMC Adapter | | This specifies which MMC adapter card you are using. The choices are MMC Adapter 0 and MMC Adapter 1. |
| Slot Number | | This specifies the workstation slot number in which the MMC adapter card is installed. The value must be an integer between 1 and 8. |
| Channel Address | | This specifies the last two digits of the 370 subchannel address to be used for the MMC adapter card. The value must be an even 2 digit hexadecimal address, corresponding to **the last two digits of the line address of the host.** |
| Channel Speed | | This specifies the speed of the channel as either DC Interlock or streaming mode in megabits per second. The choices are DC Interlock, 1.9 Mb/sec, 2.7 Mb/sec, 3.4 Mb/sec, or 4.5 Mb/sec. |
| **For CLAW-NSCA (ESCON) Connections Only** | | |
| NSCA Adapter | | This specifies which NSCA card you are using. Select either NSCA Adapter 0 or NSCA Adapter 1. |
| Slot Number | | This specifies the workstation slot number in which the NSCA Adapter card is installed. The value must be an integer between 1 and 8. |
| Local CLAW Address | | The last two digits specify the 370 subchannel which is to be used for the NSCA adapter card. The value must be an even 2 digit hexadecimal address, corresponding to the **last two digits** of the line address of the host. |

*Table 3 (Page 3 of 3). OS/2 LAN Server Front-End Processor Installation Worksheet*

| Information Needed | Your Value | Description |
|---|---|---|
| Remote CLAW Address | | This specifies the hexadecimal address of the fiber connection between the front-end processor and the host, as it is known on the ES/9000* processor. The value must be an even 2 digit hexadecimal address. |
| Direct Fiber/Switched Port | | Choose between these two fields to indicate the form of connection between the front-end processor and the mainframe. If you select Switched Port, also specify values for Port Address and IOCP CU Address. |
| Port Address | | For Switched Port connections, this specifies the port number of the switch connection to the ESCON* channel. Specify a 2-digit hexadecimal address. |
| IOCP CU Address | | For Switched Port connections, this specifies the value from the CUADD parameter of the CNTLUNIT statement for the ESCON channel in the IOCP table for the ES/9000. Specify a 1 digit hexadecimal address. |

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

To install the OS/390 LAN Server software that runs the front-end processor, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive for a local install.

   For the English version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   For the Japanese version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP

| 5647-A01 V2R5M0
| Install Diskette (1 of 2)

| OS/390 LAN Server: Japanese
| OS/2 LAN Srvr 3.0/4.0/5.0 FEP
| 5647-A01 V2R5M0
| Install Diskette (2 of 2)

**Note:**

You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSINST*** for a local install, or

   ***drive:\BFSINST*** to install from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 Lan Server Menu.

5. If you have a previous version of OS/390 LAN Server installed, you must remove it before you can install this version. This version will overwrite the existing BFS.INI file. If you wish to save your existing BFS.INI file, rename it before beginning the formal installation process for OS/390 LAN Server.

   If you do NOT have a previous version of OS/390 LAN Server installed, all of the choices under "Local Services" should be grayed-out except "Install/Configure FEP drivers."

   On the OS/390 LAN Server Menu, select 'Install/Configure FEP drivers'. This will bring up the 'Install Path Selection' panel.

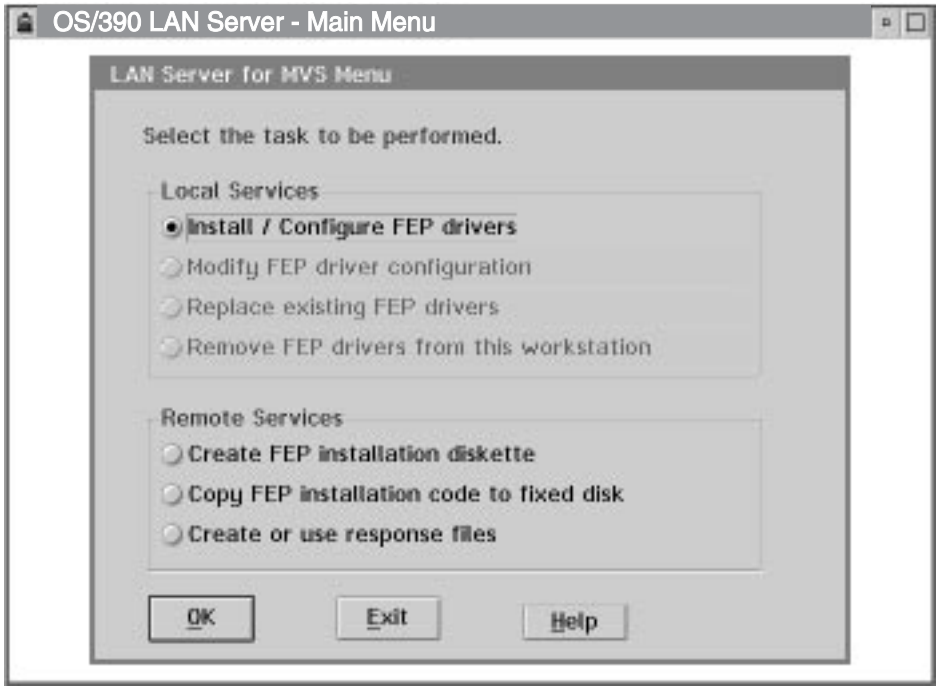


*Figure 2. OS/390 LAN Server Menu - Select Install/Configure Front-End Processor drivers*

6. On the 'Install Path Selection' panel, fill in the entry fields. Use the values on the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40 to fill in the fields. Click on the 'OK' pushbutton when you are done to bring up the 'OS/2 LAN Server Path Selection' panel.


*Figure 3. Install Path Selection*

7. If a path you typed on the panel does not exist, you will see another window appear on the 'Install Path Selection' panel. Click on the 'Yes' pushbutton to create the path.


*Figure 4. Create Install Path*

8. On the 'OS/2 LAN Server Path Selection' panel, fill in the entry field using the value from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to bring up the :'Set configuration' panel.

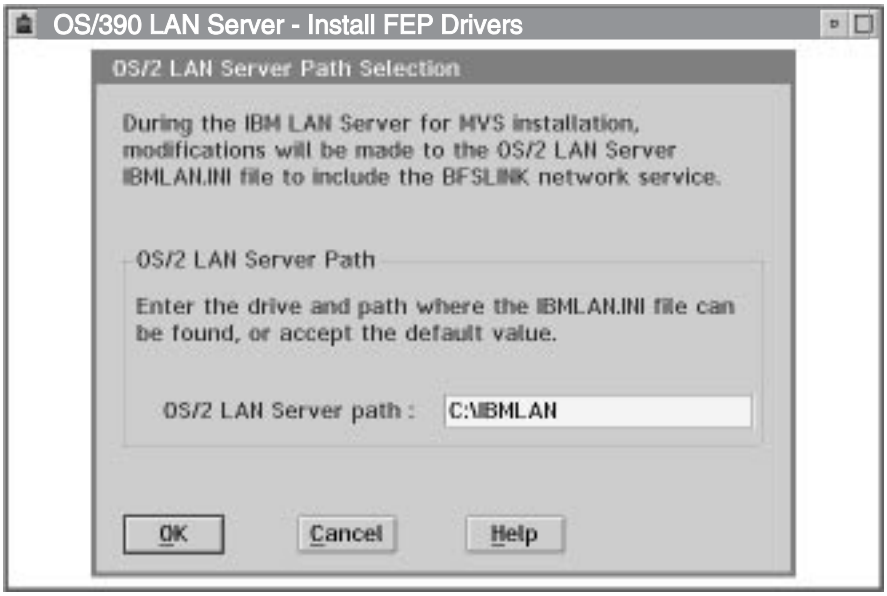


*Figure 5. OS/2 LAN Server Path Selection*

9. On the 'Set configuration' panel, fill in the entry fields using the values from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40.

   If you are making a CM/2 connection, click on the 'OK' pushbutton when you are done, to start the installation.

   If you are making a CLAW connection, click on the 'OK' pushbutton to bring up an additional 'Set configuration' panel.

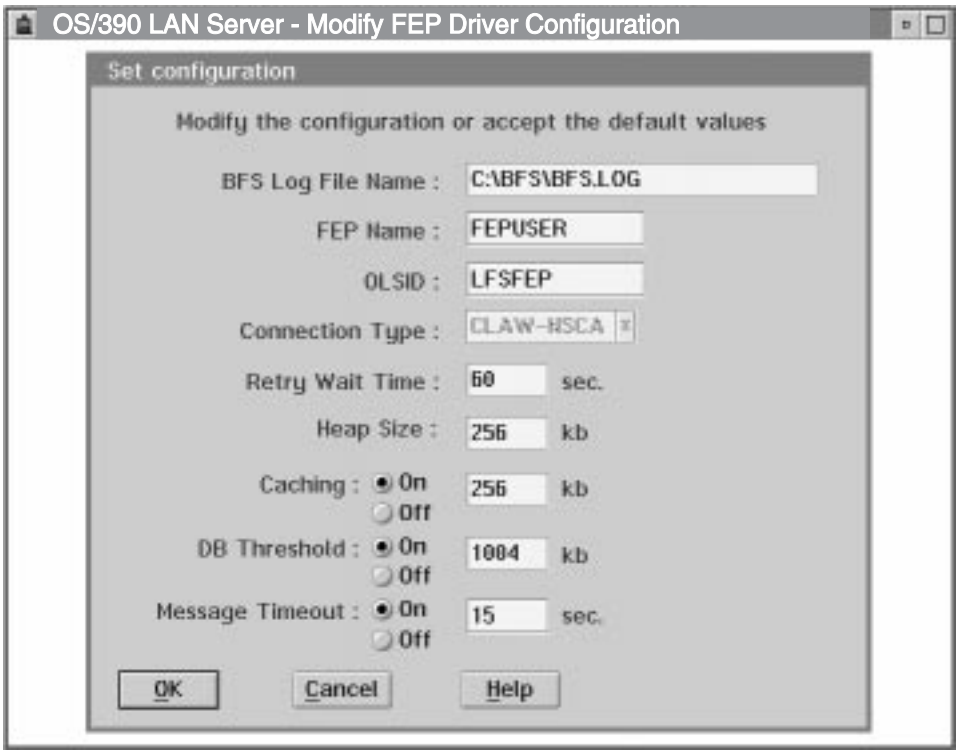


*Figure 6. Set Configuration - Modify Configuration or Accept Defaults*

10. **(CLAW-MMC CONNECTIONS ONLY)** On the 'Set configuration' panel, the first item to select will be the type of MMC Adapter. Fill in the entry fields using the values from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to start the installation.

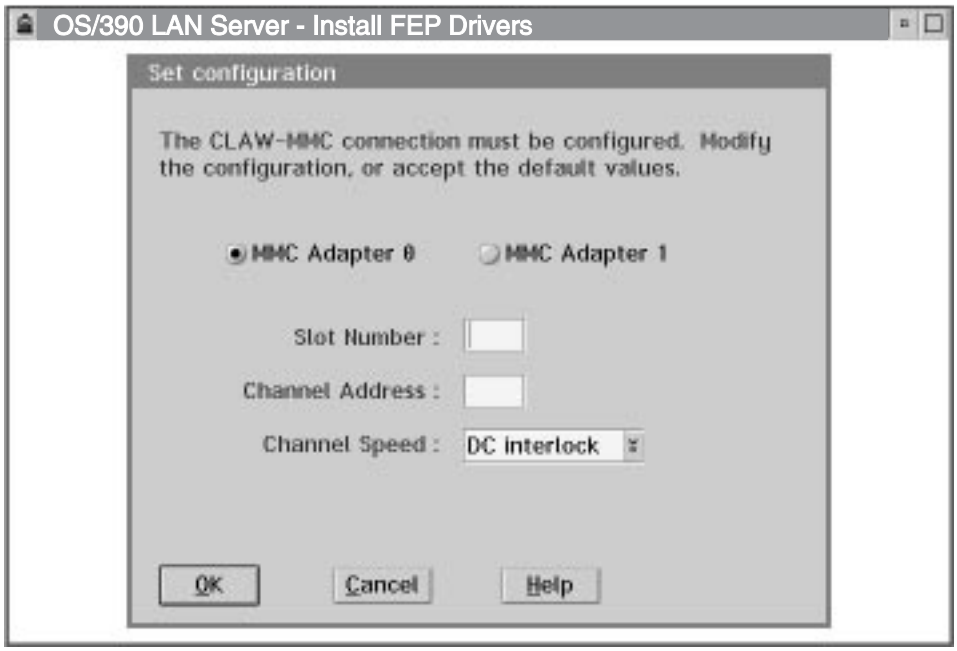


*Figure 7. Set Configuration - CLAW-MMC Connections Only - MMC Adaptor*

11. **(CLAW-NSCA CONNECTIONS ONLY)** On the next 'Set configuration' panel, the first item to select will be the type of NSCA Adapter. Fill in the entry fields using the values from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to start the installation.

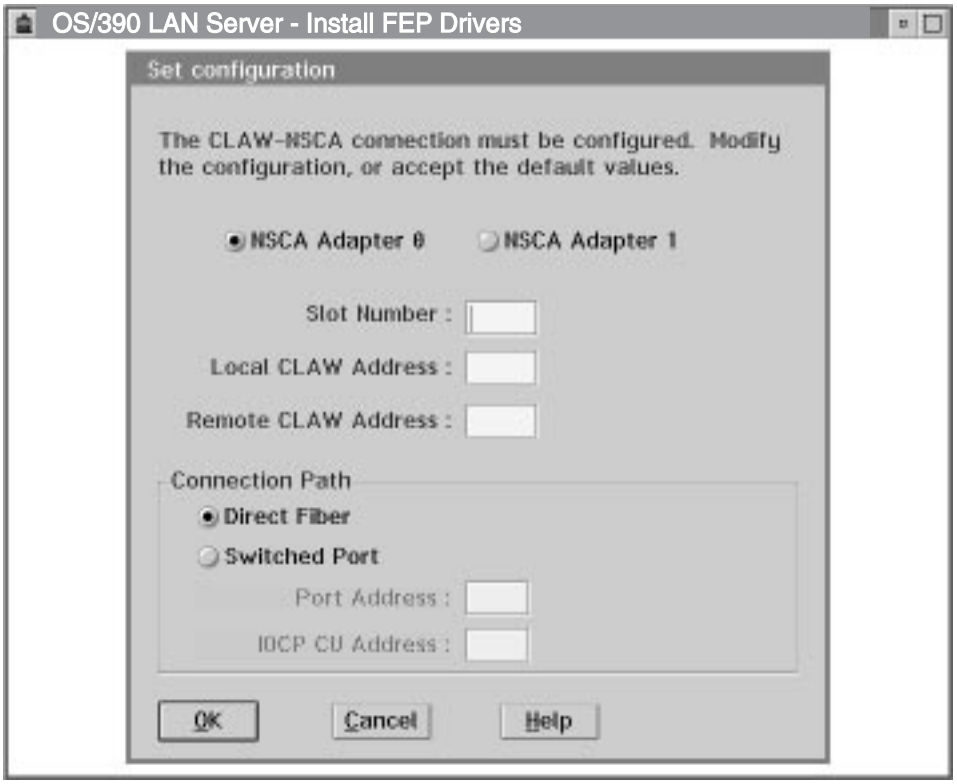


*Figure 8. Set Configuration - CLAW-NSCA Connections Only - NSCA Adaptor*

12. While the installation progresses, you will see a panel indicating which files are being copied and unpacked, and what percent of the installation is now complete.

    **Note:** If you choose to cancel the installation, system errors are likely to occur if OS/390 LAN Server is started. If you wish to use OS/390 LAN Server successfully following a cancel of the installation, begin the installation process again.

13. When the initial installation is complete, a window will appear indicating that the OS/390 LAN Server front-end processor drivers have been installed and that some new files are being automatically created. When this process is complete, the 'IBMLAN.INI modification' panel will appear.

14. Make a selection on the 'IBMLAN.INI modification' panel.

    If you select 'Modify IBMLAN.INI automatically', your original IBMLAN.INI will be renamed to IBMLAN.BFS and a new IBMLAN.INI will automatically be created.

    If you select 'Do NOT modify IBMLAN.INI', a file called IBMLAN.NEW will automatically be created. You will need to manually edit your IBMLAN.INI file to reflect what is in the IBMLAN.NEW file before you try to use the front-end processor drivers.

After you make your selection, click on the 'OK' pushbutton to bring up the 'CONFIG.SYS modification' panel.


*Figure 9. IBMLAN.INI Modification*

15. Make a selection on the 'CONFIG.SYS modification' panel.

    If you select 'Modify CONFIG.SYS automatically', your original CONFIG.SYS will be renamed to CONFIG.BFS and a new CONFIG.SYS will automatically be created.

    If you select 'Do NOT modify CONFIG.SYS', a file called CONFIG.NEW will automatically be created. You will need to manually edit your CONFIG.SYS file to reflect what is in the CONFIG.NEW file before you try to use the front-end processor drivers.

    After you make your selection, click on the 'OK' pushbutton to complete the installation process.

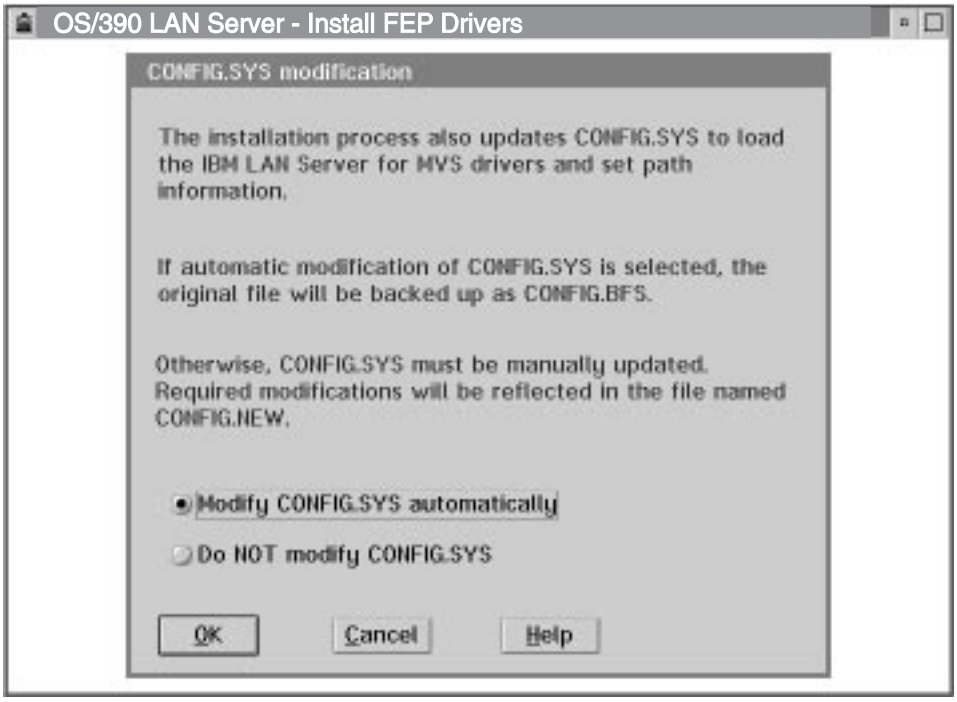


*Figure 10. CONFIG.SYS Modification*

16. When the entire front-end processor driver installation is complete, you will see a window indicating that the drivers were successfully installed. Click on the 'OK' pushbutton to bring up the IBM LAN Server menu.
17. You will be returned to the 'OS/390 LAN Server Menu' panel. Click on the 'Exit' pushbutton, remove the diskette, shutdown the PS/2, and then restart the PS/2 in order to invoke the changes.

## OS/2 LAN Server Front-End Processor Installation Verification

This section applies only to the OS/390 LAN Server OLS and OLS/NFS (via TCP/IP on the host) environments. Verification can be performed after completing the previous installation and tailoring steps, and after the OS/2 portion of OS/390 LAN Server has been installed on the front-end processor.

If only one file serving environment will be supported, then you only need to go through the verification procedure for that environment. To verify the front-end processor installation, perform the following steps:

1. From the OS/390 console on the host, start the OS/390 LAN Server host server.

**start runlfs**

```
Execution begins...
                                        .
                                        .
                                        .
OS/390 LAN Server Version 1.3.0, built MM/DD/YY HH.MM.SS, is ready
```

2. If CLAW connectivity is being used, the subchannels must be varied onto the OS/390 system. You must also enter a START front-end processor NAME command to the channel-connected front-end processor. This command can be included in BFS.SBFSEXEC(PROFILE) to ensure that it is always done at startup.

**start** *fepname*

3. From an OS/2 window (on the front-end processor), issue:

**net start server**
This command starts the OS/2 LAN server program.

**bfsserv**
This starts the front-end processor's OS/390 LAN Server code.

4. From another OS/2 session on the front-end processor, define the TRYD1 resource as a logical drive on the requester workstation. **If you are not already logged onto the LAN as a valid user, the system will prompt you to log on at this time.**

**net use** *h*: *****srvname***\TRYD1**
Where *h*: is the appropriate logical drive letter for the workstation. Use a letter that does NOT correspond to any existing diskette drive or fixed disk drive on the workstation. Be sure that there is a blank between the colon and *srvname*.

*srvname* is the servername of the OS/2 LAN server that you just started (this server is being used as the front-end processor). To find this name, issue "NET WHO" from the OS/2 prompt. The servername is the name under the "Requester" heading.

5. Complete the OS/2 LAN Server front-end processor verification:

**dir** *h*:
Where *h*: is the logical drive defined in the previous step.

The contents of the OS/390 LAN Server machine's TRYD1 file system should be listed on your screen with workstation compatible file identifiers.

**Note**

OS/2 LAN Server front-end processor verification is now complete.

## Terminate OS/2 LAN Server Front-End Processor Verification

1. On the front-end processor, terminate **BFSSERV**.

   BFSSERV can be ended by closing the front-end processor window.

   Close the front-end processor panel by :

   - Clicking on ***Close*** on the OS/2 pull down menu, OR
   - Pressing 'F3', OR
   - Pressing 'ALT-F4'

2. From the host, reinitialize the OS/390 LAN Server server before making it available to the user community, using one of the following two commands:

**stop runlfs**

OR

**f runlfs,shutdown**

**Note**

You are ready to place OS/390 LAN Server in production.

# Startup/Shutdown Procedures

## Host Startup

The OS/390 operator can start OS/390 LAN Server by entering **start runlfs**.

## Host Shutdown

To stop OS/390 LAN Server, enter one of the following commands:

- To shut down OS/390 LAN Server from a TSO/E administrator, enter **shutdown**.
- From an OS/390 console, enter **stop runlfs**.

## OS/2 Front-End Processor Startup

At the *x:*\ prompt, enter the command ***BFSSERV*** where **x:** is the drive where the front-end processor code resides.

## OS/2 Front-End Processor Shutdown

Close the front-end processor panel by :

- Clicking on ***Close*** on the OS/2 pull down menu OR
- Pressing 'F3' OR
- Pressing 'ALT-F4'

## Modifying the OS/2 LAN Server Front-End Processor Driver Configuration

Before you begin the formal modification process for the OS/390 LAN Server FEP drivers, complete the OS/390 LAN Server OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40.

To modify the configuration of the front-end processor drivers, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive for a local modification.

   For the English version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   For the Japanese version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   **Note:**

   You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSINST*** for a local modification, or

   ***drive:\BFSINST*** to modify from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Modify FEP driver configuration'. (Since you have already installed OS/390 LAN Server, the 'Install/Configure FEP drivers' choice under “Local Services” should be grayed-out). This will bring up the 'Modify FEP driver configuration' panel.

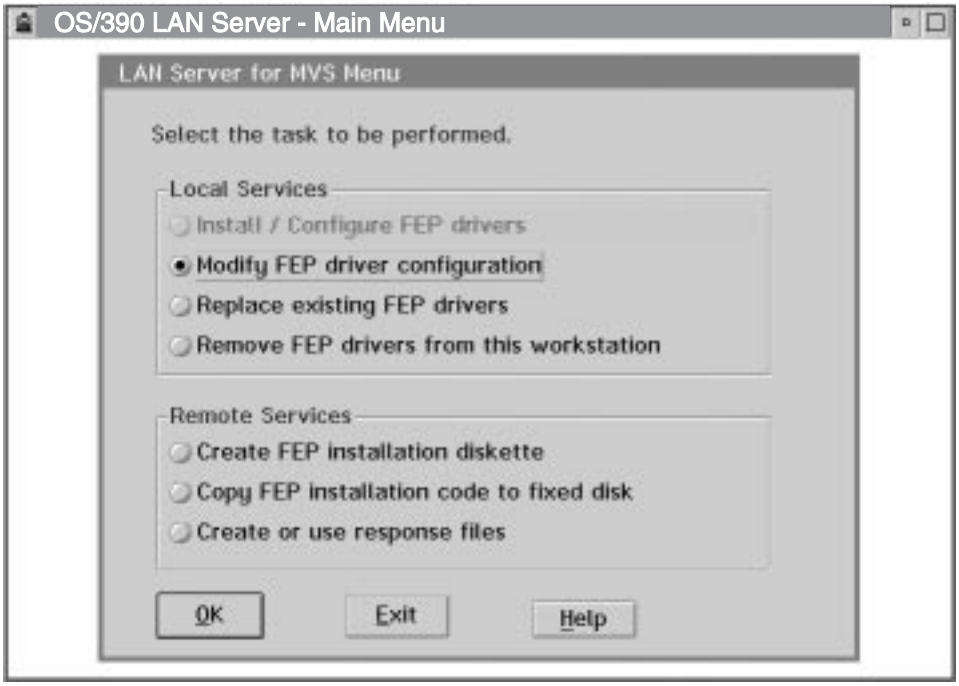


*Figure 11. OS/390 LAN Server Menu - Select Modify FEP Driver Configuration*

6. On the 'Modify FEP driver configuration' panel, fill in the entry fields. Use the values on the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40, to fill in the fields. Click on the 'OK' pushbutton when you are done.

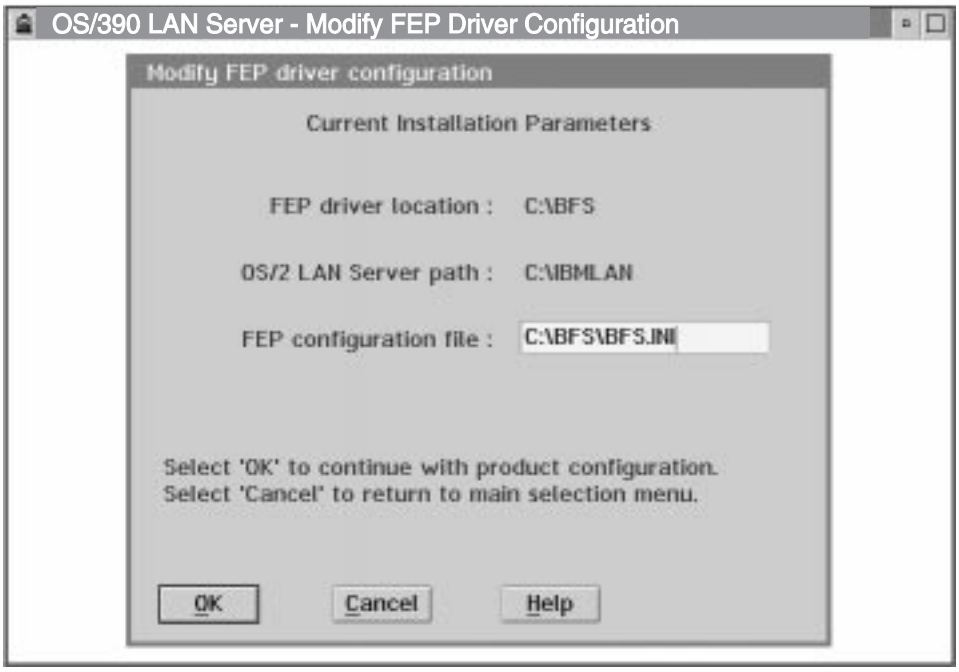


*Figure 12. Modify OS/2 FEP Driver Configuration*

7. On the 'Set configuration' panel, fill in the entry fields using the values from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40.

   If you have a CM/2 connection, click on the 'OK' pushbutton when you are done, to start the installation.

   If you are making a CLAW connection, click on the 'OK' pushbutton to bring up an additional 'Set configuration' panel.

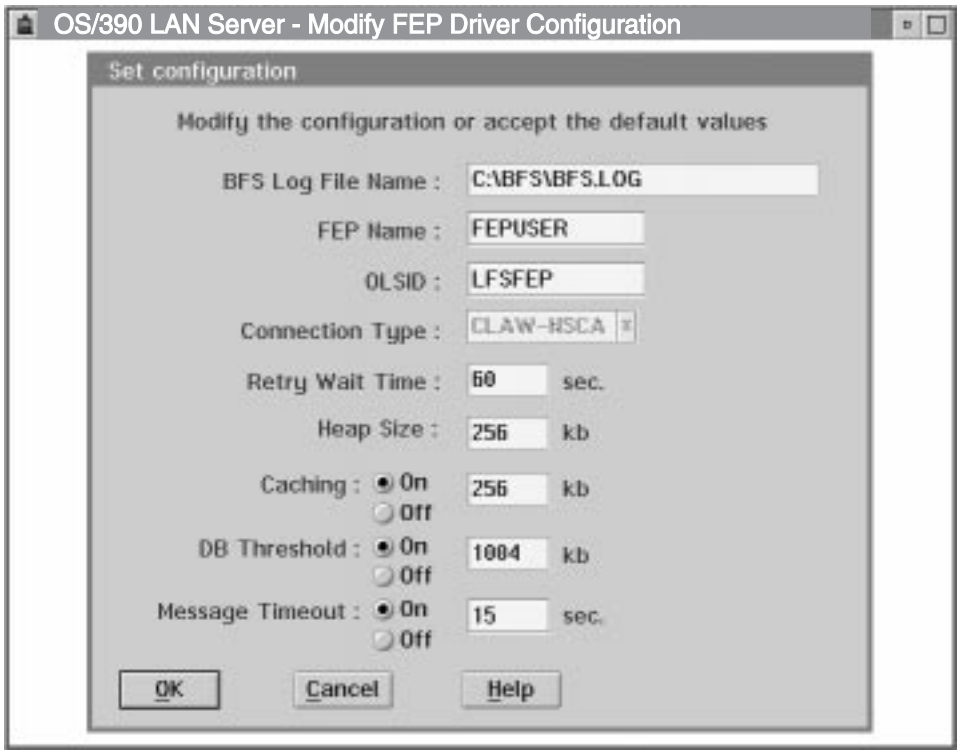


*Figure 13. Set Configuration*

8. **(CLAW-MMC CONNECTIONS ONLY)** On the 'Set configuration' panel, fill in the entry fields using the values from the OS/2 LAN Server Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to start the installation.

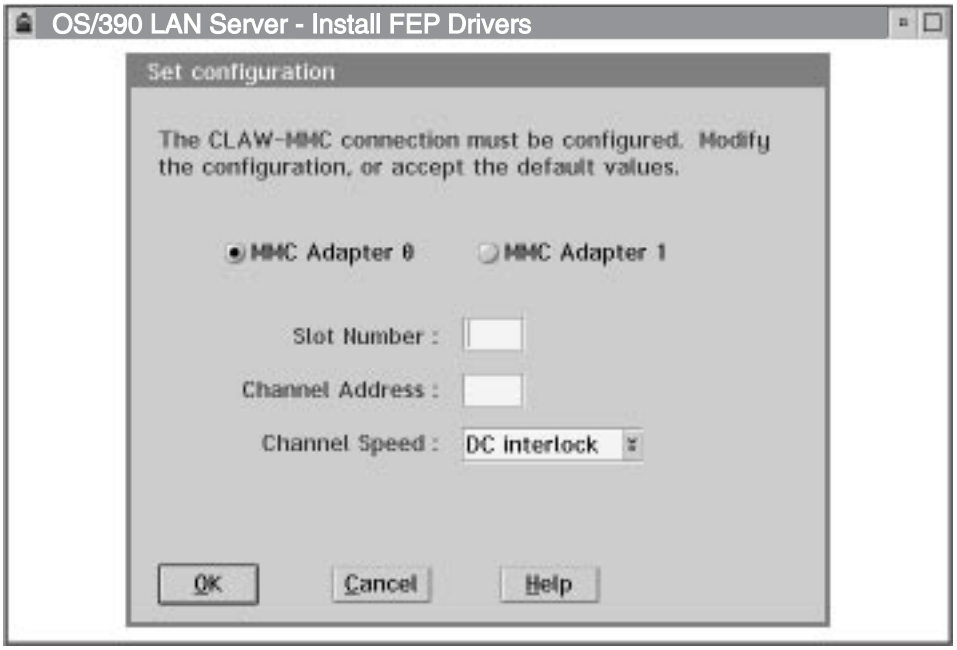


*Figure 14. Set Configuration - CLAW-MMC Connection Only*

9. **(CLAW-NSCA CONNECTIONS ONLY)** On the 'Set configuration' panel, fill in the entry fields using the values from the OS/2 LAN Server Front-End

Processor Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to start the installation.

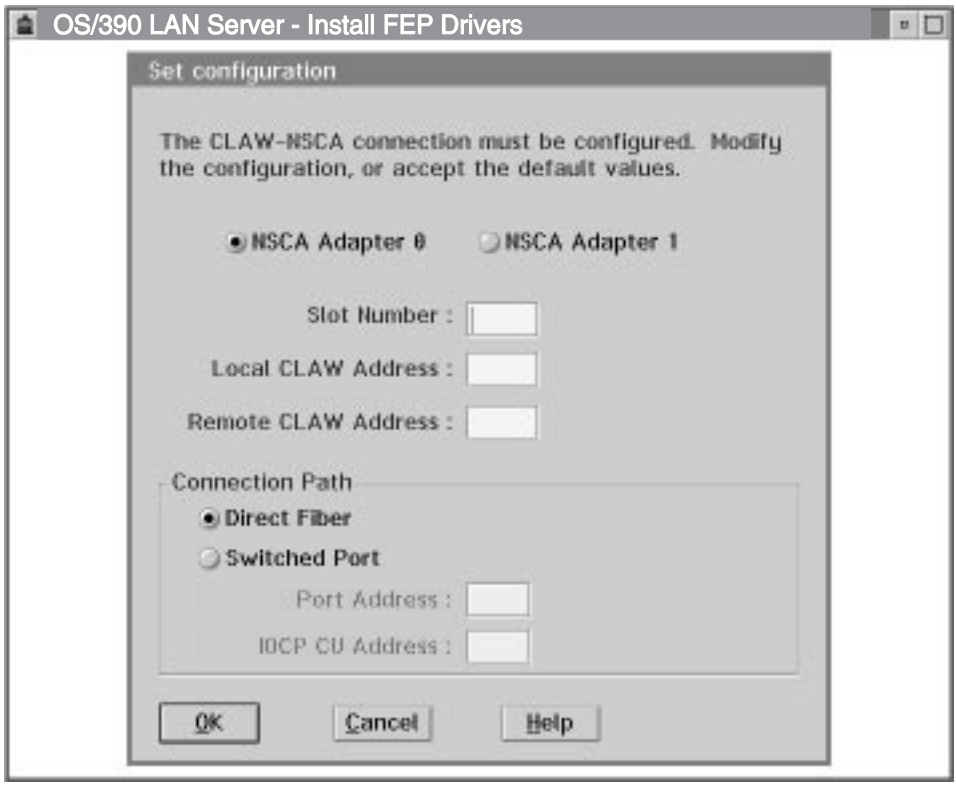


*Figure 15. Set Configuration - CLAW-NSCA Connection Only*

10. When the initial installation is complete, a window will appear indicating that the OS/390 LAN Server FEP drivers have been modified and that some new files are being automatically created. When this process is completed, the 'IBMLAN.INI modification' panel will appear.
11. Make a selection on the 'IBMLAN.INI modification' panel.

    If you select 'Modify IBMLAN.INI automatically', your original IBMLAN.INI will be renamed to IBMLAN.BFS and a new IBMLAN.INI will automatically be created.

    If you select 'Do NOT modify IBMLAN.INI', a file called IBMLAN.NEW will automatically be created. You will need to manually edit your IBMLAN.INI file to reflect what is in the IBMLAN.NEW file before you try to use the front-end processor drivers.

    After you make your selection, click on the 'OK' pushbutton to bring up the 'CONFIG.SYS modification' panel.


*Figure 16. IBMLAN.INI Modification*

12. Make a selection on the 'CONFIG.SYS modification' panel.

    If you select 'Modify CONFIG.SYS automatically', your original CONFIG.SYS will be renamed to CONFIG.BFS and a new CONFIG.SYS will automatically be created.

    If you select 'Do NOT modify CONFIG.SYS', a file called CONFIG.NEW will automatically be created. You will need to manually edit your CONFIG.SYS file to reflect what is in the CONFIG.NEW file before you try to use the front-end processor drivers.

    After you make your selection, click on the 'OK' pushbutton to complete the installation process.


*Figure 17. CONFIG.SYS Modification*

13. When the entire front-end processor driver configuration modification is complete, you will see a panel indicating the front-end processor drivers have been successfully re-configured. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Replacing OS/2 LAN Server Front-End Processor Drivers

Before you begin the formal replacement process for the OS/390 LAN Server FEP drivers, complete the OS/2 LAN Server Front-End Processor Replacement Worksheet, Table 4 below.

*Table 4. OS/2 LAN Server Front-End Processor Replacement Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| Source of Update | | This is the location of the replacement code. If you are replacing the front-end processor drivers with code that is on a diskette, type ***A:***. |
| FEP Configuration File Name | | This file is typically named BFS.INI. The BFS.INI file defines the characteristics of the connection for the OS/2 LAN Server. Specify the drive and path to the BFS.INI file (or to your FEP configuration file, if you have renamed BFS.INI to another name). |

To replace the front-end processor drivers, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive for a local replacement.

For the English version:

- If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

  OS/390 LAN Server: English
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (1 of 2)

  OS/390 LAN Server: English
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (2 of 2)

For the Japanese version:

- If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

  OS/390 LAN Server: Japanese
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (1 of 2)

  OS/390 LAN Server: Japanese
  OS/2 LAN Srvr 3.0/4.0/5.0 FEP
  5647-A01 V2R5M0
  Install Diskette (2 of 2)

**Note:**

You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSINST*** for a local replacement, or

   ***drive:\BFSINST*** to replace from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Replace existing FEP drivers'. This will bring up the 'Replace FEP drivers' panel.


*Figure 18. OS/390 LAN Server Menu - Select Replace Existing FEP Drives*

6. On the 'Replace FEP drivers' panel, fill in the entry fields. Use the values on the OS/2 LAN Server Front-End Processor Replacement Worksheet, Table 4 on page 58, to fill in the fields. Click on the 'OK' pushbutton when you are done.

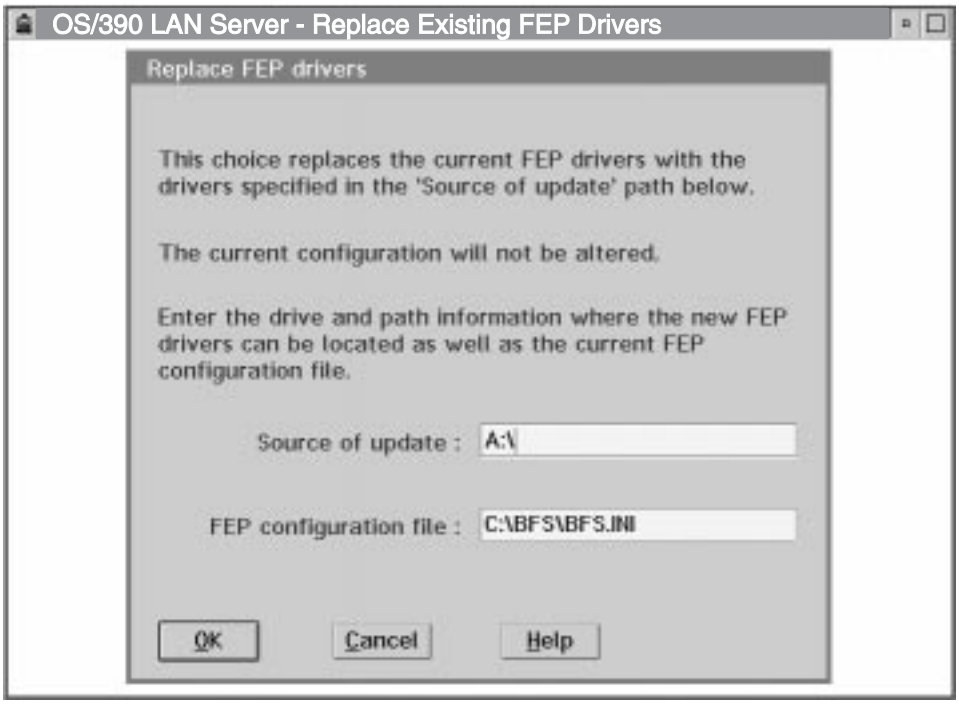


*Figure 19. Replace Front-End Processor Drivers*

7. If the BFSLINK network service is active, a panel will appear. If you wish to stop the BFSLINK service so that you can continue with the front-end processor driver update, click on the 'OK' pushbutton.
8. While the installation progresses, you will see a panel indicating which files are being updated and what percent of the replacement is complete.
9. When the entire front-end processor driver configuration replacement is complete, you will see a panel indicating the drivers were successfully replaced. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Removing OS/2 LAN Server Front-End Processor Drivers

Before you begin the formal removal process of the OS/390 LAN Server FEP drivers, complete the OS/2 LAN Server Front-End Processor Removal Worksheet, Table 5 below.

*Table 5. OS/2 LAN Server Front-End Processor Removal Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| FEP Driver Location | | This is the location of the unpacked front-end processor driver code. |
| OS/2 LAN Server Directory | | This is the path to the OS/2 LAN Server code, of which the IBMLAN.INI file is a part. Fill in the value of the OS/2 LAN Server root directory. |

To remove the front-end processor drivers, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive for a local removal.

   For the English version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   For the Japanese version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

| OS/390 LAN Server: Japanese
| OS/2 LAN Srvr 3.0/4.0/5.0 FEP
| 5647-A01 V2R5M0
| Install Diskette (1 of 2)

| OS/390 LAN Server: Japanese
| OS/2 LAN Srvr 3.0/4.0/5.0 FEP
| 5647-A01 V2R5M0
| Install Diskette (2 of 2)

**Note:**

You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\IBFSINST*** for a local removal, or

   ***drive:\IBFSINST*** to remove from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Remove FEP drivers from this workstation'. This will bring up the 'Remove FEP drivers' panel.


*Figure 20. OS/390 LAN Server Menu - Select Remove FEP Drivers from this Workstation*

6. On the 'Remove FEP drivers' panel, fill in the entry fields. Use the values on the OS/2 LAN Server Front-End Processor Removal Worksheet, Table 5 on page 61, to fill in the fields. Click on the 'OK' pushbutton when you are done.

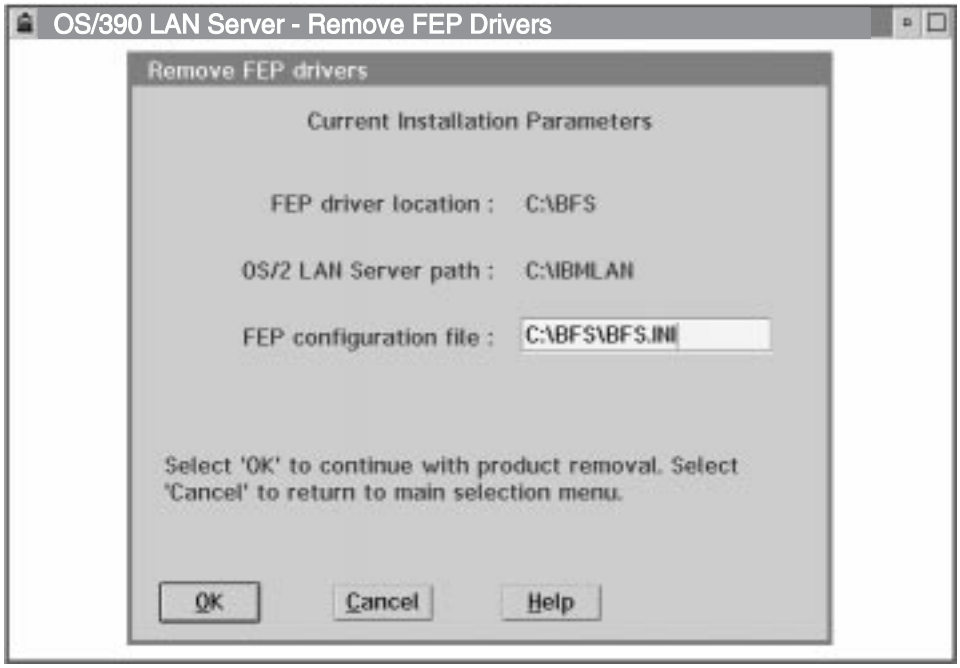


*Figure 21. Remove Front-End Processor Drivers*

7. You will see a confirmation panel, asking if you are certain you wish to remove the front-end processor drivers. Click on the 'OK' pushbutton to start the front-end processor driver removal.

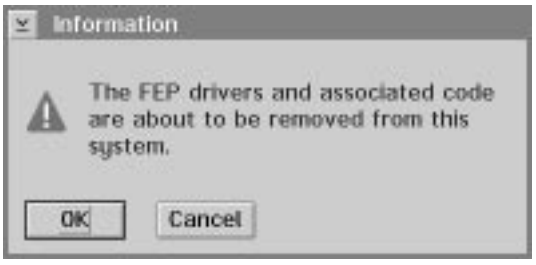


*Figure 22. Information Panel - FEP Drivers are About to be Removed*

8. When the initial removal is complete, a window will appear indicating that the OS/390 LAN Server FEP drivers have been removed and that some files are being automatically deleted. When this process is complete, the 'IBMLAN.INI modification' panel will appear.
9. Make a selection on the 'IBMLAN.INI modification' panel.

   If you select 'Modify IBMLAN.INI automatically', your original IBMLAN.INI will be renamed to IBMLAN.BFX, and a new IBMLAN.INI that does not reference the front-end processor drivers will automatically be created.

   If you select 'Do NOT modify IBMLAN.INI', a file called IBMLAN.NEW will automatically be created. You will need to manually edit your IBMLAN.INI file to reflect what is in the IBMLAN.NEW file before you try to use other programs.

   Click on the 'OK' pushbutton to bring up the 'CONFIG.SYS modification' panel.

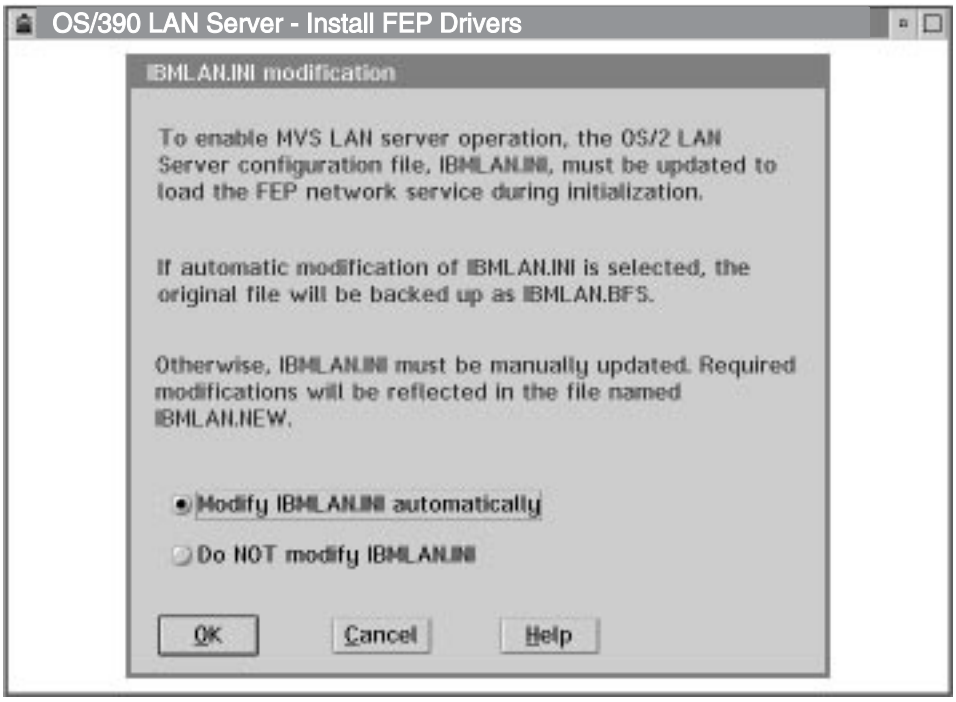


*Figure 23. IBMLAN.INI Modification*

10. Make a selection on the 'CONFIG.SYS modification' panel.

    If you select 'Modify CONFIG.SYS automatically', your original CONFIG.SYS will be renamed to CONFIG.BFS and a new CONFIG.SYS that does not reference the front-end processor drivers will automatically be created.

    If you select 'Do NOT modify CONFIG.SYS', a file called CONFIG.NEW will automatically be created. You will need to manually edit your CONFIG.SYS file to reflect what is in the CONFIG.NEW file before you try to use other programs.

    Click on the 'OK' pushbutton to complete the removal process.

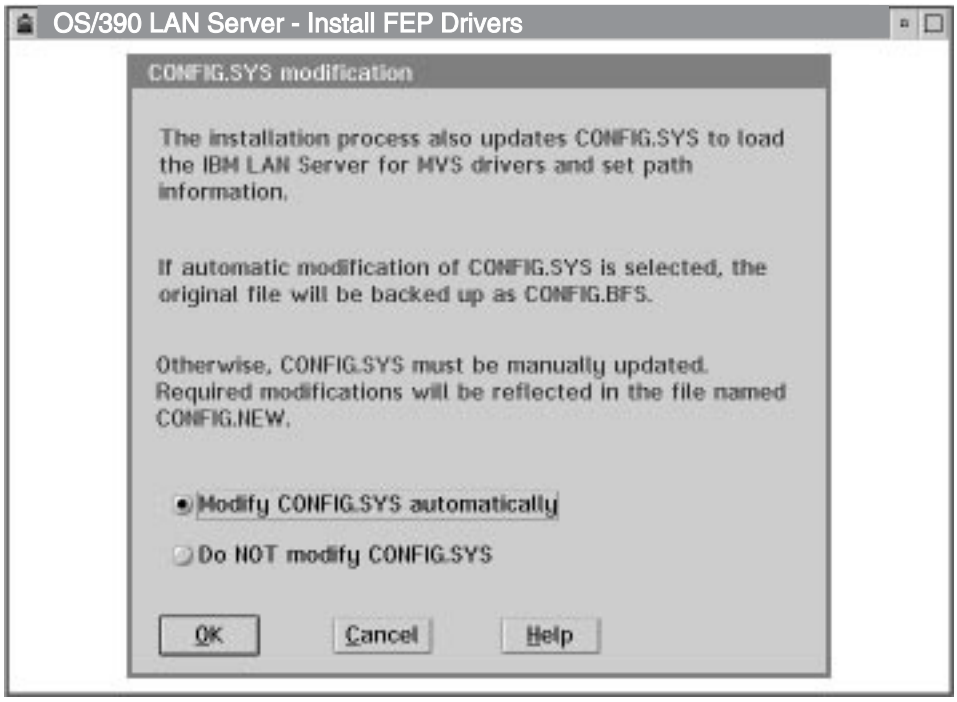


*Figure 24. CONFIG.SYS Modification*

11. When the entire front-end processor driver removal is complete, you will see a panel indicating the drivers and associated code were removed from the system. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

**Note!**

After the OS/390 LAN Server front-end processor drivers have been removed from the workstation, it is the system administrator's responsibility to remove any prior references to the FEP name, OLSID, and channel addresses from the CLAW configuration files.

## Creating an OS/2 LAN Server Front-End Processor Installation Diskette

This process creates a copy of the packed OS/390 LAN Server FEP installation code packed files on a high-capacity 3.5" diskette.

Before you begin the formal front-end processor installation diskette creation process for the OS/390 LAN Server front-end processor drivers, obtain a high-capacity 3.5" blank, formatted diskette, and complete the Create OS/2 LAN Server Front-End Processor Installation Diskette Worksheet, Table 6 below.

| *Table 6. Create OS/2 LAN Server Front-End Processor Installation Diskette Worksheet* | | |
|---|---|---|
| **Information Needed** | **Your Value** | **Where to Find It** |
| **For All Connection Types** | | |
| Installation Source | | This is the location of the OS/390 LAN Server source code, either on your local workstation, or on a fixed disk within the network. |
| Target Diskette Drive | | This is the target diskette drive location where you want the FEP driver code to be copied. Type the diskette drive letter. |

## Creating an OS/2 LAN Server Front-End Processor Installation Diskette Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

To copy the OS/390 LAN Server software that runs the front-end processor, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive to create a diskette locally.

   For the English version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   For the Japanese version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

| OS/390 LAN Server: Japanese
| OS/2 LAN Srvr 3.0/4.0/5.0 FEP
| 5647-A01 V2R5M0
| Install Diskette (2 of 2)

**Note:**

You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSINST*** to create a diskette locally, or

   ***drive:\BFSINST*** to create a diskette from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Create FEP installation diskette'. This will bring up the 'Create FEP Installation Diskette' panel.


*Figure 25. OS/390 LAN Server Menu - Select Create FEP Installation Diskette*

6. On the 'Create FEP Installation Diskette' panel, fill in the entry fields. Use the values on the OS/390 LAN Server Create OS/2 LAN Server Front-End Processor Installation Diskette Worksheet, Table 6 on page 66, to fill in the fields. Then insert a high-capacity 3.5" diskette in the diskette drive. Click on the 'OK' pushbutton when you are done to begin creating the installation diskette.

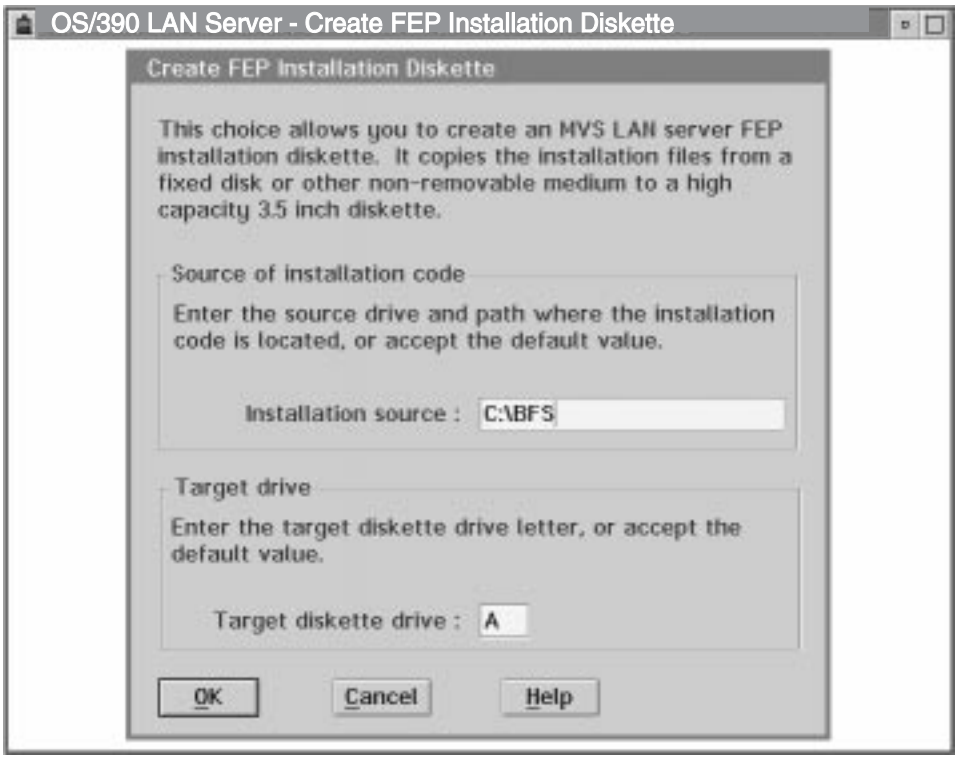


*Figure 26. Create OS/2 LAN Server Front-End Processor Installation Diskette*

7. Before the copying actually begins, the program will verify that all required files are present at the installation source location. While that occurs, the following panel will appear.

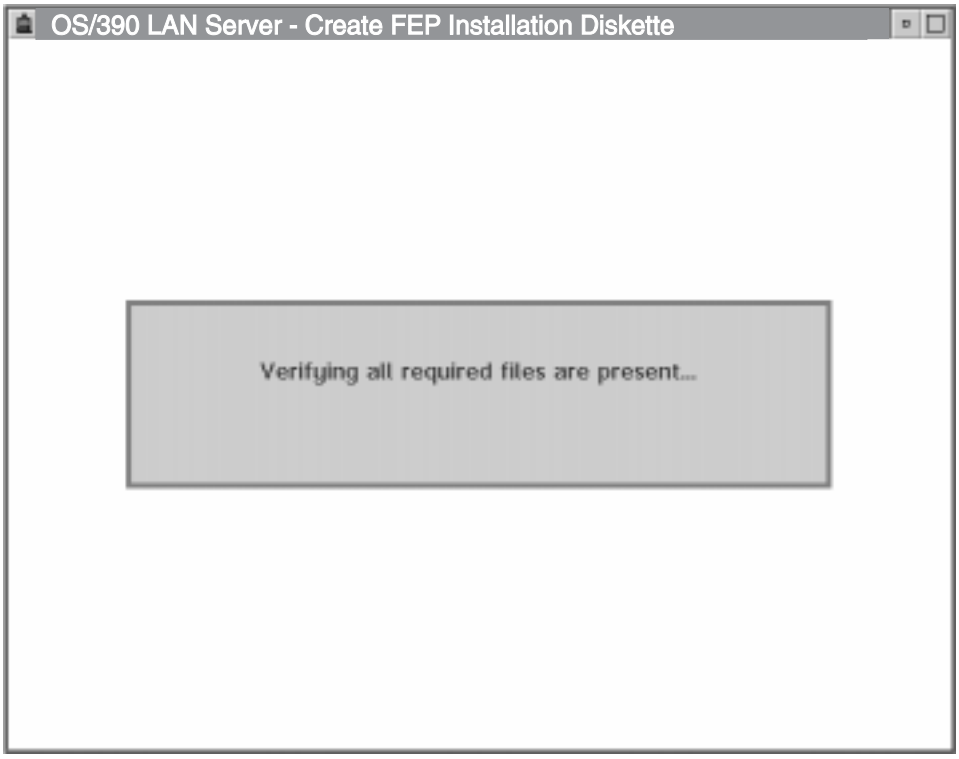


*Figure 27. Verifying All Required Files Are Present*

8. If one or more files cannot be found, a message window will appear. Refer to the Error Log for details on which files were not found.
9. If you didn't insert a high-capacity 3.5 " diskette in the diskette drive, a window would appear. Insert the diskette, then click on the 'OK' pushbutton.
10. While the copy to diskette progresses, you will see this panel indicating which files are being copied and what percent of the copy to diskette is now complete.
11. When the entire FEP driver copy to diskette is complete, you will see a panel. Click on the 'OK' pushbutton.

## Copying OS/2 LAN Server Front-End Processor Installation Code to the Fixed Disk

Before you begin the formal copy to fixed disk process for the OS/390 LAN Server front-end processor drivers, complete the Copy OS/2 LAN Server Front-End Processor Installation Code to Fixed Disk Worksheet, Table 7 below.

*Table 7. Copy OS/2 LAN Server Front-End Processor Installation Code to Fixed Disk Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| Installation Source | | This is the location of the OS/390 LAN Server source code (either on fixed disk or on diskette). Specify the drive and path. |
| Target Drive | | This is the target fixed disk drive location where you want the front-end processor driver code to be copied. Specify the drive and path. |

## Creating Custom Response Files

Before you begin the formal process of creating custom response files for the OS/390 LAN Server FEP drivers, complete the Installation Worksheet, Table 3 on page 40.

This section explains the creation of custom response files using a graphical user interface. To create custom response files using a command-based user interface, refer to “Creating Custom Response Files from a Command-Based Interface” on page 79.

## Creating a Custom Response File Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***“x:\”*** or ***“x.xx”***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

To create a custom OS/390 LAN Server response file for front-end processor installation, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive for a local response file creation.

   For the English version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)
     /lines>

   For the Japanese version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   **Note:**

   > You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSINST*** to create the response file locally, or

   ***drive:\BFSINST*** to create the response file from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Create or use response files'. This will bring up the 'Create or use custom response files' panel.

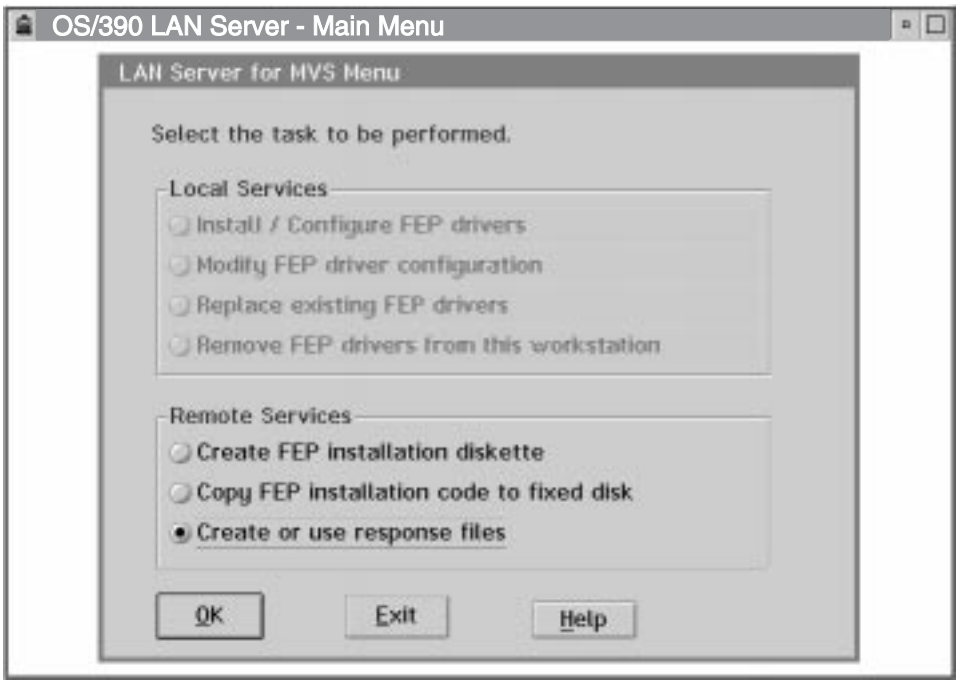


*Figure 28. OS/390 LAN Server Menu - Select Create or Use Response Files*

6. On the 'Create or use custom response files' panel, select 'Create an LS for MVS response file' and click on the 'OK' pushbutton to bring up the 'Create custom response file' panel.

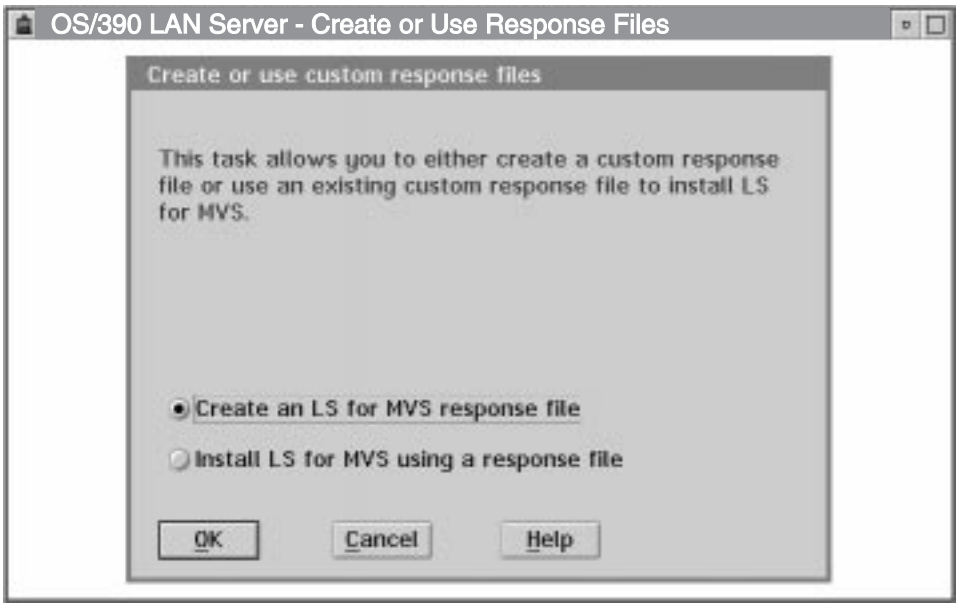


*Figure 29. Create or Use Custom Response Files*

7. On the 'Create custom response file' panel, fill in the entry fields. Use the values on the Installation Worksheet, Table 3 on page 40, to fill in the fields. Click on the 'OK' pushbutton when you are done to bring up the next 'Create custom response file' panel.

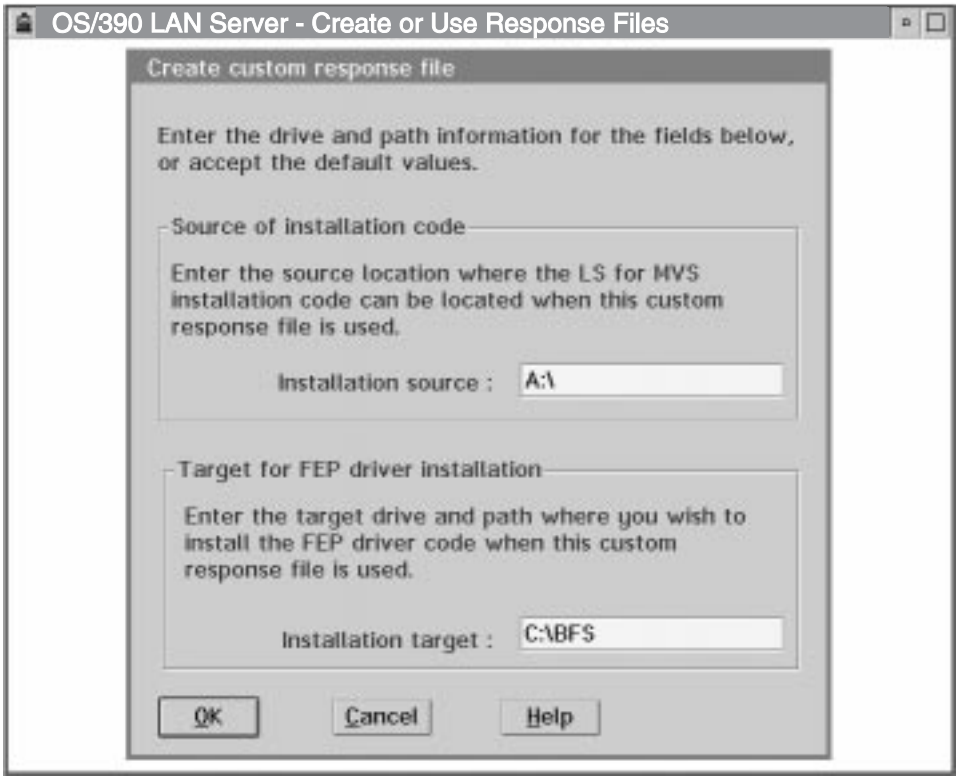


*Figure 30. Create Custom Response File - Drive and Path Information*

8. On this 'Create custom response file' panel, fill in the entry field using the OS/2 LAN Server path value from the Installation Worksheet, Table 3 on page 40. When you are done, click on the 'OK' pushbutton to bring up the 'Set configuration' panel.

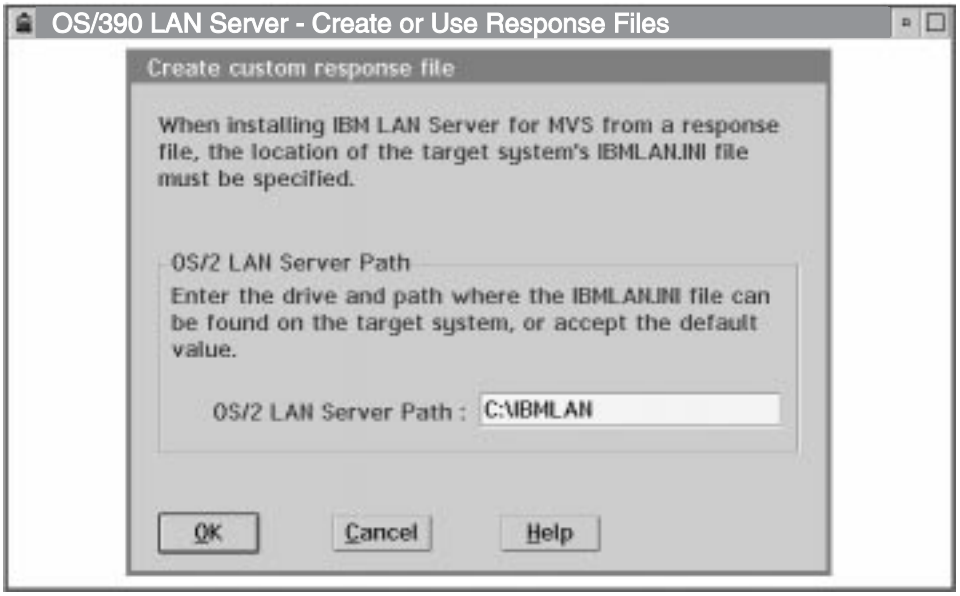


*Figure 31. Create Custom Response File - OS/2 LAN Server Path*

9. On the 'Set configuration' panel, fill in the entry fields using the values from the Installation Worksheet, Table 3 on page 40.

If you are making a PWSCS or CM/2 connection, click on the 'OK' pushbutton when you are done, to bring up the 'Save Response File to Drive' panel.

If you are making a CLAW connection, click on the 'OK' pushbutton to bring up an additional 'Set configuration' panel.

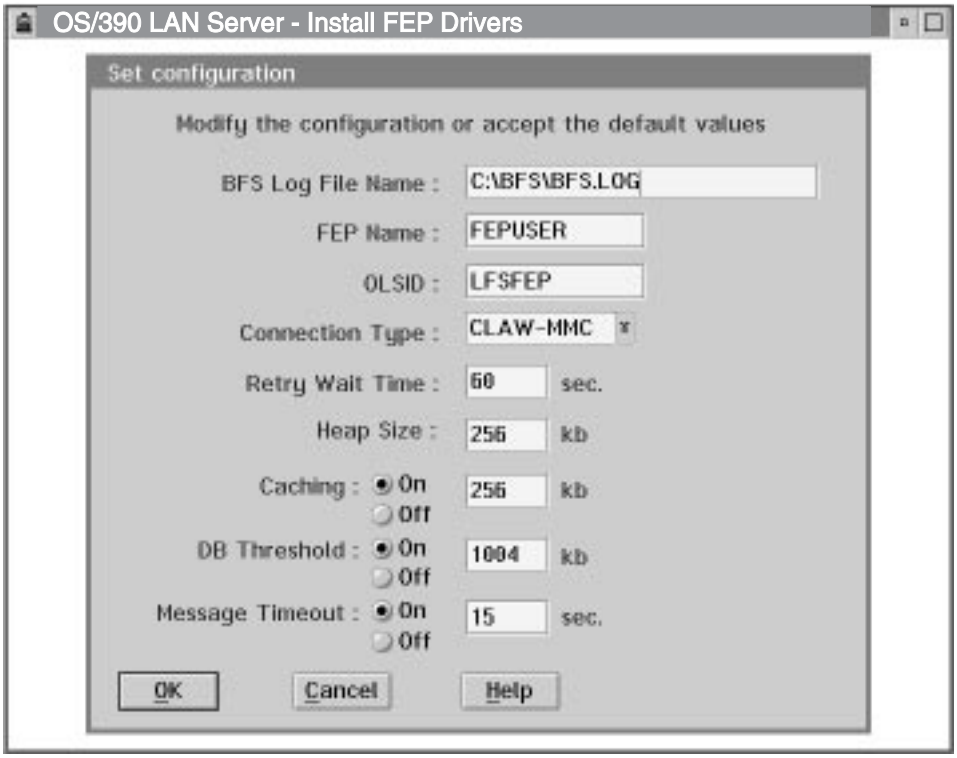


*Figure 32. Set Configuration*

10. **(CLAW-MMC CONNECTIONS ONLY)** On the 'Set configuration' panel, fill in the entry fields using the values from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to bring up the 'Save Response File to Drive' panel.

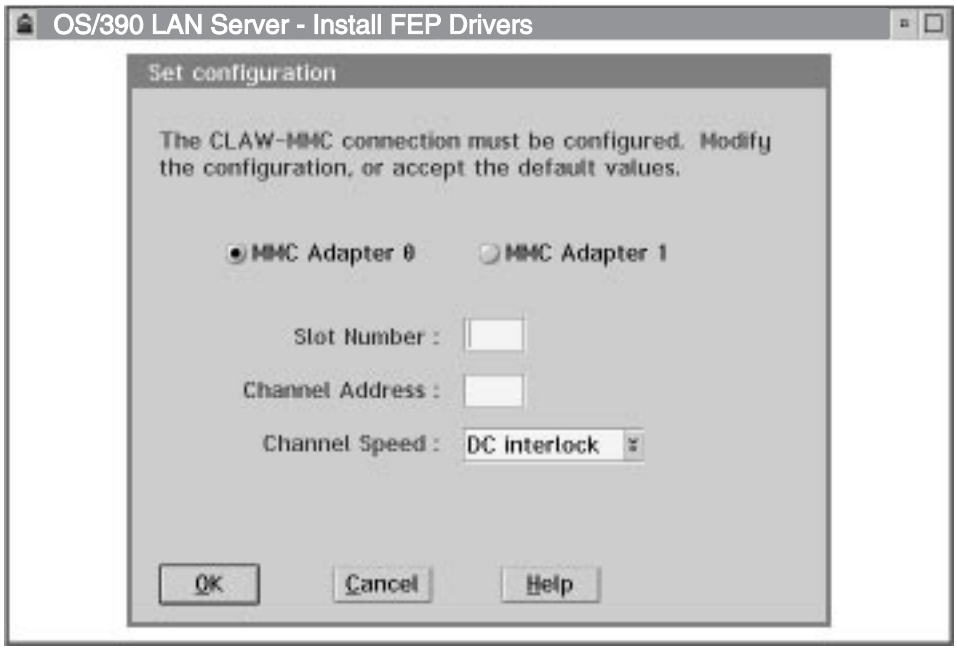


*Figure 33. Set Configuration - CLAW-MMC Connection Only*

11. **(CLAW-NSCA CONNECTIONS ONLY)** On the 'Set configuration' panel, fill in the entry fields using the values from the OS/2 LAN Server Front-End Processor Installation Worksheet, Table 3 on page 40. Click on the 'OK' pushbutton when you are done to bring up the 'Save Response File to Drive' panel.

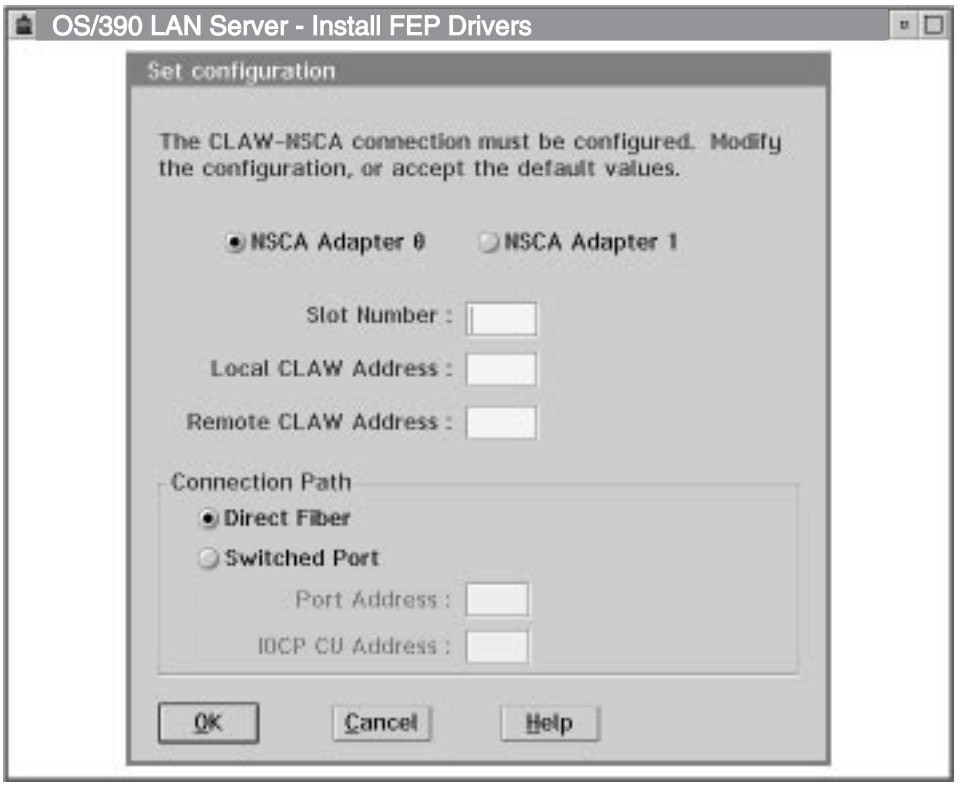


*Figure 34. Set Configuration - CLAW-NSCA Connection Only*

12. On the 'Save Response File to Drive' panel, either type in the drive, path, and file name of the response file in the 'Save as Response File Name' field, or select your response file using the 'Drive', 'Directory', and 'File' menus. The directory specified must already exist on your system. Use the values on the Installation Worksheet, Table 3 on page 40 to fill in the fields. Click on the 'OK' pushbutton to begin the installation process.

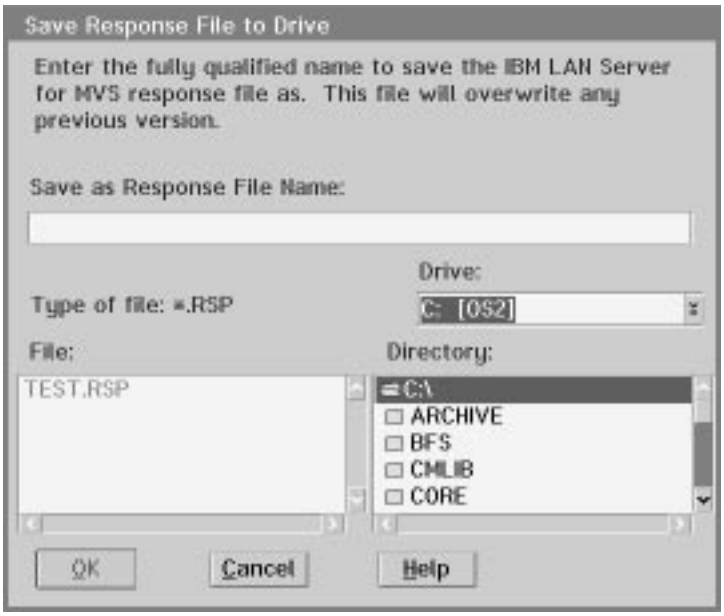


*Figure 35. Save Response File to Drive*

13. When the custom response file has been created, you will see a panel indicating the OS/390 LAN Server custom response file was successfully created. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Using OS/2 Custom Response Files

Before you begin the formal process of using custom response files for the OS/390 LAN Server front-end processor drivers, complete the Using OS/2 Custom Response Files Worksheet, Table 8 below.

*Table 8. Using OS/2 Custom Response Files Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| Response File Name | | This is the drive and path and filename of the custom response file you will use to perform the FEP driver code installation. You will most likely get this filename and path from your LAN Administrator. |

## Using a Custom Response File Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

This response may also be used by a code server for a CID installation.

To use a custom OS/390 LAN Server response file for front-end processor installation, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the correct Installation Diskettes in the A: drive to use response files from your local workstation.

   For the English version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: English
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   For the Japanese version:

   - If the front-end processor has OS/2 LAN Server 3.0/4.0/5.0 installed, choose the diskettes labeled:

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (1 of 2)

     OS/390 LAN Server: Japanese
     OS/2 LAN Srvr 3.0/4.0/5.0 FEP
     5647-A01 V2R5M0
     Install Diskette (2 of 2)

   **Note:**

   You must install OS/2 LAN Server on the front-end processor before installing OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled. If you are delivering multimedia assets, you must also install IBM Ultimedia on the front-end processor before installing OS/390 LAN Server front-end processor code.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSINST*** to use the response file locally, or

   ***drive:\BFSINST*** to use the response file from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Create or use response files'. This will bring up the 'Create or use custom response files' panel.

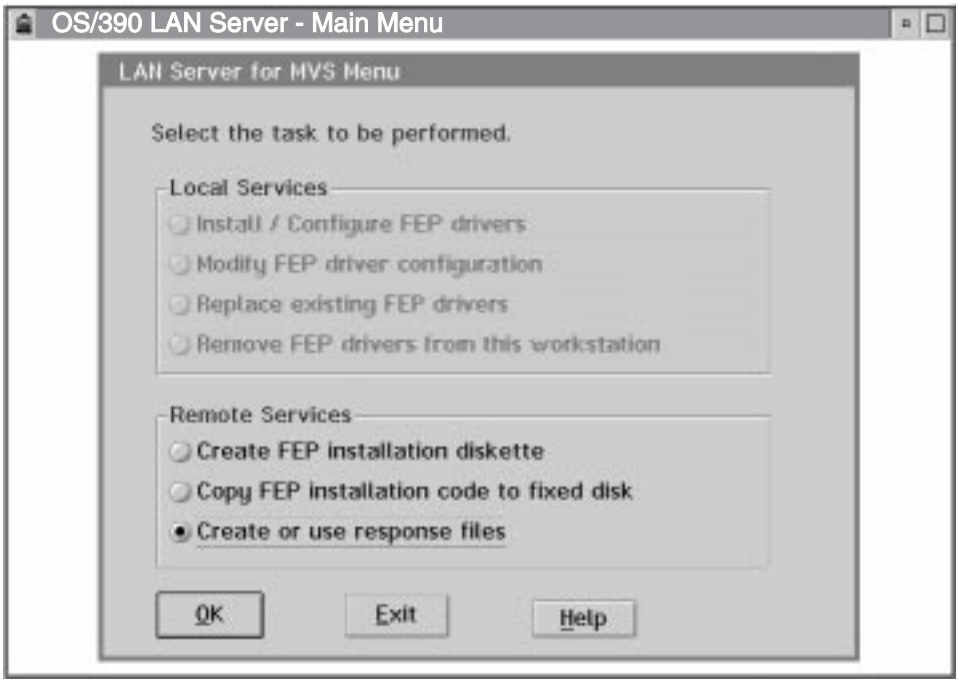


*Figure 36. OS/390 LAN Server Menu - Select Create or Use Response Files*

6. On the 'Create or use custom response files' panel, select 'Install LS for MVS using a response file' and click on the 'OK' pushbutton to bring up the 'Install Using a Response File' panel.

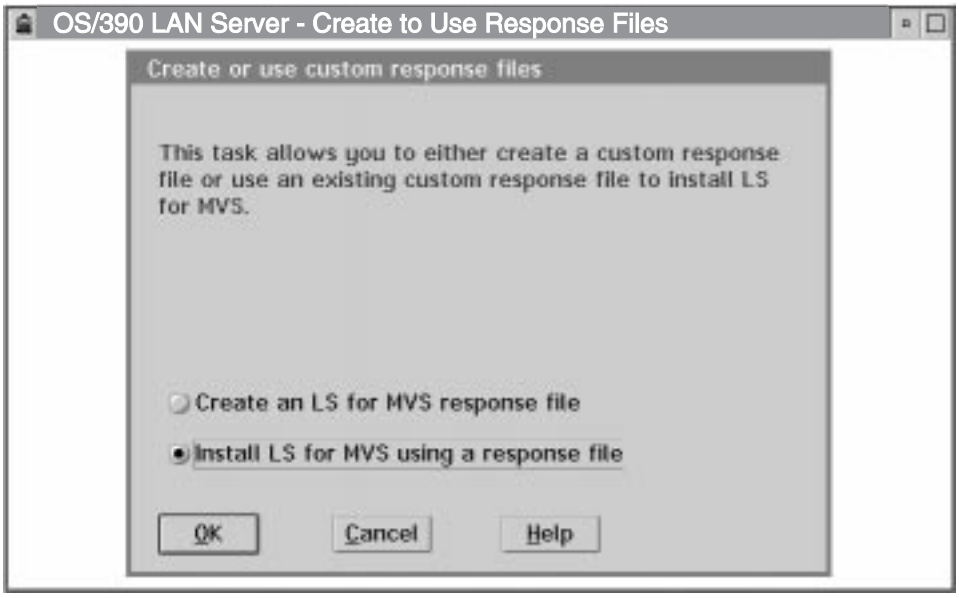


*Figure 37. Create or Use Custom Response Files*

7. On the 'Install Using a Response File' panel, either type in the drive, path, and filename of the response file in the 'Open Response File Name' field, or select your response file using the 'Drive', 'Directory', and 'File' menus. Use the values on the Using OS/2 Custom Response Files Worksheet, Table 8 on page 75, to fill in the fields. Click on the 'OK' pushbutton to begin the installation process.

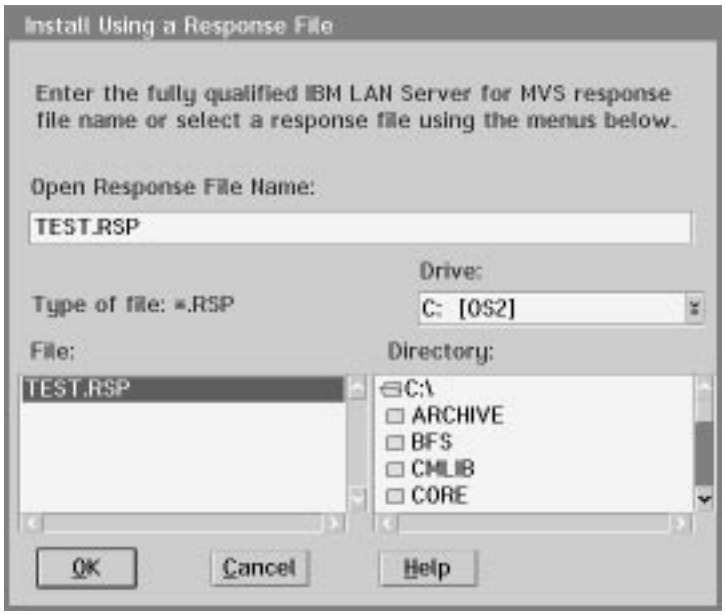


*Figure 38. Install Using a Response File*

8. While the installation progresses, you will see a panel indicating that files are being copied.
9. When the entire FEP driver installation is complete, you will see a panel indicating the FEP drivers and associated code were successfully installed on

the system. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Creating Custom Response Files from a Command-Based Interface

OS/390 LAN Server can also be installed with a response file through the OS/2 command line rather than traversing the GUI installation interface. This feature enables the CID unattended install mode of the installation program. The installation command syntax to enable this mode is:

```
BFSINST /R:d:\path\fname1.ext /S:d:\path /T:d:\path
        /L1:d:\path\fname2.ext /L2:d:*.path\fname3.ext
```

## Parameters and Descriptions

**/R:** The value supplied is a fully qualified specification (drive, path, filename, and extension). The value is the name of the response file supported for BFSINST. The file name is expected to be in the format of *.RSP, where '*' refers to any valid filename and 'RSP' is that file extension. This is a required parameter and BFSINST will terminate if it is omitted.

**/S:** The value supplied contains the source path where the File Services FEP installation code is to be installed from. This parameter will override the 'LFS_INSTALL_FROM' value specified in the response file. It is an optional parameter.

**/T:** The value supplied contains the destination path where the File Services FEP installation code is to be installed to. This parameter will override the 'LFS_INSTALL_TO' value specified in the response file. It is an optional parameter.

**/L1:** The value supplied contains the fully qualified filename (drive, path, filename and extension) of the installation error log file. If an invalid name is specified, or if this file could not be created, the installation error logging will occur to the default filename and location (\OS2\INSTALL\BFSINERR.LOG).

**/L2:** The value supplied contains the fully qualified filename (drive, path, filename and extension) of the installation history log file. If an invalid name is specified, or if this file could not be created, the installation history logging will occur to the default filename and location (\OS2\INSTALL\BFSINHST.LOG).

## Return Codes

BFSINST will issue 1 of 2 possible return codes consistent with software distribution management (SDM) conventions. The currently supported return codes and their definitions are explained below:

| Return Code (2 byte Hex) | Description |
|---|---|
| **FE 00** | Successful program termination - Reboot and do not invoke the install again. |
| **FE 12** | Successful program termination, but severe error messages logged - Check log, correct the error(s), and invoke the install program again. |

## BFSINST Response File Format

BFSINST response files are ASCII-based files which contain keyword=value pairs and comments. Comments are generally designated by lines which have an asterisk(*) or a semicolon(:) in the first column. Any non-keyword will be ignored as well. The complete list of keywords is listed below:

**Keyword** **Description**

**LFS_INSTALL_FROM** This keyword specifies where the BFSINST program is to search for the front-end processor packed files to install to the target system. This is a required parameter.

**LFS_INSTALL_TO** This keyword specifies where the front-end processor executable code is to be installed on the system executing the BFSINST installation program. This is a required parameter.

**LFS_INSTALL_INI** This keyword specifies the location on the target system where the OS/2 LAN Server software initialization file (IBMLAN.INI) resides. This is a required parameter.

**BFS_LOG_FILE** This keyword specifies the name of the file (on the front-end processor) to be used to collect log and trace data for OS/390 LAN Server activities. This is an optional parameter. If this parameter is not specified, the default value of C:\BFS\BFS.LOG will be used for this file.

**FEP_NAME** This keyword specifies the name of the front-end processor that is used to connect with host programs. Only alphanumeric characters or '#', '$', '@', '.', '+', or '-' are valid. A maximum of 8 characters is permitted. This is a required parameter.

**OLSID** This keyword specifies the symbolic destination name of a global resource declared by OS/390 LAN Server in a server virtual machine. Only alphanumeric characters or '#', '$', '@', '.', '+', or '-' are valid. A maximum of 8 characters is permitted. This is a required parameter.

**CONNECTION** This keyword specifies the type of connection between the front-end processor and the host system This keyword may take one of three values - 'PWSCS', 'CLAW', or 'CM/2'. If this parameter is omitted, a PWSCS connection will be used.

**RETRY_WAIT_TIME** This keyword specifies the number of seconds the front-end processor should wait between retrying to contact the host resource. The value may range from 1 to 3600. If this parameter is omitted, the default value of '60' will be used.

**HEAP_SIZE** This indicates the size of the heap region, an area of free storage from which an application can dynamically allocate blocks of storage. This value defaults to 64KB.

**CACHING** This keyword specifies whether caching is active or inactive on the front-end processor. This value may range from 256 to 16384 (kbytes), or be set to 'OFF' or 'ON'. If this value is set to 'ON', a value of 256 will be used. This is an optional parameter, and if omitted, caching will be in active.

**DB_THRESHOLD** This keyword specifies a file size above which an alternate caching scheme will be used. The threshold file size is a multiple of 1024 bytes. This value can be a maximum of 7 digits in size.

This is an optional parameter, and if omitted, it will default to '1004'.

**MESSAGE_TIMEOUT** This keyword specifies whether messages should be displayed at the front-end processor console, and if so, for how long. The value may range from 0 to 60 seconds. This is an optional parameter, and if omitted, will default to '15'.

**ADAPTER_NUMBER** This keyword specifies which microchannel adapter is to be used if a 'CLAW' connection is used for front-end processor communication. The value may be either '0' or '1'. This is a required parameter when a 'CLAW' connection is used; otherwise it is ignored.

**DD_NAME** This keyword specifies to the host system which physical connectivity the CLAW link is using. The value may be either '$PSCA' for a CLAW-MMC connection type, or '$NSCA' for a CLAW-NSCA connect type. This is a required parameter when a CLAW-NSCA connection is used. If this parameter is omitted, and 'CONNECTION' = CLAW is specified, this value will default to '$PSCA'; otherwise it is ignored.

**CLAW_ADDRESS** This keyword specifies the 370 subchannels which are to be used by the CLAW-attached adapter. This value must be any even, 2 digit, hexadecimal address. This is a required parameter for CLAW connections; otherwise it is ignored.

**ADAPTER_SLOT** This keyword specifies the workstation slot number where either the MMC or NSCA adapter card is installed. This is a required 1 digit parameter for a CLAW connection; otherwise it is ignored.

**CHANNEL_SPEED** This keyword specifies whether the CLAW connection with the MMC adapter is to run in DC interlock or streaming mode. The values may range from 0 to 4, corresponding to DC interlock, 1.9 Mb/sec, 2.7 Mb/sec, 3.4 Mb/sec, and 4.5 Mb/sec. This is a required parameter for a CLAW-MMC connection type; otherwise it is ignored.

**REMOTE_ADDRESS** This keyword specifies the hexadecimal address of the fiber connection as it is known on the ES/9000 processor. The value must be any even, 2 digit, hexadecimal address. This is a required parameter when a CLAW-NSCA connection is specified; otherwise it is ignored.

**DIRECT_FIBER** This keyword specifies what data will be used when writing the CLAW-NSCA configuration file. If the value is 'OFF', the data specified by the CU_ADDRESS and PORT_ADDRESS keywords will be used. If the value is 'ON', the value '010' will be used. This is a required parameter when a CLAW-NSCA connection is specified; otherwise it is ignored.

**PORT_ADDRESS** This keyword specifies the port number of the switch connection to the ESCON channel. The value must be any 2 digit hexadecimal address. This is a required parameter if DIRECT_FIBER = 'OFF'.

**CU_ADDRESS** This keyword specifies the value on the CUADD parameter of the CNTLUNIT statement for the ESCON channel in the IOCP table for the ES/9000. The value must be any 1 digit hexadecimal value. This is a required parameter if DIRECT_FIBER = 'OFF'.

## Sample Response File

```
Example 1 : Suppose you want to create a PWSCS connected front-end
            processor named 'FEPTEST', OLSID named 'OLSIDTST', and
            512kb reserved for the cache size.

;
;  OS/390 LAN Server - Response file
;

LFS_INSTALL_FROM = A:\
LFS_INSTALL_TO   = C:\BFS
LFS_INSTALL_INI  = C:\IBMLAN
BFS_LOG_FILE     = C:\BFS\BFS.LOG
FEP_NAME         = FEPTEST
OLSID            = OLSIDTST
CONNECTION       = PWSCS
RETRY_WAIT_TIME  = 60
HEAP_SIZE        = 64
CACHING          = 512
DB_THRESHOLD     = 1004
MESSAGE_TIMEOUT  = 15

Example 2 : Suppose you want to create a CLAW-MMC connected front-end
            processor named 'FEPTEST', OLSID named 'OLSIDTST', 256kb
            reserved for the cache size, a channel speed of 2.7Mb/sec,
            a single MMC adapter installed in slot number 4, and a
            channel address of x'A2'.

;
;  OS/390 LAN Server - Response file
;

LFS_INSTALL_FROM = A:\
LFS_INSTALL_TO   = C:\BFS
LFS_INSTALL_INI  = C:\IBMLAN
BFS_LOG_FILE     = C:\BFS\BFS.LOG
FEP_NAME         = FEPTEST
OLSID            = OLSIDTST
CONNECTION       = CLAW
RETRY_WAIT_TIME  = 60
HEAP_SIZE        = 64
CACHING          = 256
DB_THRESHOLD     = 1004
MESSAGE_TIMEOUT  = 15
CLAW_ADDRESS     = A2
ADAPTER_SLOT     = 4
CHANNEL_SPEED    = 2
DD_NAME          = $PSCA       (optional)
ADAPTER_NUMBER   = 0


Example 3 : Suppose you want to create a CLAW-NSCA connected front-end
```

```
                processor named 'FEPTEST', OLSID named 'OLSIDTST', 256kb
                reserved for the cache size, the double buffer threshold
                disabled, a local channel address of x'C4', a remote channel
                address of x'30', a port address of x'6C', and IO control
                unit parameter of 5.

                The target system has the OS/2 LAN Server software installed
                on the 'D' drive, and the front-end processor code is to be
                installed to the 'E:\BFS' drive.  The system also has
                access to another computer's drive where the installation
                code is located and has accessed that drive as 'Z:'.

;
;  OS/390 LAN Server - Response file
;

LFS_INSTALL_FROM = Z:\
LFS_INSTALL_TO   = E:\BFS
LFS_INSTALL_INI  = D:\IBMLAN
BFS_LOG_FILE     = E:\BFS\BFS.LOG
FEP_NAME         = FEPTEST
OLSID            = OLSIDTST
CONNECTION       = CLAW
RETRY_WAIT_TIME  = 60
HEAP_SIZE        = 64
CACHING          = 256
DB_THRESHOLD     = OFF
MESSAGE_TIMEOUT  = 15
CLAW_ADDRESS     = C4
REMOTE_ADDRESS   = 30
ADAPTER_SLOT     = 2
DIRECT_FIBER     = OFF
PORT_ADDRESS     = 6C
CU_ADDRESS       = 5
DD_NAME          = $NSCA
ADAPTER_NUMBER   = 0
```

## Error and History Logging

During either attended or unattended (CID) installation, a history file shall be created. The default name for this file is BFSINHST.LOG and will be located in the system's \OS2\INSTALL directory. This file records all significant events of each of the OS/390 LAN Server options. The default filename and location may only be changed during a command line (unattended) installation as specified by the /L2 parameter.

If an error is encountered during any OS/390 LAN Server installation/ configuration task, details concerning the error shall be logged. The default name for this file is BFSINERR.LOG and will be located in the system's \OS2\INSTALL directory. The default filename and location may only be changed during a command line (unattended) installation as specified by the /L1 parameter.

# Performance Tuning

## Introduction

To optimize OS/390 LAN Server front-end processor performance, it is important to understand the relationship between LAN Server for OS/2 and OS/390 LAN Server front-end processor code.

When a file services request is redirected to the front-end processor, OS/2 LAN Server first receives the request. It then passes the request to the OS/390 LAN Server front-end processor code, which then sends the request to the OS/390 LAN Server host code. When the request is fulfilled by the host code, the OS/390 LAN Server front-end processor receives the results from the host; then passes the results back to the requesting client.

If you are delivering multimedia assets, LAN Server Ultimedia code must be installed on the front-end processor. The OS/390 LAN Server front-end processor code uses the LAN Server Ultimedia code to manage bandwidth on LAN.

## NSCA Adapter (Hardware Settings)

Ensure that the **Preemption Timer** is set to 1.0 microsecond (usec), which is the default. **Do not set this to any value other than the 1.0 default.** Change the **Fairness Control** to **disable**.

## OS/2 LAN Server Parameters

Since the OS/2 LAN Server code performs front-end processing before the client request is handed to the front-end processor code, the tuning of certain OS/2 LAN Server parameters can affect OS/390 LAN Server performance. Specifically:

- IBMLAN.INI - Networks Section

  *x1* variable in the *net*parameter - Since OS/2 LAN Server is the network interface for the front-end processor, this parameter is applicable. Follow the directions for OS/2 LAN Server.
  *x2* variable in the *net*parameter - Since OS/2 LAN Server is the network interface for the front-end processor, this parameter is applicable. Follow the directions for OS/2 LAN Server.

- IBMLAN.INI - Requester Section

  *Maxcmds* - Set this to a minimum of **32**.
  *sesstimeout* - Set this to a minimum of **180**.

- IBMLAN.INI - Server Section

  *autodisconnect* - When a session is disconnected from OS/2 LAN Server, it is also disconnected from OS/390 LAN Server. Follow the directions for OS/2 LAN Server.
  *maxconnections* - OS/390 LAN Server front-end processor code does not use this parameter. The maximum number of connections to OS/390 LAN Server shares is 2048.

  OS/390 LAN Server connections do not count against the OS/2 LAN Server limits.

*maxlocks* - This parameter is not applicable to OS/390 LAN Server resources. Byte range locking is maintained by the OS/390 LAN Server host code, not the front-end processor code.
*maxopens* - This parameter is not applicable to OS/390 LAN Server resources. The number of opens is unlimited, but the OS/390 LAN Server consumes some of its heap for each open file; so in practice, the number of opens is limited by the OS/390 LAN Server front-end processor code heap. Additionally, storage at the OS/390 host is consumed by open file control blocks, placing a practical limit on the number of open files.

OS/390 LAN Server open files do not count against the OS/2 LAN Server limits.
*maxsearches* - This parameter is not applicable to OS/390 LAN Server resources. Searches are performed by the OS/390 LAN Server host code, not the front-end processor code.
*maxsessopens* -This parameter is not applicable to OS/390 LAN Server resources. OS/390 LAN Server open files do not count against the OS/2 LAN Server limits.
*maxsessreqs* - This parameter is not applicable to OS/390 LAN Serverresources. OS/390 LAN Server open files do not count against the OS/2 LAN.
*maxshares* - OS/390 LAN Server shares do count against the OS/2 LAN Server limits. Hence, you must account for OS/390 LAN Server resources when setting the OS/2 LAN Server parameter.
*maxusers* - Since this is a client connection parameter, clients that NET USE to an OS/390 LAN Server resource, count against this OS/2 LAN Server parameter. Follow the directions for OS/2 LAN Server.
*numbigbuf* - This parameter is not applicable to OS/390 LAN Server resources. OS/390 LAN Server host code and front-end processor code have their own buffering scheme.
*numreqbuf* - In addition to the buffers required by OS/2 LAN Server to receive the file services requests from the clients, OS/390 LAN Server front-end processor code consumes additional buffers when serving OS/390 LAN Server resources. You should allocate four buffers per requester of OS/390 LAN Server resources (OS/2 LAN Server resource users are recommended to have 2 buffers). Request buffer shortages generally result in slow performance. **Set this to a minimum of 150**.
*sizreqbuf* - Follow the directions for OS/2 LAN Server.
*srvheuristics* - All heuristics described for OS/2 LAN Server are applicable to OS/390 LAN Server. **The only heuristic that should be altered from the default is position 15. The value should be set to 9.** Since OS/390 LAN Server opportunistic locking strategy involving multiple front-end processors is more complex than OS/2 LAN Server's, the timeout should be higher than the default.

- \IBMCOM\PROTOCOL.INI

  Under the MAC section, change **recvbufs** = 2 to **30**
  Change Piggyback Acknowledgements from **1** to **0** on both the server and all requestors (clients).

## Cache and Heap

OS/390 LAN Server front-end processor code maintains its own cache and heap. The cache is used to buffer files locally at the front-end processor, boosting overall performance. If front-end processor caching is used, allocating a large cache is a good idea if there are a lot of simultaneously open files. However, allocating a large cache decreases memory available for other applications running on the front-end processor, and may hurt performance of memory constrained front-end processors.

The heap is pre-allocated memory used to build internal control blocks used by the OS/390 LAN Server front-end processor code. If the front-end processor needs heap space and it is not available because not enough was allocated, clients may not be able to access OS/390 LAN Server resources. Hence, it is a good idea to allocate a large heap, especially if there are a lot of simultaneous clients and/or clients with many connections to LAN Server for OS/390 resources. However, allocating a large heap decreases memory available for other applications running on the front-end processor, and may hurt performance of memory constrained front-end processors.

To maximize the OS/390 LAN Server front-end processor heap and cache, do the following:

- Use the OS/390 LAN Server front-end processor code install panels to set the heap and cache size.
- On the LFSESA.IFS statement in CONFIG.SYS, add /USEALLMEM to the end of the statement if your Network Interface card is able to use addresses above 16M.

When serving OS/390 LAN Server resources, the OS/2 LAN Server cache is not utilized. Additionally, OS/2 LAN Server does not require a large heap, because most heap usage is for OS/2 LAN Server file serving. However, if you plan to use OS/2 LAN Server running on the front-end processor to serve local OS/2 resources, in addition to OS/390 LAN Server resources, you must allocate OS/2 LAN Server cache and heap sufficient for local server performance.

To minimize the OS/2 LAN Server heap and cache, do the following:

- For OS/2 LAN Server 3.x:

  - On the HPFS386.IFS statement in CONFIG.SYS, add /CACHE:1024 to the end of the statement.
  - On the HPFS386.IFS statement in CONFIG.SYS, add /USEALLMEM to the end of the statement if your Network Interface card is able to use addresses above 16M.

- For OS/2 LAN Server 4.x:

  - Specify a CACHESIZE of 1024 or lower in the HPFS386.INI file.
  - Specify USEALLMEM in the HPFS386.INI file if your Network Interface card is able to use addresses above 16M.
  - Do not specify a MAXHEAP value in the HPFS386.INI file. Let the OS/2 LAN Server code dynamically manage its heap.

- OS/2 LAN Server ULTIMEDIA Parameters

  OS/390 LAN Server front-end processor code utilizes the LAN reservation features of OS/2 LAN Server Ultimedia. Disk bandwidth reservation is

performed by the LAN Server for OS/390 host code. Hence, you do not need to specify the DISK section in RRS.INI.

Refer to the OS/2 LAN Server documentation for more information on these parameters.

# Chapter 4. NFS Front-End Processor Installation

## Introduction

OS/390 LAN Server allows NFS users to concurrently access resources on the S/390* hosts.

The OS/390 LAN Server NFS front-end processor drivers are found on the 3.5" Installation Diskette provided. This diskette consists of the file system drivers and related files that are installed within each OS/2 machine that will communicate with OS/390 LAN Server. (Once installed, the OS/2 machine is referred to as an OS/390 LAN Server NFS front-end processor.) The files that are included on this diskette are listed below.

```
List of files required for a CLAW-MMC ($PSCA) connection
---------------------------------------------------------

Packed filename on diskette           Filename after unpack

   BFSNFS.EX_                              BFSNFS.EXE
   BFSNFS.HL_                              BFSNFS.HLP
   BFSNFS.IC_                              BFSNFS.ICO
   BFSNFS.IN_                              BFSNFS.INI
   BFSNFS.MS_                              BFSNFS.MSG
   CU3172B.CL_                             CU3172B.CLW
   MMCSTRT.EX_                             MMCSTRT.EXE
   NETWORK.CF_                             NETWORK.CFG
   PCADDI.SY_                              PCADDI.SYS
   PCAMSG.MS_                              PCAMSG.MSG
   PSCA.AB_                                PSCA.ABS
   PSCA0.CF_                               PSCA0.CFG
   SYSLEVEL.BF_                            SYSLEVEL.BFS


List of files required for a CLAW-NSCA ($NSCA) connection
----------------------------------------------------------

Packed filename on diskette           Filename after unpack

   BFSNFS.EX_                              BFSNFS.EXE
   BFSNFS.HL_                              BFSNFS.HLP
   BFSNFS.IC_                              BFSNFS.ICO
   BFSNFS.IN_                              BFSNFS.INI
   BFSNFS.MS_                              BFSNFS.MSG
   NETWORK.CF_                             NETWORK.CFG
   NSCA0.CF_                               NSCA0.CFG
   NSCA960.OU_                             NSCA960.OUT
   NSCADDI.SY_                             NSCADDI.SYS
   NSCAMCM.CO_                             NSCAMCM.CON
   NSCAMCM.EX_                             NSCAMCM.EXE
   NSCAMCM.PO_                             NSCAMCM.POR
   NSCAMSG.MS_                             NSCAMSG.MSG
   NSCASTRT.EX_                            NSCASTRT.EXE
```

```
   SCCLAWR.ST_                                SCCLAWR.STD
   SCCLAWS.ST_                                SCCLAWS.STD
   SYSLEVEL.BF_                               SYSLEVEL.BFS


List of files required for NFS FEP installation program
-------------------------------------------------------

Filename on diskette

   UNPACK.EXE
   BFSNINST.DLL
   BFSNINST.MSG
   BFSNINST.HLP
   BFSNINST.EXE
```

## NFS Front-End Processor Installation Worksheet

*Table 9 (Page 1 of 3). NFS Front-End Processor Installation Worksheet*

| Information Needed | Your Value | Description |
|---|---|---|
| **For All Connection Types** | | |
| Installation Source | | This is the location of the OS/390 LAN Server source code. If you are installing from the Installation Diskette, it will be ***A:***. |
| Installation Target | | This is the target location where you want the NFS front-end processor driver code to be installed on your server or network. Give the drive and path. If you specify a directory that does not currently exist, the directory will be created for you. If you specify a subdirectory that does not currently exist, the subdirectory will be created for you if the directory itself already exists. That is, the system can create only one new directory layer automatically. The default is: **C:\BFS.** |
| BFS Log File Name | | This record specifies the name of the file to be used to collect log and trace data. The path specified must already exist. The default is **installation target path\BFSNFS.LOG**. |
| Front-End Processor Name | | This is the name the front-end processor will use to connect with host programs. The entry in this field must exactly match the fepname value in the LINK record in the CONFIG file on the OS/390 server, and the LINK record in the NETWORK.CFG on the NFS front-end processor. |
| NFSID | | This specifies the name of the file server to which the NFS front-end processor is to connect. The entry in this field must match the value in the NFSID record in the CONFIG file on the OS/390 server. The default is LFSN front-end processor. |

| *Table 9 (Page 2 of 3). NFS Front-End Processor Installation Worksheet* | | |
|---|---|---|
| **Information Needed** | **Your Value** | **Description** |
| Connection Type | | This indicates the type of connection between your host server and the front-end processor. The choices are **CLAW-MMC** and **CLAW-NSCA**. The default is CLAW-MMC. |
| Retry Wait Time | | This indicates the number of seconds the front-end processor should wait before it tries again to establish a connection with the host, when such a connection has been unsuccessful or lost. The values may range from 1 to 3600 seconds. The default is **60** seconds. |
| Filesize Threshold | | This indicates the buffering threshold. Files smaller than this value will not be readahead buffered. The default is **336k**. |
| Message Timeout | | This indicates whether or not messages are displayed at the NFS front-end processor console and, if so, for how long. The default is **OFF**. |
| NFSPort | | This field specifies the NFS port number that will be registered with the port mapper as the NFS server. The values may range from 1 to 65535. The default is **2049**. |
| Maximum Users | | This field specifies the maximum number of concurrent NFS clients that are supported. The values may range from 64 to 2048. The default is **256**. |
| Readahead Buffers | | This field specifies the total number of readahead buffers that will be used on the NFS front-end-processor to satisfy NFS client read requests. The values may range from 100 to 500. The default is **100**. |
| Readahead Buffer Size | | This indicates the amount of data which will be pre-fetched from a buffered file. The values may range from 8k to 60k. The default is **32k**. |
| Readahead Timeout | | This is the length of time that buffered data will remain cached. The values may range from 1 to 60 seconds. The default is **3** seconds. |
| Sequential Read Threshold | | This indicates the number of sequential reads that must occur before a file is buffered. The values may range from 0 to 99. The default is **3**. |
| RPC Buffers | | This indicates the number of buffers preallocated by the NFS front-end processor to contain NFS request and response RPCs. The values may range from 100 to 1000. The default is **150**. |
| Threads | | This indicates the number of threads. The values may range from 4 to 256. The default is **16**. |
| **For CLAW-MMC Connections Only** | | |
| MMC Adapter | | This specifies which MMC adapter card you are using. The choices are MMC Adapter 0 and MMC Adapter 1. |
| Slot Number | | This specifies the workstation slot number in which the MMC adapter card is installed. The value must be an integer between 1 and 8. |

| *Table 9 (Page 3 of 3). NFS Front-End Processor Installation Worksheet* | | |
|---|---|---|
| **Information Needed** | **Your Value** | **Description** |
| Channel Address | | This specifies the last two digits of the 370 subchannel address to be used for the MMC adapter card. The value must be an even 2 digit hexadecimal address, corresponding to **the last two digits of the line address of the host.** |
| Channel Speed | | This specifies the speed of the channel as either DC Interlock or streaming mode in megabits per second. The choices are DC Interlock, 1.9 Mb/sec, 2.7 Mb/sec, 3.4 Mb/sec, or 4.5 Mb/sec. |
| **For CLAW-NSCA (ESCON) Connections Only** | | |
| NSCA Adapter | | This specifies which NSCA card you are using. Select either NSCA Adapter 0 or NSCA Adapter 1. |
| Slot Number | | This specifies the workstation slot number in which the NSCA Adapter card is installed. The value must be an integer between 1 and 8. |
| Local CLAW Address | | The last two digits specifies the 370 subchannel which is to be used for the NSCA adapter card. The value must be an even 2 digit hexadecimal address, corresponding to the **last two digits** of the line address of the host. |
| Remote CLAW Address | | This specifies the hexadecimal address of the fiber connection between the front-end processor and the host, as it is known on the ES/9000* processor. The value must be an even 2 digit hexadecimal address. |
| Direct Fiber/Switched Port | | Choose between these two fields to indicate the form of connection between the front-end processor and the mainframe. If you select Switched Port, also specify values for Port Address and IOCP CU Address. |
| Port Address | | For Switched Port connections, this specifies the port number of the switch connection to the ESCON* channel. Specify a 2-digit hexadecimal address. |
| IOCP CU Address | | For Switched Port connections, this specifies the value from the CUADD parameter of the CNTLUNIT statement for the ESCON channel in the IOCP table for the ES/9000. Specify a 1 digit hexadecimal address. |

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

To install the OS/390 LAN Server software that runs the front-end processor, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.

3. Insert the Installation Diskette/s in the A: drive for a local install.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** for a local install, or

   ***drive:\BFSNINST*** to install from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. If you have a previous version of OS/390 LAN Server installed, you must remove it before you can install this version. This version will overwrite the existing BFSNFS.INI file. If you wish to save your existing BFSNFS.INI file, rename it before beginning the formal installation process for OS/390 LAN Server.

   If you do NOT have a previous version of OS/390 LAN Server installed, all of the choices under "Local Services" should be grayed-out except "Install/Configure FEP drivers."

   On the OS/390 LAN Server Menu, select 'Install/Configure FEP drivers'. This will bring up the 'Install Path Selection' panel.

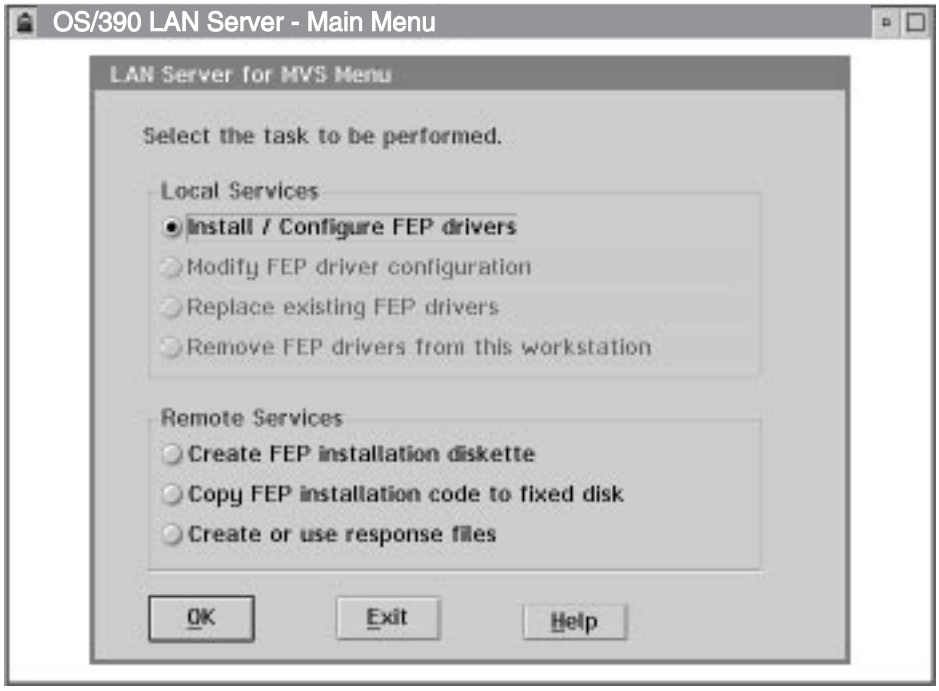


*Figure 39. OS/390 LAN Server Menu - Select Install/Configure Front-End Processor Drivers*

6. On the 'Install Path Selection' panel, fill in the entry fields. Use the values on the NFS front-end processor Installation Worksheet, Table 9 on page 90, to fill in the fields. Click on the 'OK' pushbutton when you are done to bring up the 'Set configuration' panel.


*Figure 40. Install Path Selection*

7. If a path you typed on the 'Install Path Selection' screen does not exist, another window will appear on the 'Install Path Selection' panel. Click on the 'Yes' pushbutton to create the path.


*Figure 41. Create Install Path*

8. On the 'Set configuration' panel, fill in the entry fields using the values from the NFS front-end processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up the 'Set configuration' panel for the CLAW connection.

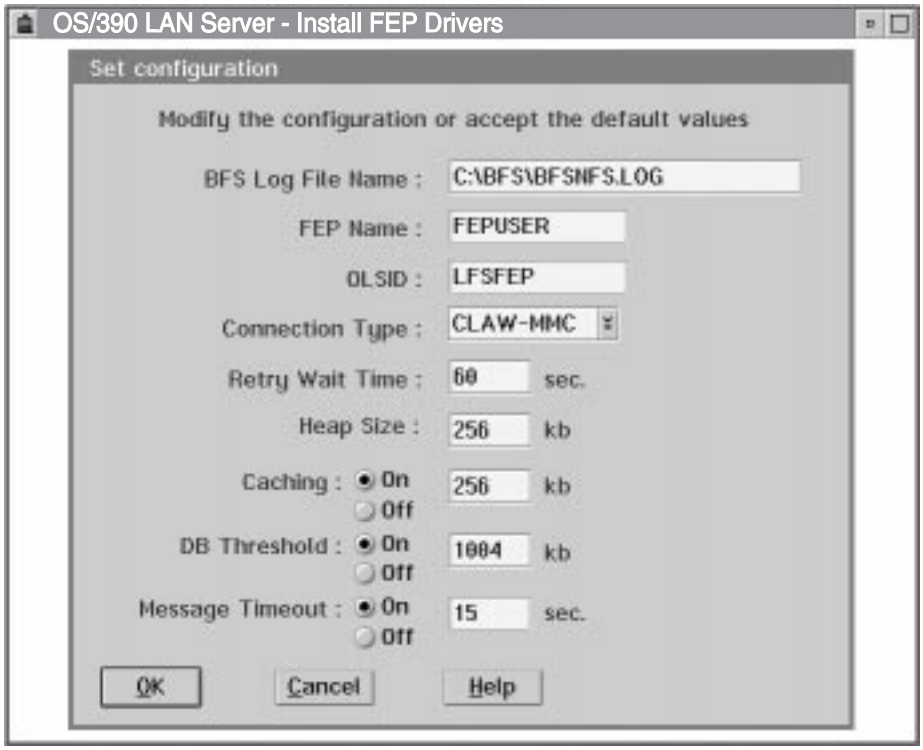


*Figure 42. Set Configuration - Modify Configuration or Accept Defaults*

9. **(CLAW-MMC CONNECTIONS ONLY)** On the 'Set configuration' panel, the first item to select will be the type of MMC Adapter. Fill in the entry fields using the values from the NFS front-end processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up an additional 'Set configuration' panel.

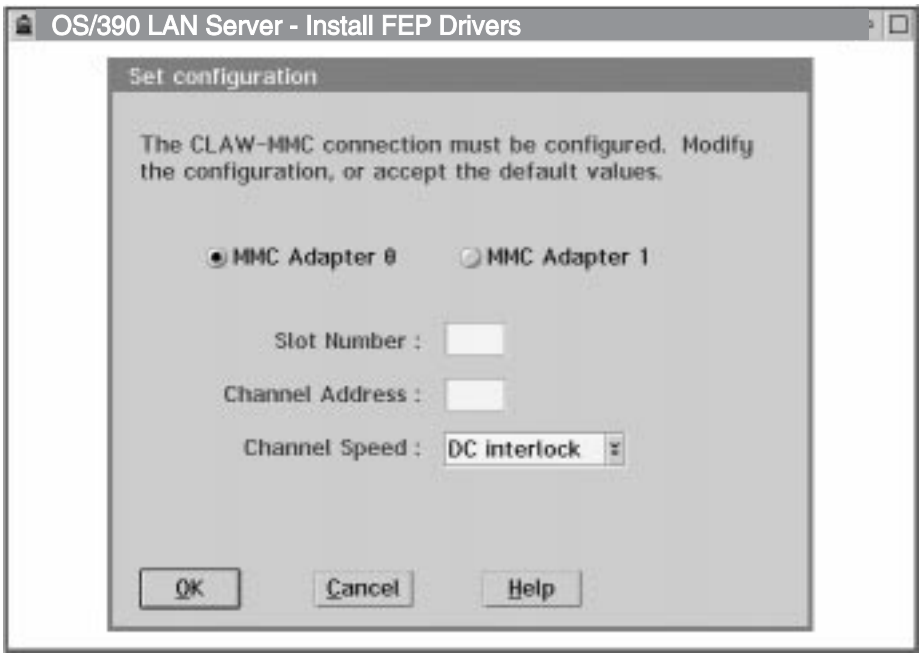


*Figure 43. Set Configuration - CLAW-MMC Connections Only - MMC Adaptor*

10. **(CLAW-NSCA CONNECTIONS ONLY)** On the 'Set configuration' panel, the first item to select will be the type of NSCA Adapter. Fill in the entry fields using the values from the NFS Front-End Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up an additional 'Set configuration' panel.

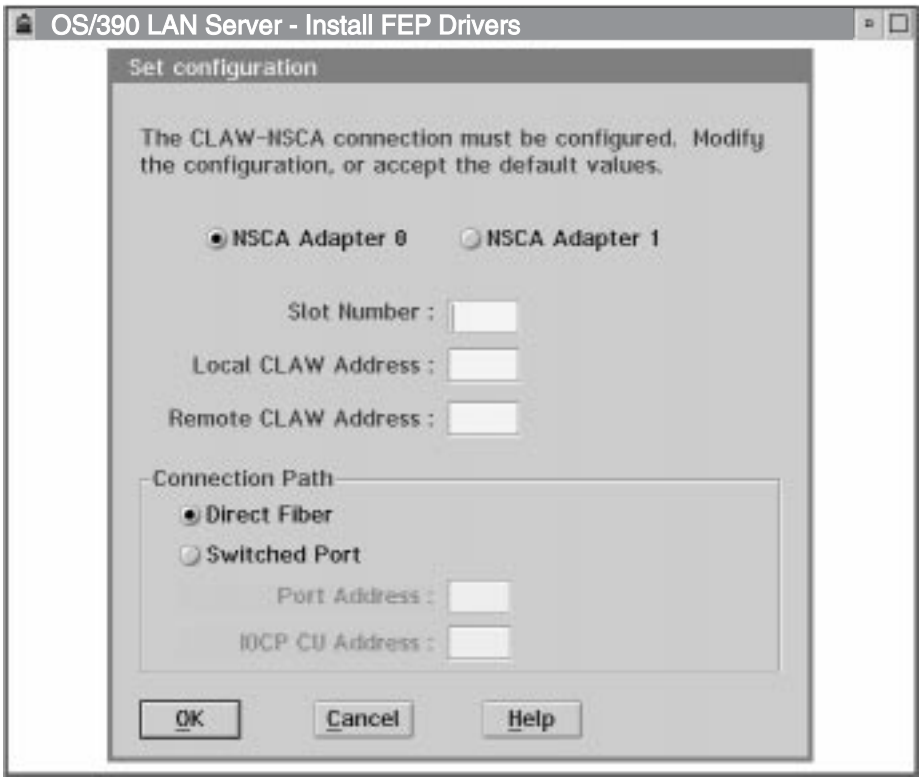


*Figure 44. Set Configuration - CLAW-NSCA Connections Only - NSCA Adaptor*

11. While the installation progresses, you will see a panel indicating which files are being copied and unpacked, and what percent of the installation is now complete.

    **Note:** If you choose to cancel the installation, system errors are likely to occur if OS/390 LAN Server is started. If you wish to use OS/390 LAN Server successfully following a cancel of the installation, begin the installation process again.

12. When the initial installation is complete, another window will appear indicating that the NFS front-end processor drivers have been installed and that some new files are being automatically created. When this process is complete, the 'CONFIG.SYS modification' panel will appear.

13. Make a selection on the 'CONFIG.SYS modification' panel.

    If you select 'Modify CONFIG.SYS automatically', your original CONFIG.SYS will be renamed to CONFIG.BFS and a new CONFIG.SYS will automatically be created.

    If you select 'Do NOT modify CONFIG.SYS', a file called CONFIG.NEW will automatically be created. You will need to manually edit your CONFIG.SYS file to reflect what is in the CONFIG.NEW file before you try to use the NFS front-end processor drivers.

    After you make your selection, click on the 'OK' pushbutton to complete the installation process.

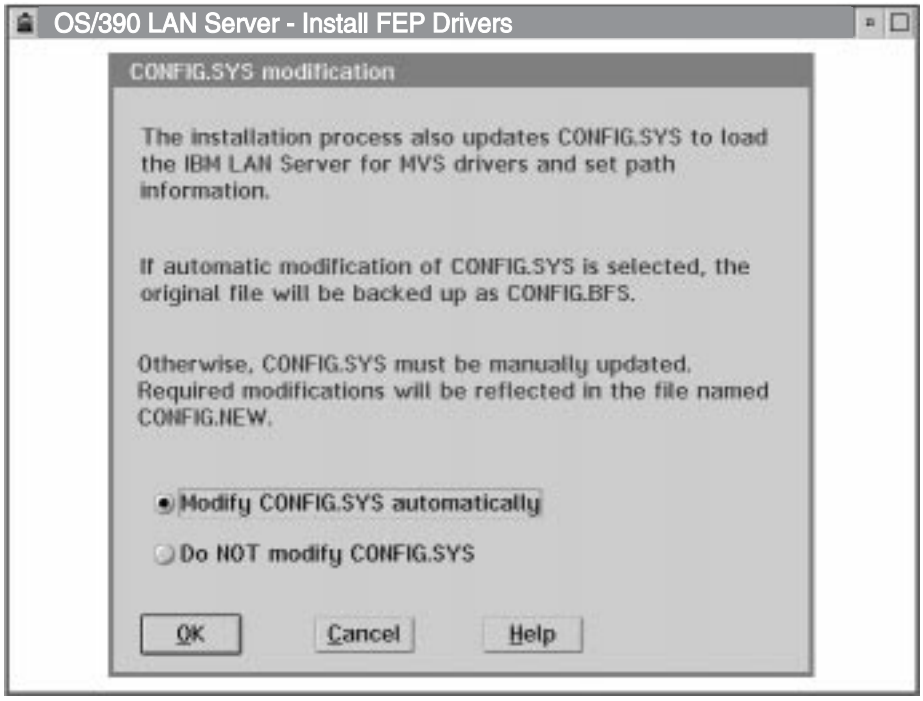


*Figure 45. CONFIG.SYS Modification*

14. When the entire NFS front-end processor driver installation is complete, you will see a window indicating that the drivers were successfully installed. Click on the 'OK' pushbutton to bring up the OS/390 LAN Server menu.

15. On the OS/390 LAN Server menu, click on the 'Exit' pushbutton, remove the diskette, shutdown the front-end processor, and then restart the front-end processor to invoke the changes.

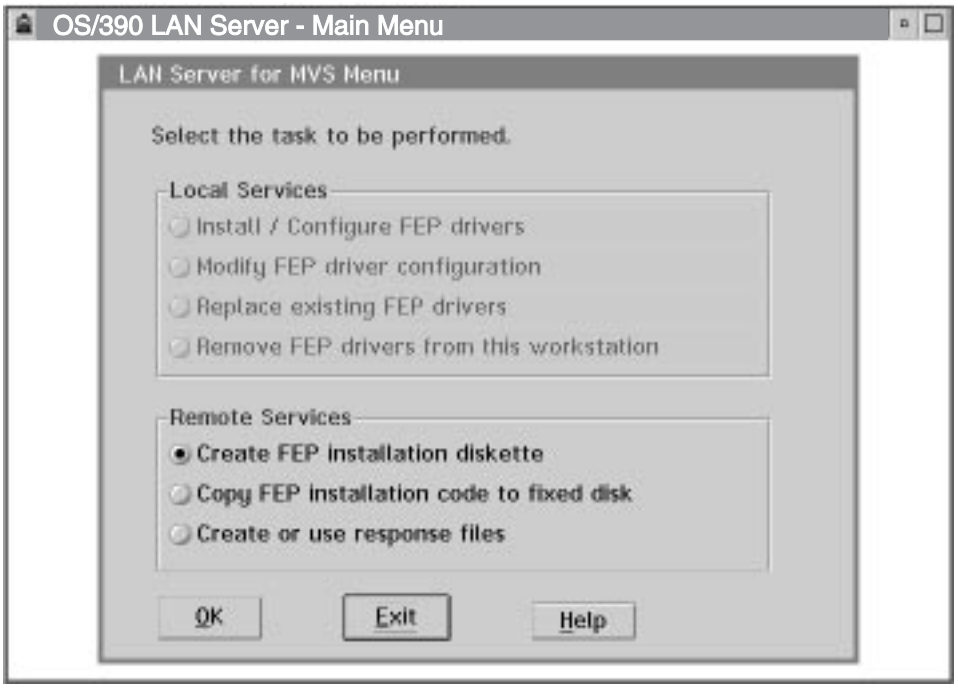


*Figure 46. OS/390 LAN Server Menu*

## NFS Front-End Processor Installation Verification

The following steps should be performed after completing all installation steps to verify the success of your OS/390 LAN Server installation:

**Note:** This section assumes you have installed the OS/390 LAN Server host code and set up everything to support the NFS front-end processor.

1. Before starting the OS/390 LAN Server host server, verify that you have performed all of the following steps:
   - Allocate and initialize a linear data set to hold workstation data.
   - Define resource access control, via the EXPORTS configuration file.
   - Define the CLAW connection for the NFS front-end processor.
2. Start the OS/390 LAN Server host server by entering the following from the host console:

**start runlfs**

```
File Services Version 1.1.2000, built MM/DD/YY HH.MM.SS, is ready
```

3. Start the NFS front-end processor by entering the following from an OS/2 window (on the NFS front-end processor). This will start the NFS front-end processor's OS/390 LAN Server code.

**bfsnfs**

4. From an NFS client, issue a MOUNT command for the /trylfs file system.

   **Note:** This assumes the trylfs file system was defined and created on the OS/390 host.

   a. The following MOUNT command would be used on an RS/6000 workstation:

**mount -n** *mvshost* **-v nfs -o soft,retry=1,ro /trylfs,ro /***mountpoint*

*mvshost* is the symbolic name of the host NFS server to which the NFS front-end processor will connect (NFSID).

*mountpoint* is the point in the local file system to which you want to mount the OS/390 LAN Server directory.

**Notes:**

1. soft,retry=1 are recommended just in case the installation did not complete correctly.
2. ro must be specified in both the logical and host option strings.
3. /trylfs is the remote file system. This must be entered in lowercase characters, as shown.

   b. The following MOUNT command would be used on a front-end processor workstation:

**mount h:** *mvshost***:/trylfs,ro**

*mvshost* is the symbolic name of the host NFS server to which the NFS front-end processor will connect (NFSID).

**Notes:**

1. ro must be specified in both the logical and host option strings.
2. /trylfs is the remote file system. This must be entered in lowercase characters, as shown.

5. Complete the OS/390 LAN Server host verification:

   a. The following command would be issued on an RS/6000 workstation:

**ls -la /***mountpoint*

The contents of the /trylfs file system should be listed on your screen in the form *filename.filetype* entered in lowercase.

   b. The following command would be issued on a front-end processor workstation:

| | |
|---|---|
| **dir h:** | The contents of the /trylfs file system should be listed on your screen in the form *filename.filetype* entered in lowercase. |

**Note**

NFS front-end processor verification is now complete.

## Terminate NFS Front-End Processor Verification

1. On the NFS front-end processor, terminate **BFSNFS**. BFSNFS can be ended by closing the NFS front-end processor window. (Refer to the 'NFS Front-End Processor Shutdown' in this section.)
2. From the host, reinitialize the OS/390 LAN Server server before making it available to the user community. From the host console, enter either one of the following commands to stop the host server machine:

**stop runlfs**

-or-

**f runlfs shutdown**

# Startup/Shutdown Procedures

## Host Startup

The OS/390 operator can start OS/390 LAN Server by entering **start runlfs**.

## Host Shutdown

To stop OS/390 LAN Server, enter one of the following commands:

- To shut down OS/390 LAN Server from a TSO/E administrator, enter **shutdown**.
- From an OS/390 console, enter **stop runlfs**.

## NFS Front-End Processor Startup

At the *x:*\ prompt, enter the command ***BFSNFS*** where **x:** is the drive where the NFS front-end processor code resides.

## NFS Front-End Processor Shutdown

Close the NFS front-end processor panel by :

- Clicking on ***Close*** on the OS/2 pull down menu OR
- Pressing 'F3' OR
- Pressing 'ALT-F4'

## Modifying the NFS Front-End Processor Driver Configuration

Before you begin the formal modification process for the OS/390 LAN Server NFS front-end processor Drivers, complete the NFS front-end processor Installation Worksheet, Table 9 on page 90.

To modify the configuration of the front-end processor drivers, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or OS/2 full screen session.
3. Insert the Installation Diskette/s in the A: drive for a local modification.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

   **Note:**

   > OS/2 LAN Server must be installed on the front-end processor before the OS/390 LAN Server front-end processor code. Any time the OS/2 LAN Server code is upgraded, the OS/390 LAN Server code may need to be reinstalled.

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** for a local modification, or

   ***drive:\BFSNINST*** to modify from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Modify FEP driver configuration'. (Since you have already installed OS/390 LAN Server, the 'Install/Configure FEP drivers' choice under "Local Services" should be grayed-out). This will bring up the 'Modify FEP driver configuration' panel.

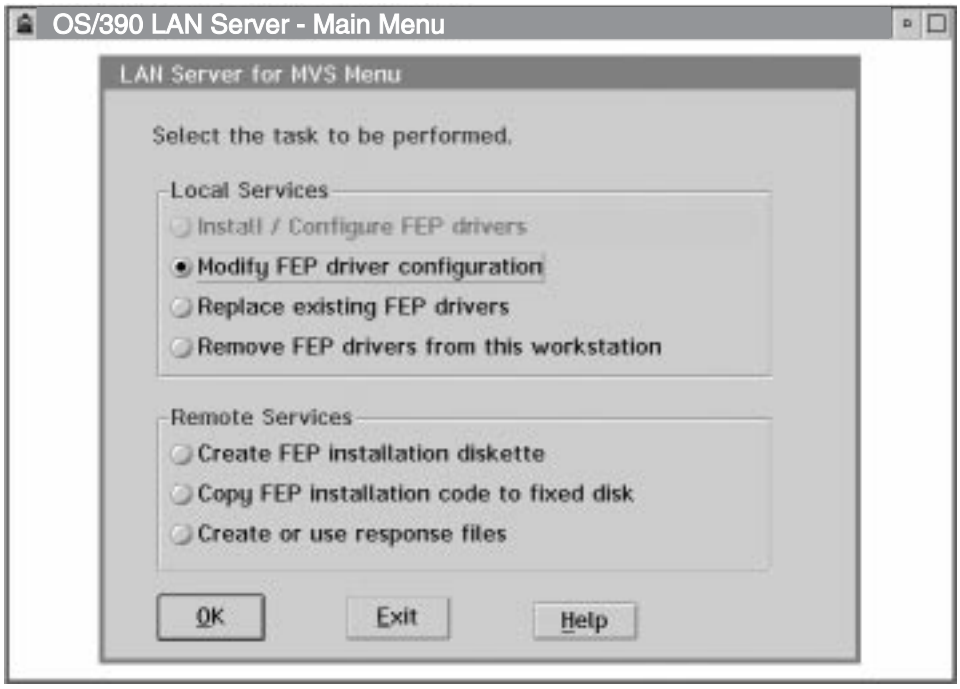


*Figure 47. OS/390 LAN Server Menu - Select Modify FEP driver configuration*

6. On the 'Modify FEP driver configuration' panel, fill in the entry fields. Use the values on the NFS Front-End Processor Installation Worksheet, Table 9 on page 90, to fill in the fields. Click on the 'OK' pushbutton when you are done.

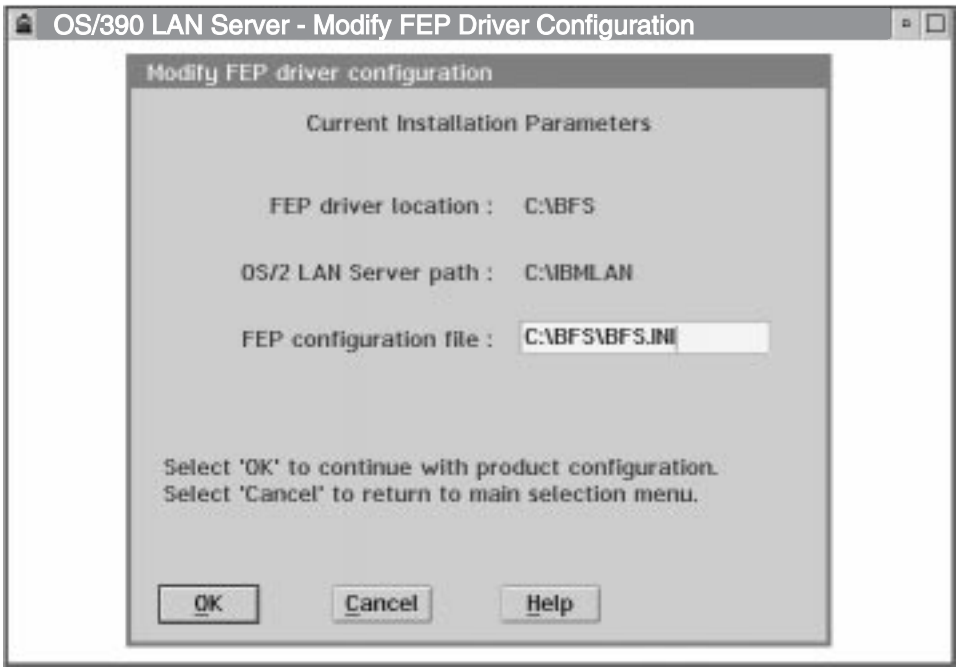


*Figure 48. Modify FEP Driver Configuration*

7. On the 'Set configuration' panel, fill in the entry fields using the values from the NFS Front-End Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up the 'Set configuration' panel for the CLAW connection.

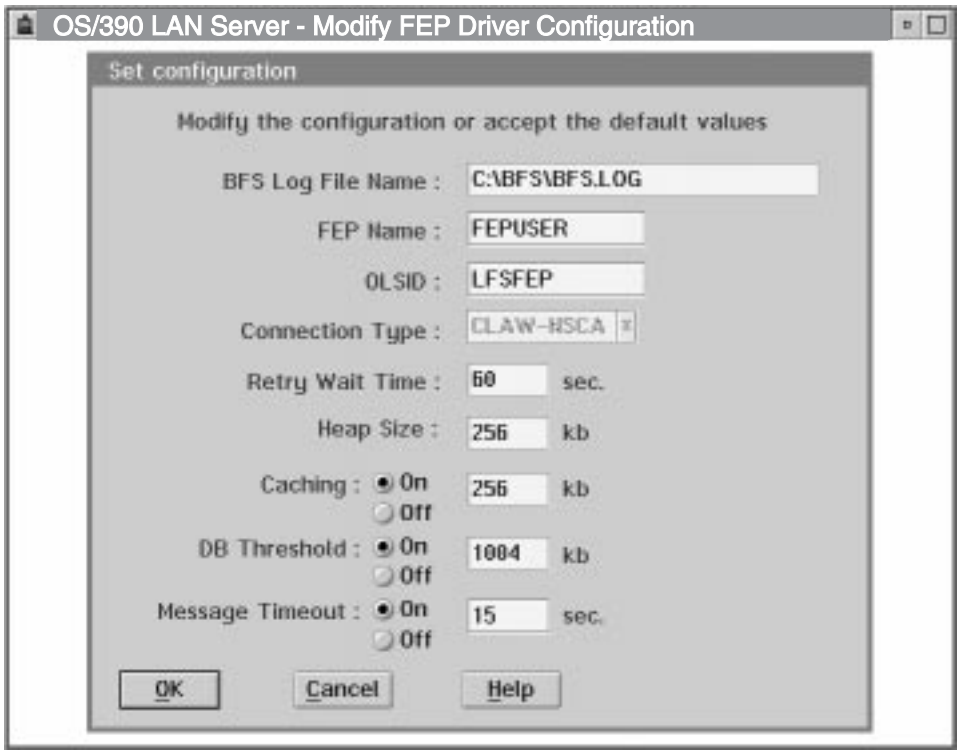


*Figure 49. Set Configuration*

8. **(CLAW-MMC CONNECTIONS ONLY)** On the 'Set configuration' panel shown below, fill in the entry fields using the values from the NFS Front-End Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up an additional 'Set configuration' panel.

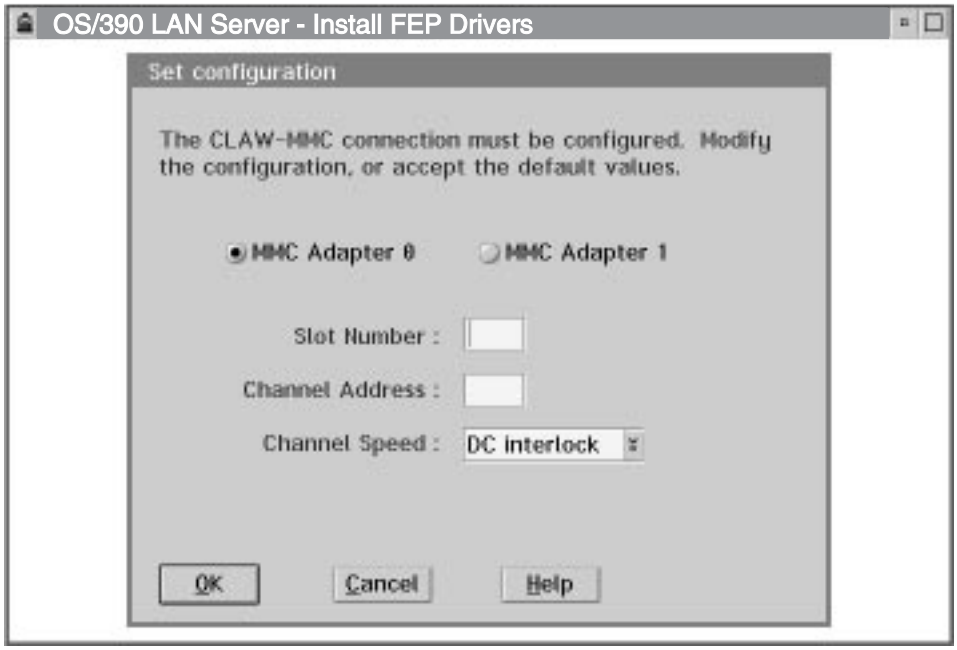


*Figure 50. Set Configuration - CLAW-MMC Connection Only*

9. **(CLAW-NSCA CONNECTIONS ONLY)** On the 'Set configuration' panel shown below, fill in the entry fields using the values from the NFS Front-End

Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up an additional 'Set configuration' panel.

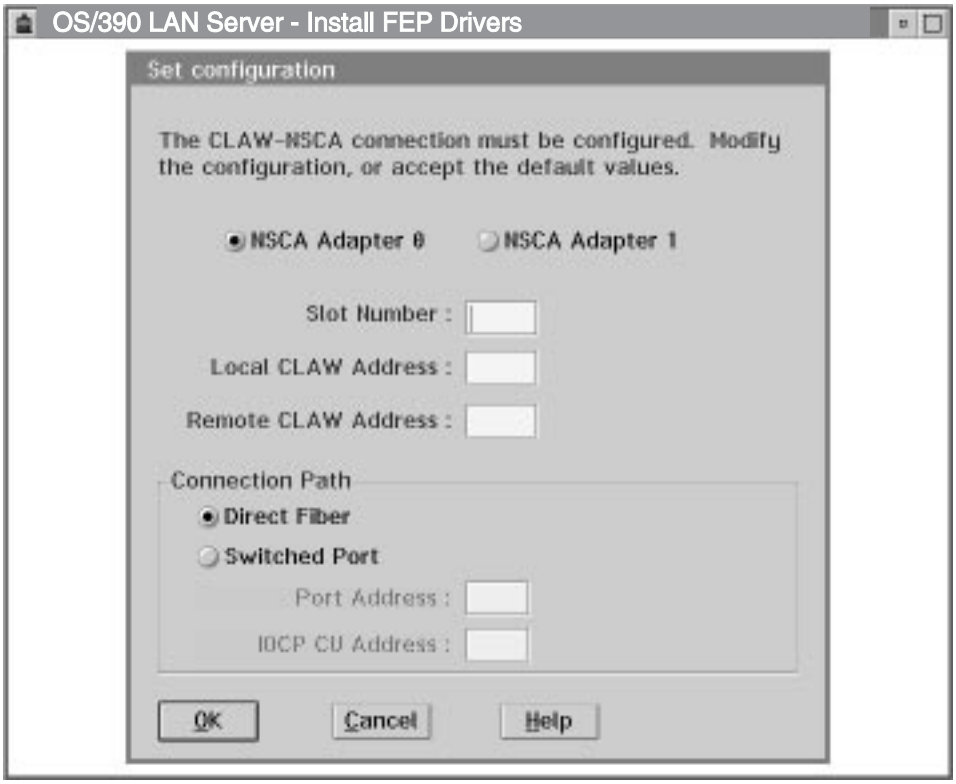


*Figure 51. Set Configuration - CLAW-NSCA Connection Only*

10. On this 'Set configuration' panel, fill in the entry fields using the values from the NFS Front-End Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to begin the installation.
11. When the initial installation is complete, a window will appear indicating that the OS/390 LAN Server front-end processor drivers have been modified and that some new files are being automatically created. When this process is completed, the 'CONFIG.SYS modification' panel will appear.
12. Make a selection on the 'CONFIG.SYS modification' panel.

    If you select 'Modify CONFIG.SYS automatically', your original CONFIG.SYS will be renamed to CONFIG.BFS and a new CONFIG.SYS will automatically be created.

    If you select 'Do NOT modify CONFIG.SYS', a file called CONFIG.NEW will automatically be created. You will need to manually edit your CONFIG.SYS file to reflect what is in the CONFIG.NEW file before you try to use the front-end processor drivers.

    After you make your selection, click on the 'OK' pushbutton to complete the installation process.

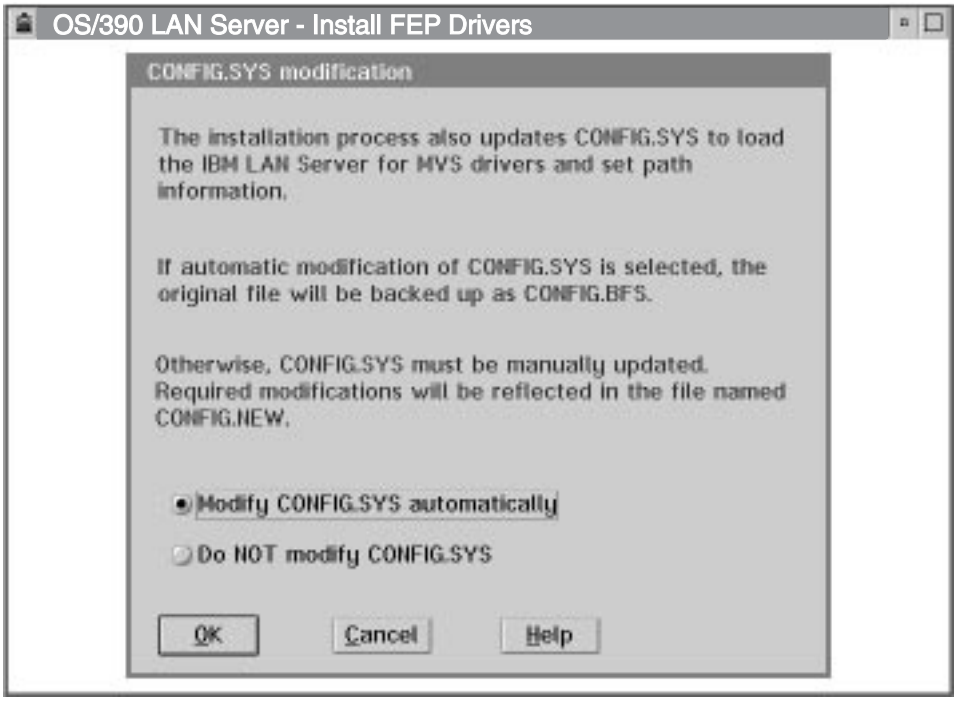


*Figure 52. CONFIG.SYS Modification*

13. When the entire front-end processor driver configuration modification is complete, you will see a panel indicating the front-end processor drivers have been successfully re-configured. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Replacing NFS Front-End Processor Drivers

Before you begin the formal replacement process for the OS/390 LAN Server NFS front-end processor drivers, complete the NFS Front-End Processor Replacement Worksheet, Table 10 below.

*Table 10. NFS Front-End Processor Replacement Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| Source of Update | | This is the location of the replacement code. If you are replacing the front-end processor drivers with code that is on a diskette, type ***A:***. |
| FEP Configuration File Name | | This file is typically named BFSNFS.INI. The BFSNFS.INI file defines the characteristics of the connection for the OS/2 NFS front-end processor. Specify the drive and path to the BFSNFS.INI file (or to your FEP configuration file, if you have renamed BFSNFS.INI to another name). |

To replace the front-end processor drivers, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or OS/2 full screen session.

3. Insert the Installation Diskette/s in the A: drive for a local replacement.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** for a local replacement, or

   ***drive:\BFSNINST*** to replace from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Replace existing FEP drivers'. This will bring up the 'Replace FEP drivers' panel.

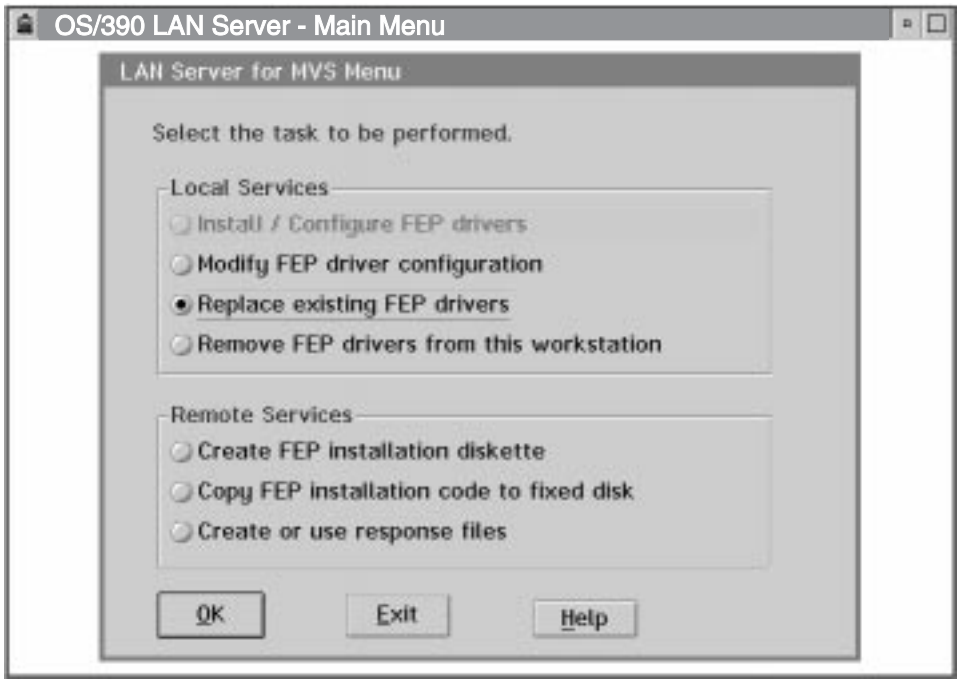


*Figure 53. OS/390 LAN Server Menu - Select Replace Existing FEP Drivers*

6. On the 'Replace FEP drivers' panel, fill in the entry fields. Use the values on the NFS Front-End Processor Driver Replacement Worksheet, Table 10 on

page 105, to fill in the fields. Click on the 'OK' pushbutton when you are done.

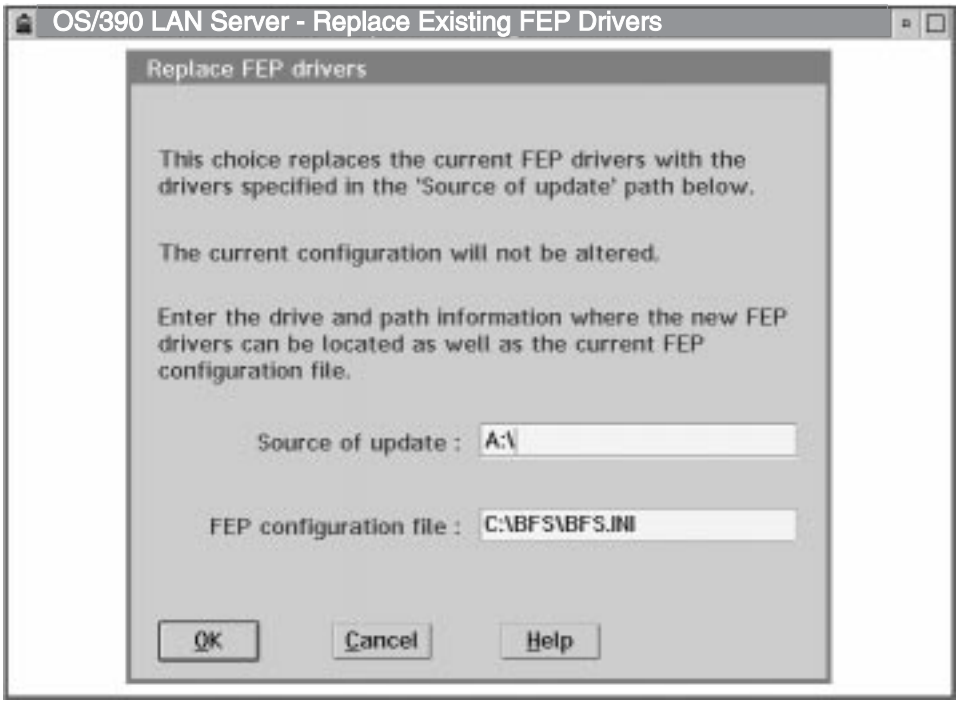


*Figure 54. Replace Front-End Processor Drivers*

7. While the installation progresses, you will see a panel indicating which files are being updated and what percent of the replacement is now complete.
8. When the entire front-end processor driver configuration replacement is complete, you will see a panel indicating the front-end processor drivers were successfully replaced. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Removing NFS Front-End Processor Drivers

Before you begin the formal removal process of the OS/390 LAN Server NFS front-end processor drivers, complete the OS/390 LAN Server NFS Front-End Processor Removal Worksheet, Table 11 below.

*Table 11. NFS Front-End Processor Removal Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| Front-End Processor Driver Location | | This is the location of the unpacked FEP driver code. |

To remove the front-end processor drivers, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or OS/2 full screen session.
3. Insert the Installation Diskette/s in the A: drive for a local removal.

| For the English version, the NFS diskettes are labeled:

| OS/390 LAN Server: English
| NFS FEP
| 5647-A01 V2R5M0
| Install Diskette (1 of 2)

| OS/390 LAN Server: English
| NFS FEP
| 5647-A01 V2R5M0
| Install Diskette (2 of 2)

| For the Japanese version, the NFS diskette is labeled:

| OS/390 LAN Server: Japanese
| NFS FEP
| 5647-A01 V2R5M0
| Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** for a local removal, or

   ***drive:\BFSNINST*** to remove from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Remove FEP drivers from this workstation'. This will bring up the 'Remove FEP drivers' panel.

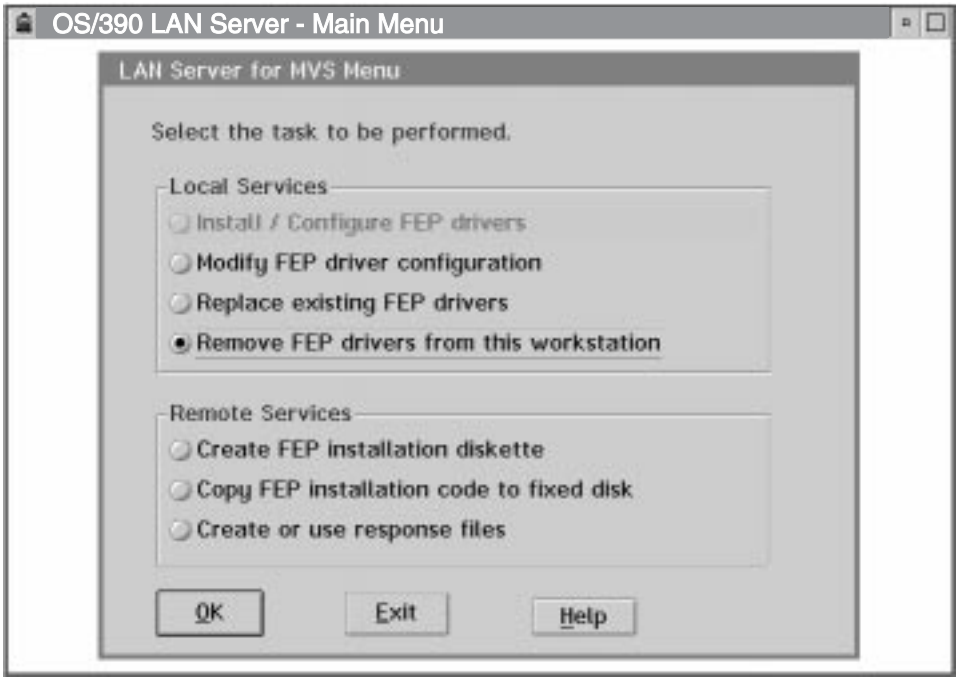


*Figure 55. OS/390 LAN Server Menu - Select Remove FEP Drivers from This Workstation station*

6. On the 'Remove FEP drivers' panel, fill in the entry fields. Use the values on the NFS Front-End Processor Driver Removal Worksheet, Table 11 on

page 107, to fill in the fields. Click on the 'OK' pushbutton when you are done.

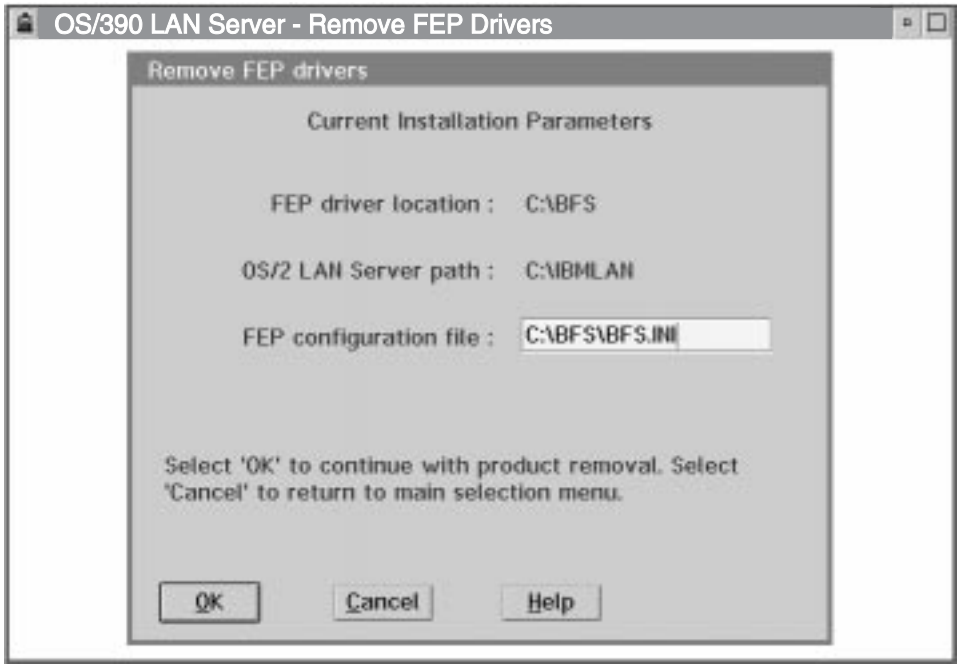


*Figure 56. Remove FEP Drivers*

7. You will see a confirmation panel asking if you are certain you wish to remove the FEP drivers. Click on the 'OK' pushbutton to start the FEP driver removal.

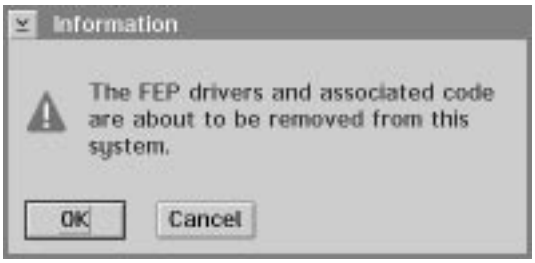


*Figure 57. Information Panel - FEP Drivers About to be Removed*

8. When the initial removal is complete, a window will appear indicating that the OS/390 LAN Server front-end processor drivers have been removed and that some files are being automatically deleted. When this process is completed, the 'CONFIG.SYS modification' panel will appear.
9. Make a selection on the 'CONFIG.SYS modification' panel.

   If you select 'Modify CONFIG.SYS automatically', your original CONFIG.SYS will be renamed to CONFIG.BFS and a new CONFIG.SYS that does not reference the front-end processor drivers will automatically be created.

   If you select 'Do NOT modify CONFIG.SYS', a file called CONFIG.NEW will automatically be created. You will need to manually edit your CONFIG.SYS file to reflect what is in the CONFIG.NEW file before you try to use other programs.

   Click on the 'OK' pushbutton to complete the removal process.

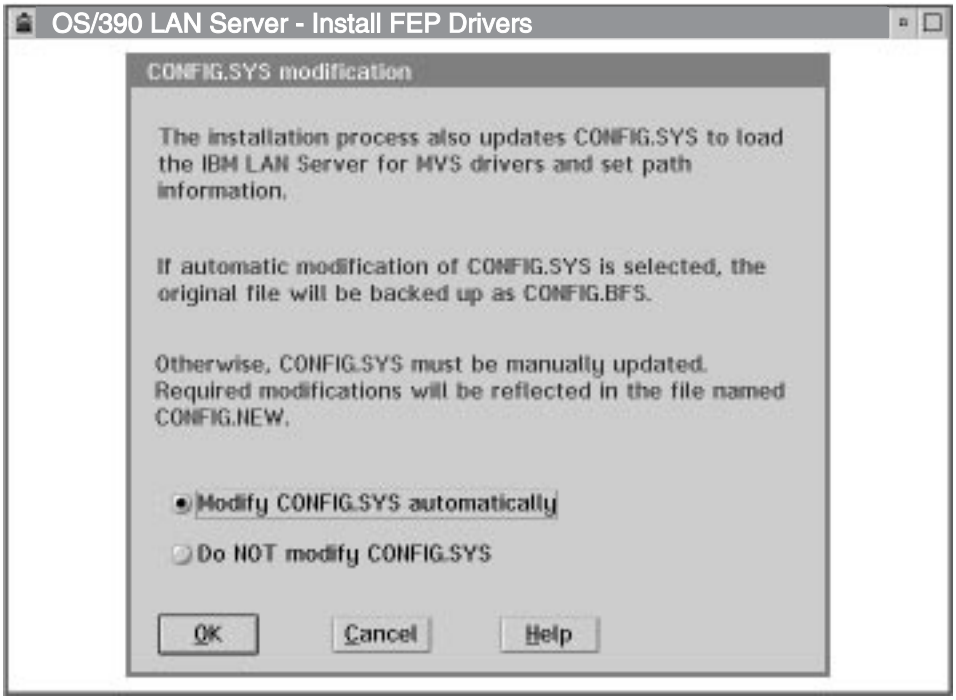


*Figure 58. CONFIG.SYS Modification*

10. When the entire front-end processor driver removal is complete, you will see a panel indicating this information. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

**Note!**

After the OS/390 LAN Server NFS front-end processor drivers have been removed from the workstation, it is the system administrator's responsibility to remove any prior references to the front-end processor name, NFSID, and channel addresses from the CLAW configuration files.

## Creating a FEP Installation Diskette

This process creates a copy of the packed OS/390 LAN Server NFS front-end processor installation code packed files on a high-capacity 3.5" diskette.

**Note:** If this option is not selectable, you must perform the "Copy FEP Installation Code to Fixed Disk" operation.

Before you begin the formal NFS front-end processor installation diskette creation process for the OS/390 LAN Server NFS FEP drivers, obtain a high-capacity 3.5" blank, formatted diskette, and complete the Create NFS Front-End Processor Installation Diskette Worksheet shown in Table 12.

| *Table 12. Create the NFS Front-End Processor Installation Diskette Worksheet* | | |
|---|---|---|
| **Information Needed** | **Your Value** | **Where to Find It** |
| **For All Connection Types** | | |
| Installation Source | | This is the location of the OS/390 LAN Server source code, either on your local workstation, or on a fixed disk within the network. |
| Target Diskette Drive | | This is the target diskette drive location where you want the front-end processor driver code to be copied. Type the diskette drive letter. |

## Creating a Front-End Processor Installation Diskette Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

To copy the OS/390 LAN Server software that runs the front-end processor, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the Installation Diskette/s in the A: drive to create a diskette locally.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** to create a diskette locally, or

   ***drive:\BFSNINST*** to create a diskette from a network drive.

The OS/390 LAN Server logo screen will be displayed.

Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Create FEP installation diskette'. This will bring up the 'Create Front-End Processor Installation Diskette' panel.

   **Note:** If this option is not selectable, you must perform the "Copy FEP Installation Code to Fixed Disk" operation.

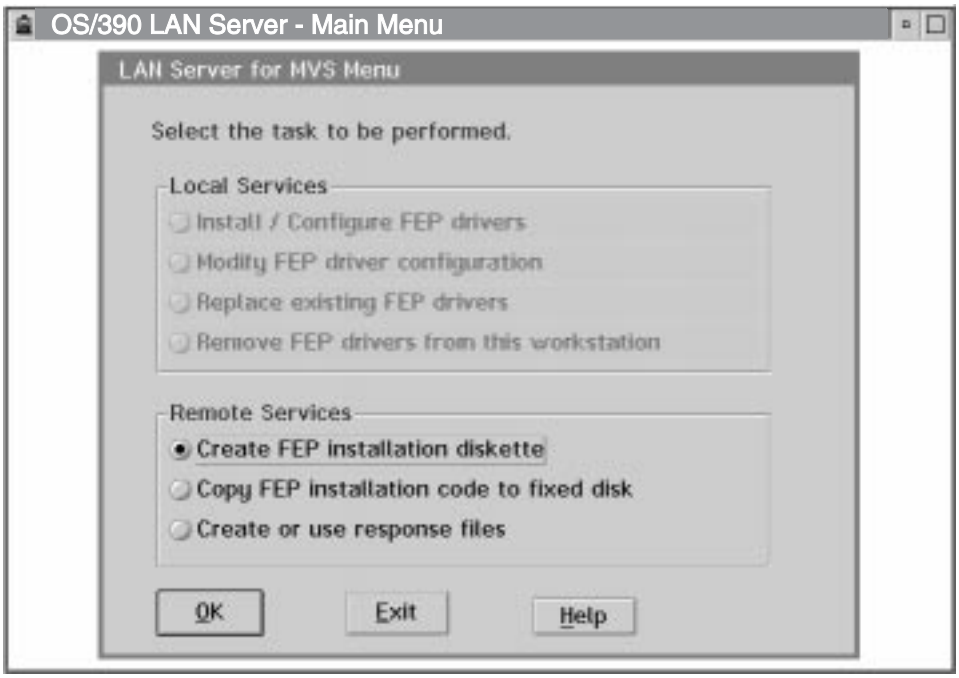


*Figure 59. OS/390 LAN Server Menu - Select Create NFS Front-End Processor Installation Diskette*

6. On the 'Create FEP Installation Diskette' panel, fill in the entry fields. Use the values on the OS/390 LAN Server Create NFS Front-End Processor Installation Diskette Worksheet, Table 12 on page 111, to fill in the fields. Then insert a high-capacity 3.5" diskette in the diskette drive. Click on the 'OK' pushbutton when you are done to begin creating the installation diskette.

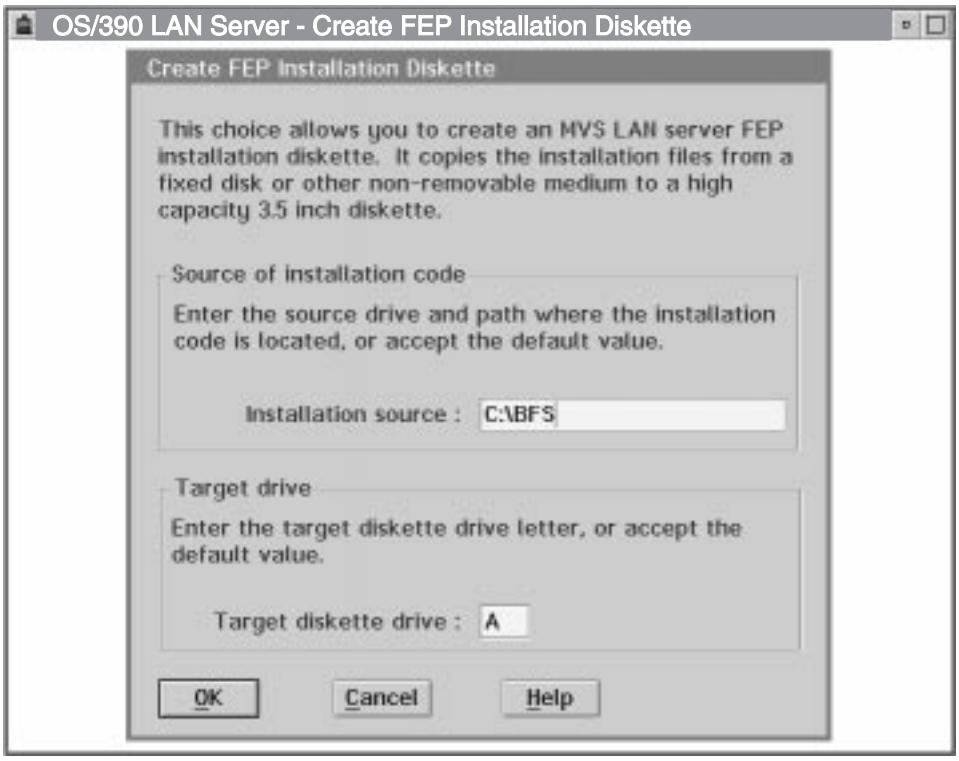


*Figure 60. Create Front-End Processor Installation Diskette*

7. Before the copying actually begins, the program will verify that all required files are present at the installation source location. While that occurs, a message window will be displayed.
8. If one or more files cannot be found, a message will appear. Refer to the Error Log for details on which files were not found.
9. If you didn't insert a high-capacity 3.5 " diskette in the diskette drive, a panel will appear. Insert the diskette, then click on the 'OK' pushbutton.
10. While the copy to diskette progresses, you will see a panel indicating which files are being copied and what percent of the copy to diskette is now complete.
11. When the entire front-end processor driver copy to diskette is complete, you will see a panel indicating the diskette was successfully created. Click on the 'OK' pushbutton.

## Copying FEP Installation Code to the Fixed Disk

Before you begin the formal copy to fixed disk process for the OS/390 LAN Server NFS front-end processor drivers, complete the Copy NFS Front-End Processor Installation Code to Fixed Disk Worksheet, Table 13 below.

| *Table 13. Copy NFS Front-End Processor Installation Code to Fixed Disk Worksheet* | | |
|---|---|---|
| **Information Needed** | **Your Value** | **Where to Find It** |
| **For All Connection Types** | | |
| Installation Source | | This is the location of the OS/390 LAN Server source code (either on fixed disk or on diskette). Specify the drive and path. |
| Target Drive | | This is the target fixed disk drive location where you want the front-end processor driver code to be copied. Specify the drive and path. |

## Copying NFS Front-End Processor Installation Code to Fixed Disk Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

The copy of the front-end processor installation code may also be placed on a code server to enable CID installation.

To copy the OS/390 LAN Server software that runs the front-end processor, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the Installation Diskette/s in the A: drive to perform a local copy.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** to copy locally, or

   ***drive:\BFSNINST*** to perform the copy from a network drive.

The OS/390 LAN Server logo screen will be displayed.

Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Copy FEP installation code to fixed disk'. This will bring up the 'Copy FEP Installation Code to Fixed Disk' panel.

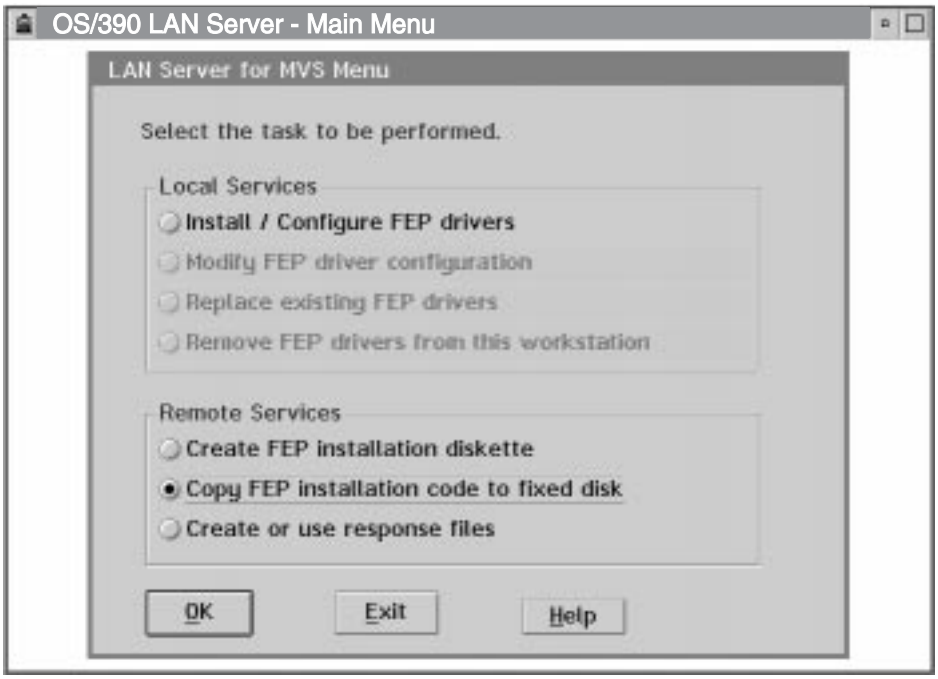


*Figure 61. OS/390 LAN Server Menu - Select Copy FEP Installation Code to Fixed Disk*

6. On the 'Copy FEP installation code to fixed disk' panel, fill in the entry fields. Use the values on the OS/390 LAN Server Copy NFS Front-End Processor Installation Code to Fixed Disk Worksheet, Table 13 on page 114, to fill in the fields. When you are done, click on the 'OK' pushbutton to begin the copy process.

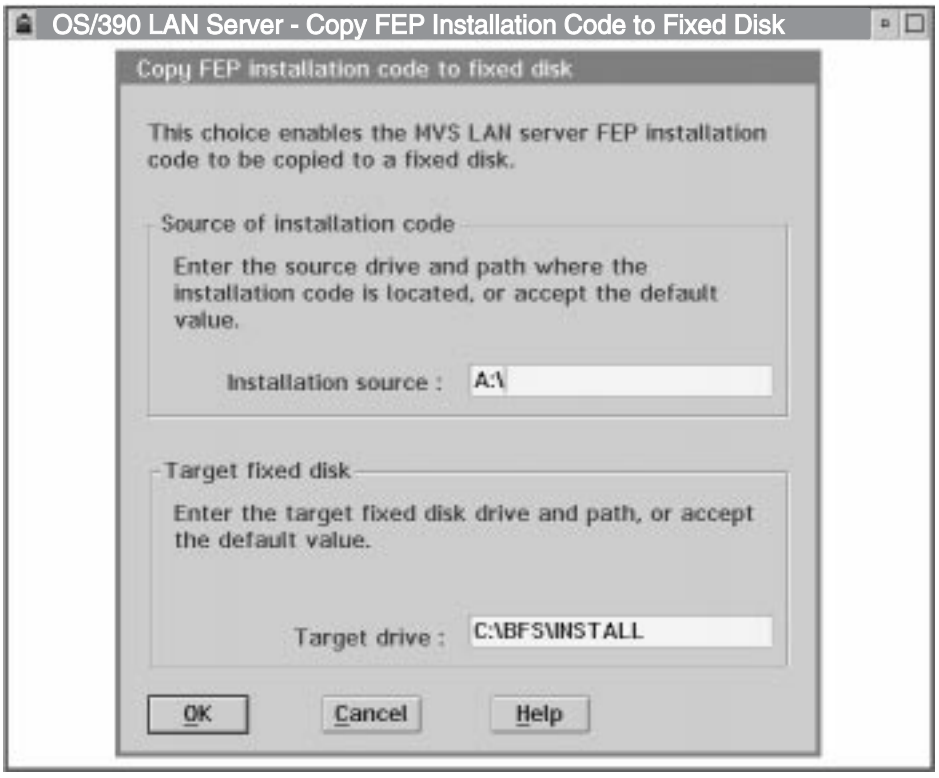


*Figure 62. OS/390 LAN Server Menu - Select Copy FEP Installation Code to Fixed Disk*

7. Before the copying actually begins, the program will verify that all required files are present at the installation source location. While that occurs, an informational window will appear.
8. If one or more files cannot be found, a panel will appear. Select 'OK' to continue with the creation, or 'Cancel' to return to the main menu. Refer to the Error Log for details on which files were not found.
9. If you do not have enough available space on the target fixed disk, a panel will appear. Free up some additional fixed disk space, then click on the 'Retry' pushbutton.
10. While the copy progresses, you will see a panel indicating that files are being copied.
11. When the entire front-end processor driver copy to fixed disk is complete, you will see a panel indicating that the code has been copied to the specified drive. Click on the 'OK' pushbutton.

## Creating NFS Front-End Processor Custom Response Files

Before you begin the formal process of creating custom response files for the OS/390 LAN Server NFS front-end processor drivers, complete the NFS Front-End Processor Installation Worksheet, Table 9 on page 90.

This section explains the creation of custom response files using a graphical user interface. To create custom response files using a command-based user interface, refer to “Creating Custom Response Files from a Command-Based Interface” on page 125.

## Creating a Custom Response File Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

To create a custom OS/390 LAN Server response file for front-end processor installation, follow these steps:

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the Installation Diskette/s in the A: drive for a local response file creation.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** to create the response file locally, or

   ***drive:\BFSNINST*** to create the response file from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Create or use response files'. This will bring up the 'Create or use custom response files' panel.

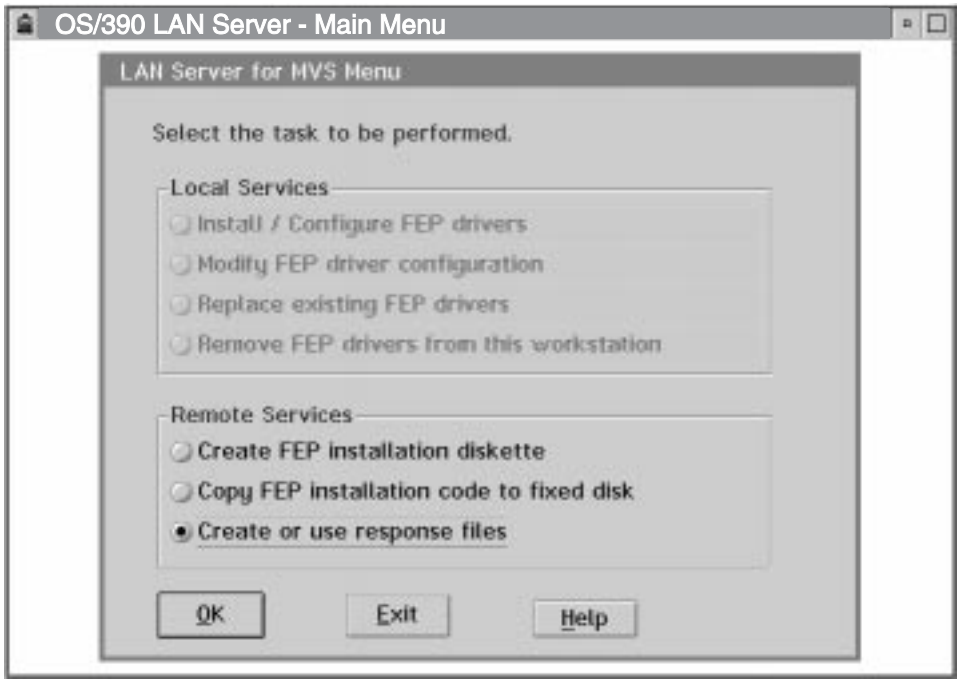


*Figure 63. OS/390 LAN Server Menu - Select Create or Use Response Files*

6. On the 'Create or use custom response files' panel, select 'Create an LS for MVS response file' and click on the 'OK' pushbutton to bring up the 'Create custom response file' panel.

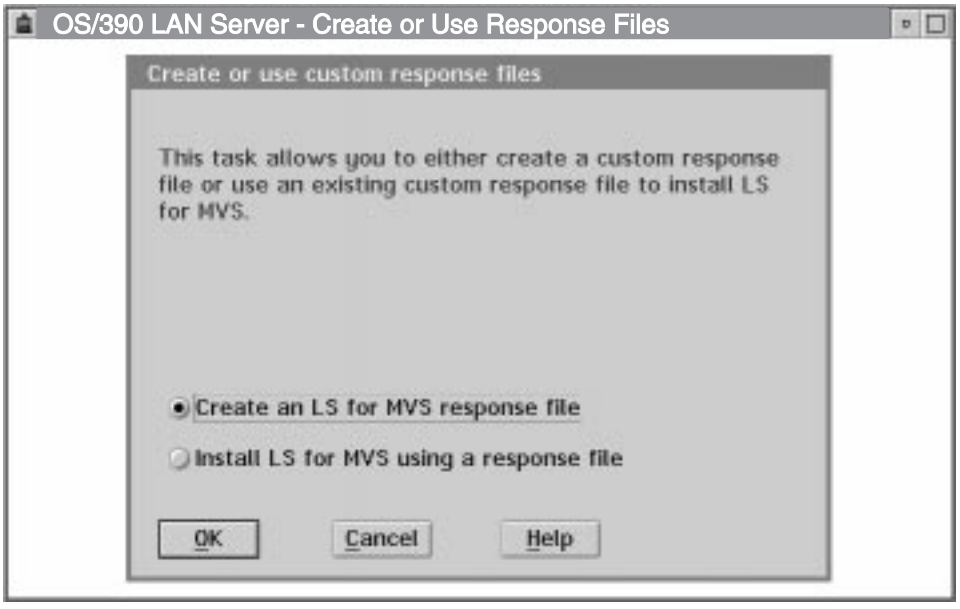


*Figure 64. Create or Use Custom Response File*

7. On the 'Create custom response file' panel, fill in the entry fields. Use the values on the Create Custom Response Files Worksheet, Table 9 on page 90, to fill in the fields. Click on the 'OK' pushbutton when you are done to bring up the 'Set configuration' panel.

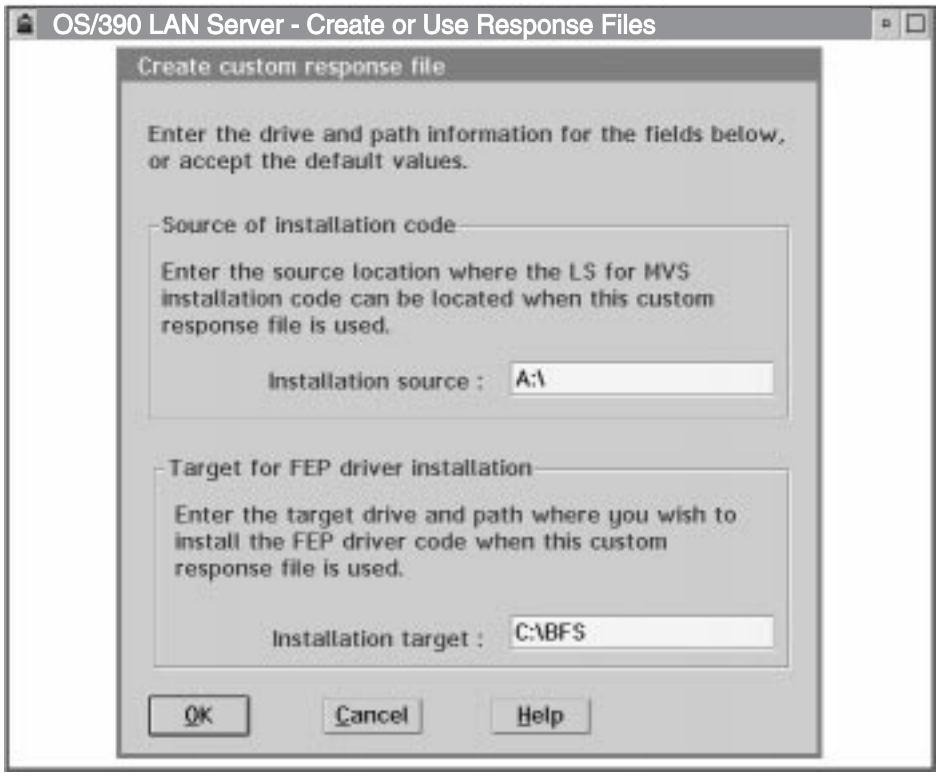


*Figure 65. Create Custom Response File*

8. On the 'Set configuration' panel, fill in the entry fields using the values from the Create Custom Response Files Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up the 'Set configuration' panel for the CLAW connection.

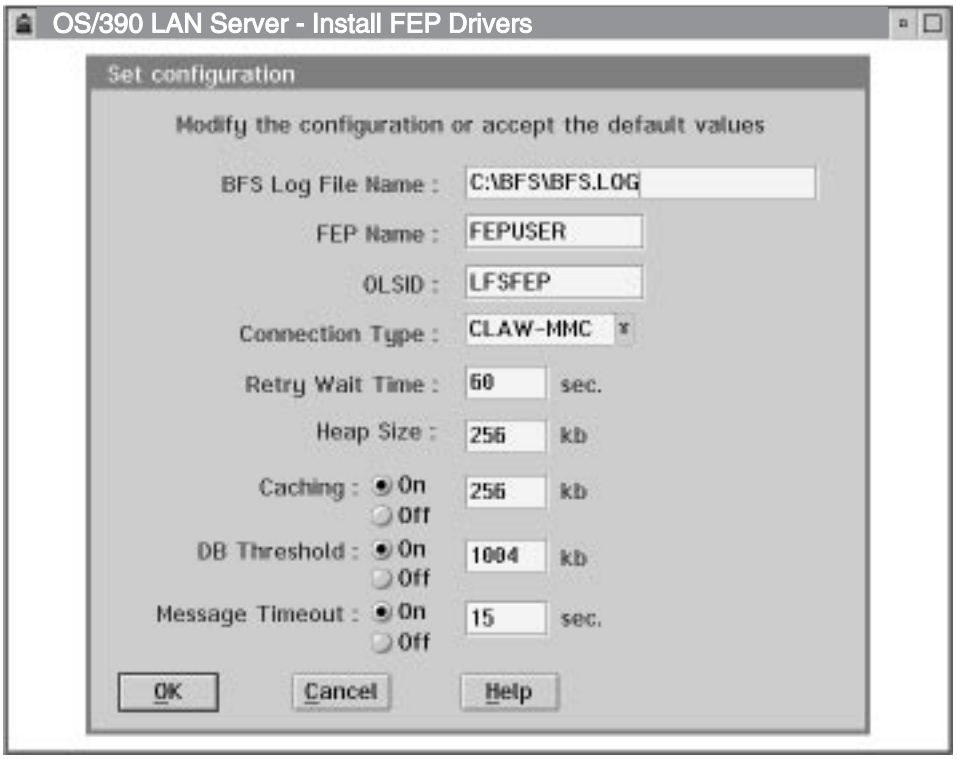


*Figure 66. Set Configuration - Modify or Accept Defaults*

9. **(CLAW-MMC CONNECTIONS ONLY)** On the 'Set configuration' panel shown below, fill in the entry fields using the values from the NFS Front-End Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up an additional 'Set configuration' panel.

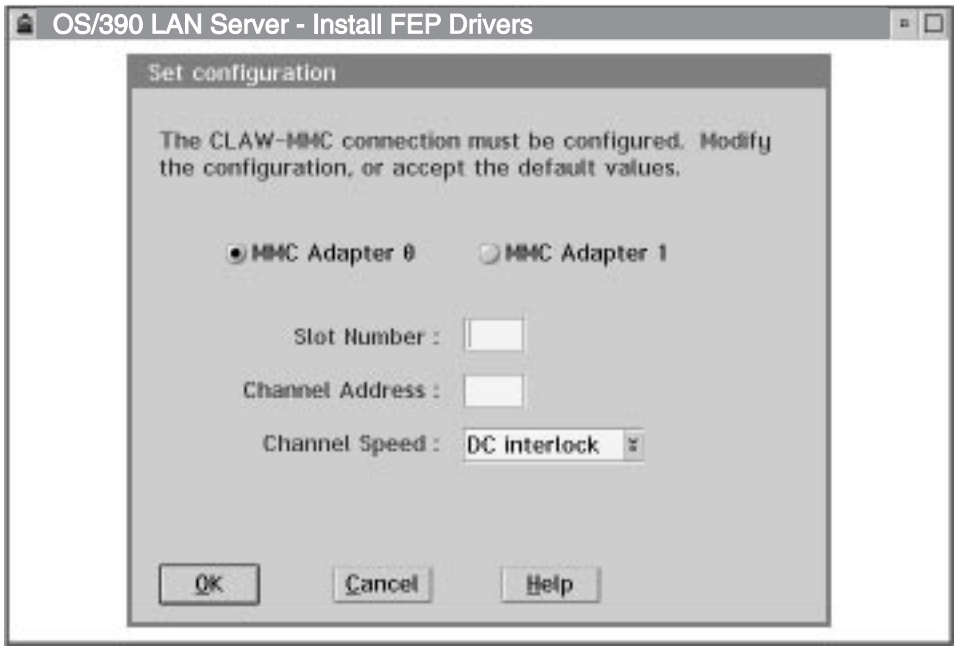


*Figure 67. Set Configuration - CLAW-MMC Connections Only*

10. **(CLAW-NSCA CONNECTIONS ONLY)** On the 'Set configuration' panel shown below, fill in the entry fields using the values from the NFS Front-End Processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up an additional 'Set configuration' panel.

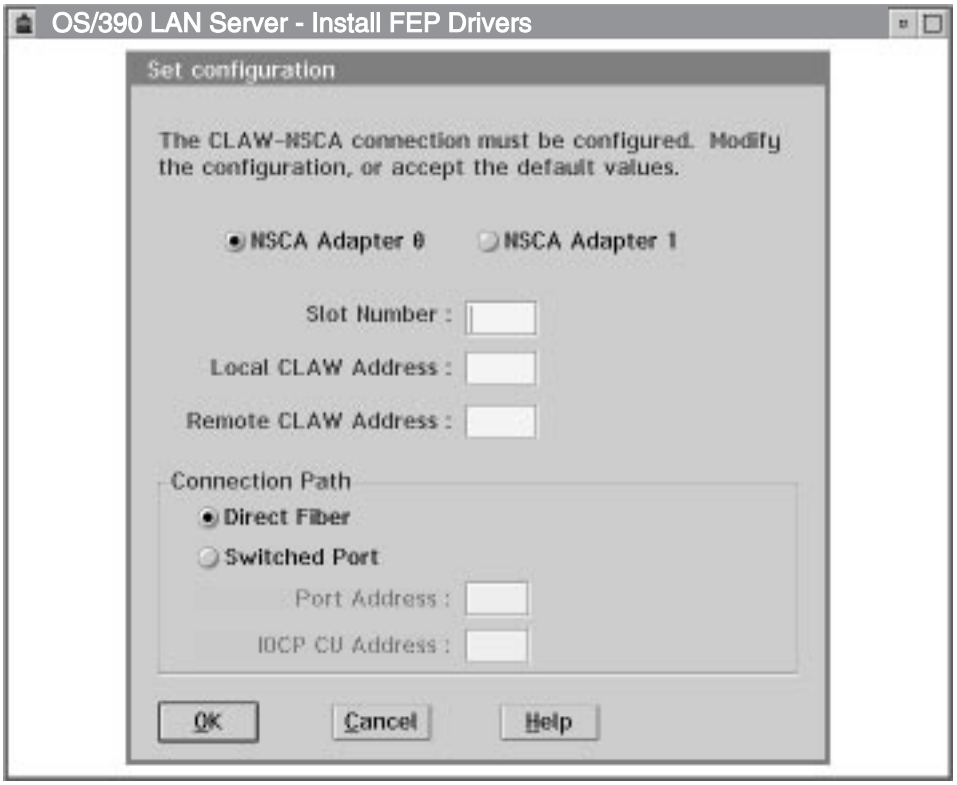


*Figure 68. Set Configuration - CLAW-NSCA Connections Only*

11. On this 'Set configuration' panel , fill in the entry fields using the values from the NFS front-end processor Installation Worksheet, Table 9 on page 90. Click on the 'OK' pushbutton when you are done to bring up the 'Save Response File to Drive' panel.
12. On the 'Save Response File to Drive' panel, either type in the drive, path and file name of the response file in the 'Save as Response File Name' field, or select your response file using the 'Drive', 'Directory', and 'File' menus. The directory specified must already exist on your system. Use the values on the Create Custom Response Files Worksheet Table 9 on page 90 to fill in the fields. Click on the 'OK' pushbutton to begin the installation process.

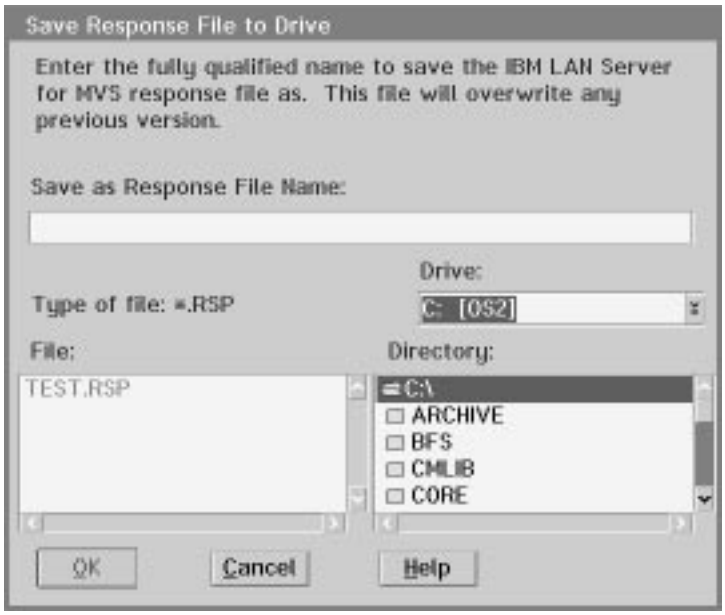


*Figure 69. Save Response File to Drive*

13. When the custom response file has been created, you will see a panel indicating the custom response file was successfully created. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Using NFS Front-End Processor Custom Response Files

Before you begin the formal process of using custom response files for the OS/390 LAN Server NFS front-end processor drivers, complete the Using NFS Front-End Processor Custom Response Files Worksheet, Table 14 below.

*Table 14. Using NFS Front-End Processor Custom Response Files Worksheet*

| Information Needed | Your Value | Where to Find It |
|---|---|---|
| **For All Connection Types** | | |
| Response File Name | | This is the drive and path and filename of the custom response file you will use to perform the FEP driver code installation. You will most likely get this filename and path from your LAN Administrator. |

## Using a Custom Response File Procedure

**GENERAL NOTE**

Throughout the remainder of this document, you will see references to ***"x:\"*** or ***"x.xx"***. This refers to the fact that the drive letters and/or version numbers can be varied. In the panel images in this document, ***C:*** is used for the examples involving a fixed disk, and ***A:*** is used for examples involving a diskette drive.

This response may also be used by a code server for a CID installation.

To use a custom OS/390 LAN Server response file for front-end processor installation, follow these steps.

1. Start the front-end processor.
2. Switch to an OS/2 window or an OS/2 full screen session.
3. Insert the Installation Diskette/s in the A: drive to use response files from your local workstation.

   For the English version, the NFS diskettes are labeled:

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 2)

   OS/390 LAN Server: English
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (2 of 2)

   For the Japanese version, the NFS diskette is labeled:

   OS/390 LAN Server: Japanese
   NFS FEP
   5647-A01 V2R5M0
   Install Diskette (1 of 1)

4. At the ***"x:\"*** prompt, type:

   ***A:\BFSNINST*** to use the response file locally, or

   ***drive:\BFSNINST*** to use the response file from a network drive.

   The OS/390 LAN Server logo screen will be displayed.

   Click on the 'OK' pushbutton to bring up the OS/390 LAN Server Menu.

5. On the OS/390 LAN Server Menu, select 'Create or use response files'. This will bring up the 'Create or use custom response files' panel.

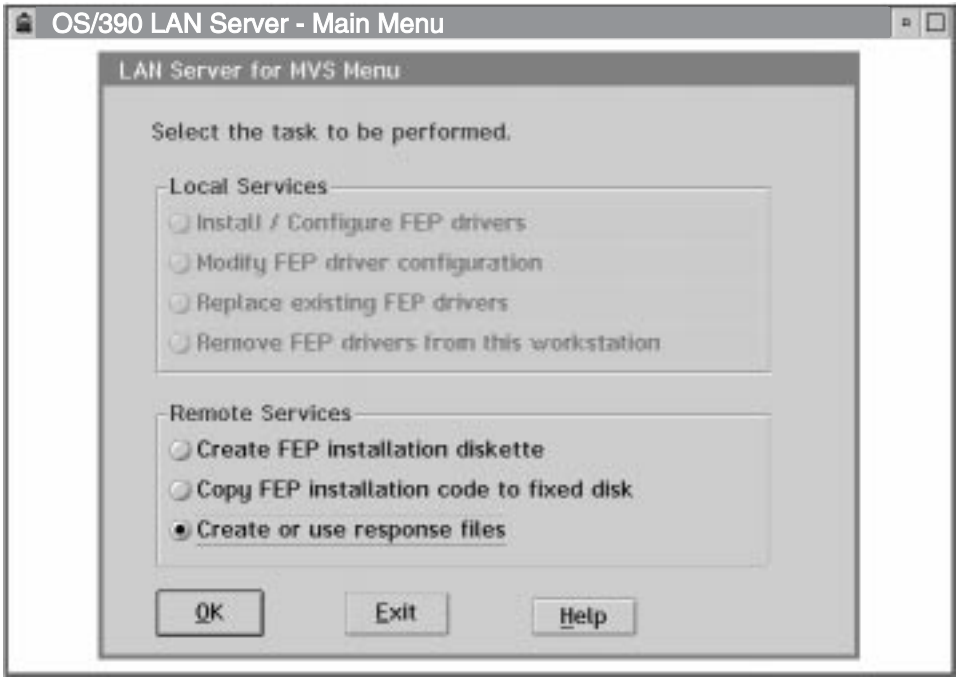


*Figure 70. OS/390 LAN Server Menu - Select Create or Use Response Files*

6. On the 'Create or use custom response files' panel, select 'Install LS for MVS using a response file' and click on the 'OK' pushbutton to bring up the 'Install Using a Response File' panel.

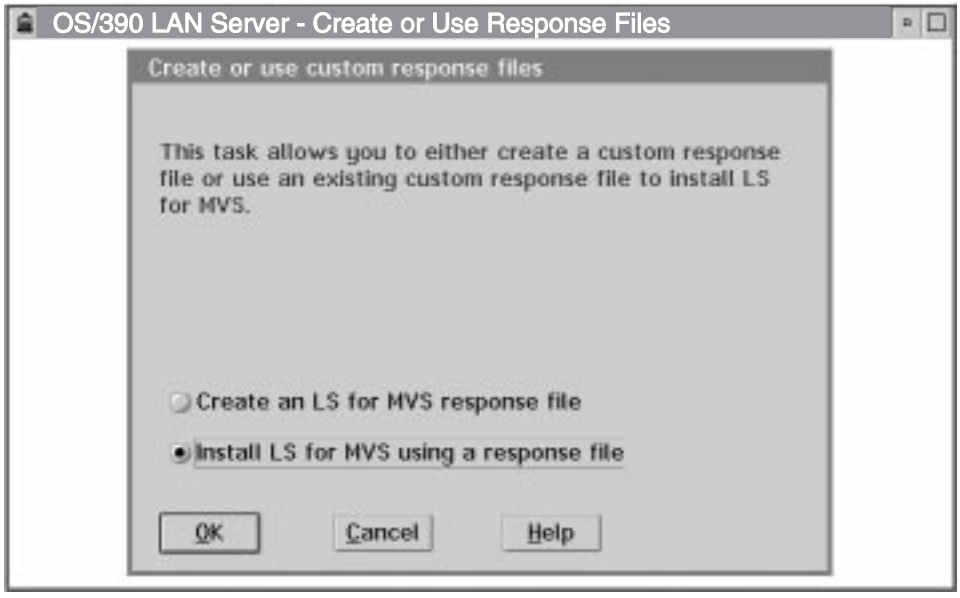


*Figure 71. Create or Use Custom Response Files*

7. On the 'Install Using a Response File' panel, either type in the drive, path, and filename of the response file in the 'Open Response File Name' field, or select your response file using the 'Drive', 'Directory', and 'File' menus. Use the values on the Using NFS Front-End Processor Custom Response Files Worksheet, Table 14 on page 122, to fill in the fields. Click on the 'OK' pushbutton to begin the installation process.

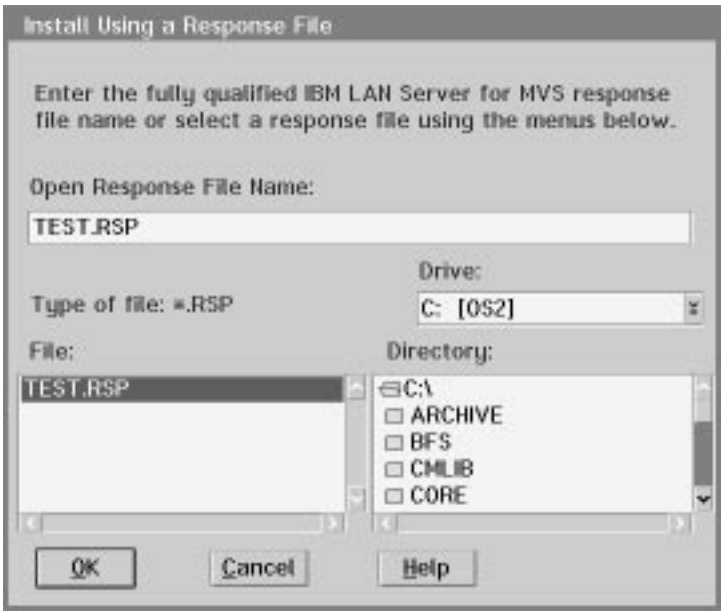


*Figure 72. Install Using a Response File*

8. While the installation progresses, you will see a panel indicating that files are being copied.
9. When the entire FEP driver installation is complete, you will see a panel indicating the front-end processor drivers and associated code were successfully installed on the system. Click on the 'OK' pushbutton, and then restart the system in order to invoke the changes.

## Creating Custom Response Files from a Command-Based Interface

OS/390 LAN Server can also be installed with a response file through the OS/2 command line rather than traversing the GUI installation interface. This feature enables the CID unattended install mode of the installation program. The installation command syntax to enable this mode is:

```
BFSINST /R:d:\path\fname1.ext /S:d:\path /T:d:\path
        /L1:d:\path\fname2.ext /L2:d:*.path\fname3.ext
```

## Parameters and Descriptions

**/R:** The value supplied is a fully qualified specification (drive, path, filename, and extension). The value is the name of the response file supported for BFSINST. The file name is expected to be in the format of *.RSP, where '*' refers to any valid filename and 'RSP' is that file extension. This is a required parameter and BFSINST will terminate if it is omitted.

**/S:** The value supplied contains the source path where the File Services front-end processor installation code is to be installed from. This parameter will override the 'LFS_INSTALL_FROM' value specified in the response file. It is an optional parameter.

**/T:** The value supplied contains the destination path where the File Services front-end processor installation code is to be installed to. This parameter will override the 'LFS_INSTALL_TO' value specified in the response file. It is an optional parameter.

**/L1:** The value supplied contains the fully qualified filename (drive, path, filename and extension) of the installation error log file. If an invalid name is specified, or if this file could not be created, the installation error logging will occur to the default filename and location (\OS2\INSTALL\BFSINERR.LOG).

**/L2:** The value supplied contains the fully qualified filename (drive, path, filename and extension) of the installation history log file. If an invalid name is specified, or if this file could not be created, the installation history logging will occur to the default filename and location (\OS2\INSTALL\BFSINHST.LOG).

## Return Codes

BFSINST will issue 1 of 2 possible return codes consistent with software distribution management (SDM) conventions. The currently supported return codes and their definitions are explained below:

| Return Code (2 byte Hex) | Description |
|---|---|
| **FE 00** | Successful program termination - Reboot and do not invoke the install again. |
| **FE 12** | Successful program termination, but severe error messages logged - Reboot, correct the error(s), and invoke the install again. |

## BFSINST Response File Format

BFSINST response files are ASCII-based files which contain keyword=value pairs and comments. Comments are generally designated by lines which have an asterisk(*) or a semicolon(:) in the first column. Any non-keyword will be ignored as well. The complete list of keywords is listed below:

| Keyword | Description |
|---|---|
| **LFS_INSTALL_FROM** | This keyword specifies where the BFSINST program is to search for the front-end processor packed files to install to the target system. This is a required parameter. |
| **LFS_INSTALL_TO** | This keyword specifies where the front-end processor executable code is to be installed on the system executing the BFSINST installation program. This is a required parameter. |
| **BFS_LOG_FILE** | This keyword specifies the name of the file (on the front-end processor) to be used to collect log and trace data for OS/390 LAN Server activities. This is an optional parameter. If this parameter is not specified, the default value of C:\BFS\BFS.LOG will be used for this file. |
| **FEP_NAME** | This keyword specifies the name of the front-end processor that is used to connect with host programs. Only alphanumeric characters or '#', '$', '@', '.', '+', or '-' are valid. A maximum of 8 characters is permitted. This is a required parameter. |
| **NFSID** | This keyword specifies the NFSID. |
| **CONNECTION** | This keyword always specifies a CLAW connection. |
| **RETRY_WAIT_TIME** | This keyword specifies the number of seconds the front-end processor should wait between retrying to contact the host resource. The value may range from 1 to 3600. If this parameter is omitted, the default value of '60' will be used. |

**FILESIZE_THRESHOLD** This indicates the file size threshold. Files smaller than this size will not be readahead buffered. The default is '336k'.

**NFS_PORT** This keyword specifies the NFS port number that will be registered with the port mapper as the NFS Server. The value may range from 1 to 65535. The default is '2049'.

**MAXUSERS** This keyword specifies the maximum number of concurrent NFS clients that are supported. The value may range from 64 to 2048. The default is '256'.

**READAHEAD_BUFFERS** This keyword specifies the total number of readahead buffers that will be used on the NFS front-end processor to satisfy NFS client read requests. The value may range from 100 to 500. The default is '100'.

**READAHEAD_BUFSIZE** This keyword specifies the amount of data that will be pre-fetched from buffered files. The value may range from 8k to 60k. The default is '32k'.

**READAHEAD_TIME** This keyword specifies the length of time that buffered data will remain cached. The value may range from 0 to 60 seconds. The default is '3'.

**SEQ_READ_THRESH** This keyword specifies the number of sequential reads that must occur before a file is buffered. The value may range from 0 to 99 reads. The default is '3'.

**RPC_BUFFERS** This keyword specifies how many buffers are preallocated by the NFS front-end processor to contain NFS request and response RPCs. The value may range from 100 to 1000. The default is '150'.

**THREADS** This keyword specifies the number of threads. The value may range from 4 to 256. The default is '16'.

**MESSAGE_TIMEOUT** This keyword specifies whether messages should be displayed at the front-end processor console, and if so, for how long. The value may range from 0 to 60 seconds. This is an optional parameter, and if omitted, will default to '0'.

**ADAPTER_NUMBER** This keyword specifies which microchannel adapter is to be used for the 'CLAW' connection. The value may be either '0' or '1'. This is a required parameter.

**DD_NAME** This keyword specifies to the system which physical connectivity the CLAW link is using. The value may be either '$PSCA' for a CLAW-MMC connection type, or '$NSCA' for a CLAW-NSCA connect type. The default is '$PSCA'.

**CLAW_ADDRESS** This keyword specifies the 370 subchannel that is to be used by the CLAW-attached adapter. This value must be any even, 2 digit, hexadecimal address. This is a required parameter for CLAW connections; otherwise it is ignored.

**ADAPTER_SLOT** This keyword specifies the workstation slot number where either the MMC or NSCA adapter card is installed. This is a required 1 digit parameter for a CLAW connection; otherwise it is ignored.

**CHANNEL_SPEED** This keyword specifies whether the CLAW connection with the MMC adapter is to run in DC interlock or streaming mode. The values may range from 0 to 4, corresponding to DC interlock, 1.9 Mb/sec, 2.7 Mb/sec, 3.4 Mb/sec, and 4.5 Mb/sec. This is a required parameter for a CLAW-MMC connection type; otherwise it is ignored.

**REMOTE_ADDRESS** This keyword specifies the hexadecimal address of the fiber connection as it is known on the ES/9000 processor. The value must be any even, 2 digit, hexadecimal address. This is a required parameter when a CLAW-NSCA connection is specified; otherwise it is ignored.

**DIRECT_FIBER** This keyword specifies what data will be used when writing the CLAW-NSCA configuration file. If the value is 'OFF', the data specified by the CU_ADDRESS and PORT_ADDRESS keywords will be used. If the value is 'ON', the value '010' will be used. This is a required parameter when a CLAW-NSCA connection is specified; otherwise it is ignored.

**PORT_ADDRESS** This keyword specifies the port number of the switch connection to the ESCON channel. The value must be any 2 digit hexadecimal address. This is a required parameter if DIRECT_FIBER = 'OFF'.

**CU_ADDRESS** This keyword specifies the value on the CUADD parameter of the CNTLUNIT statement for the ESCON channel in the IOCP table for the ES/9000. The value must be any 1 digit hexadecimal value. This is a required parameter if DIRECT_FIBER = 'OFF'.

## Sample Response File

```
Example 1 : Suppose you want to create a CLAW-MMC connected front end
            processor named 'FEPUSER', NFSID named 'LFSNFEP', a channel
            speed of 2.7Mb/sec, a single MMC adapter installed in slot
            number 4, and a channel address of x'A2'.

;
; OS/390 LAN Server - Response file
;

LFS_INSTALL_FROM = A:\
LFS_INSTALL_TO   = C:\BFS
BFS_LOG_FILE     = C:\BFS\BFSNFS.LOG
FEP_NAME         = FEPUSER
NFSID            = LFSNFEP
CONNECTION       = CLAW
RETRY_WAIT_TIME  = 60
FILESIZE_THRESHOLD = 336
MESSAGE_TIMEOUT  = OFF
NFS_PORT         = 2049
MAXUSERS         = 256
RPC_BUFFERS      = 150
READAHEAD_BUFFERS = 100
READAHEAD_BUFSIZE = 32
READAHEAD_TIME   = 3
SEQ_READ_THRESH  = 3
THREADS          = 16
```

```
CLAW_ADDRESS     = A2
ADAPTER_SLOT     = 4
CHANNEL_SPEED    = 2
DD_NAME          = $PSCA
ADAPTER_NUMBER   = 0



Example 2 : Suppose you want to create a CLAW-NSCA connected front-end
            processor named 'FEPUSER', NFSID named 'LFSNFEP', a local channel
            address of x'C4', a remote channel address of x'30', a port
            address of x'6C', and IO control unit parameter of 5.

            The target system has the OS/2 NFS FEP software installed
            on the 'Z' drive, and the front-end processor code is to be
            installed to the 'E:\BFS' drive.

;
; OS/390 LAN Server - Response file
;

LFS_INSTALL_FROM = Z:\
LFS_INSTALL_TO   = E:\BFS
BFS_LOG_FILE     = C:\BFS\BFSNFS.LOG
FEP_NAME         = FEPUSER
NFSID            = LFSNFEP
CONNECTION       = CLAW
RETRY_WAIT_TIME  = 60
FILESIZE_THRESHOLD = 336
MESSAGE_TIMEOUT  = OFF
NFS_PORT         = 2049
MAXUSERS         = 256
RPC_BUFFERS      = 150
READAHEAD_BUFFERS = 100
READAHEAD_BUFSIZE = 32
READAHEAD_TIME   = 3
SEQ_READ_THRESH  = 3
THREADS          = 16
CLAW_ADDRESS     = C4
REMOTE_ADDRESS   = 30
ADAPTER_SLOT     = 4
DIRECT_FIBER     = OFF
PORT_ADDRESS     = 6C
CU_ADDRESS       = 5
DD_NAME          = $NSCA
ADAPTER_NUMBER   = 0
```

## Error and History Logging

During either attended or unattended (CID) installation, a history file shall be created. The default name for this file is BFSINHST.LOG and will be located in the system's \OS2\INSTALL directory. This file records all significant events of each of the OS/390 LAN Server options. The default filename and location may only be changed during a command line (unattended) installation as specified by the /L2 parameter.

If an error is encountered during any OS/390 LAN Server installation/ configuration task, details concerning the error shall be logged. The default name for this file is BFSINERR.LOG and will be located in the system's \OS2\INSTALL directory. The default filename and location may only be changed during a command line (unattended) installation as specified by the /L1 parameter.

# Chapter 5. NFS Server Installation Verification

## NFS Server Verification

This section applies only to the OS/390 portion of the OS/390 LAN Server NFS and NFS/OLS environments. For installation verification of the OS/390 LAN Server NFS environment that involves an NFS front-end processor, refer to “NFS Front-End Processor Installation Verification” on page 98.

The following verification steps can be performed after completing all installation steps to verify the success of your OS/390 LAN Server installation:

1. From the OS/390 console on the host, start the OS/390 LAN Server host server.

**start runlfs**

```
Execution begins...
                                        .
                                        .
                                        .
File Services Version 1.1.2000, built MM/DD/YY HH.MM.SS, is ready
File Services is now the resource manager of resource adminid
```

2. From an NFS client, issue a MOUNT command for the /trylfs file system.

   **Note:** This assumes that the trylfs file system was defined and created on the OS/390 host.

   a. The following MOUNT command would be used on an RS/6000* workstation:

**mount -n** *mvshost* **-v nfs -o soft,retry=1,ro /trylfs,ro /***mountpoint*

*mvshost* is the TCP/IP hostname for the OS/390 system on which OS/390 LAN Server is installed.

*mountpoint* is the point in the local file system to which you want to mount the OS/390 LAN Server directory.

**Notes:**

1. soft,retry=1 are recommended just in case the installation did not complete correctly.
2. ro must be specified in both the logical and host option strings.
3. /trylfs is the remote file system. This must be entered in lowercase characters, as shown.

   b. The following MOUNT command would be used on a PS/2 workstation:

**mount h:** *mvshost***:/trylfs,ro**

*mvshost* is the TCP/IP hostname for the OS/390 system on which OS/390 LAN Server is installed.

**Notes:**

1. ro must be specified in both the logical and host option strings.
2. /trylfs is the remote file system. This must be entered in lowercase characters, as shown.

3. Complete the OS/390 LAN Server verification:

   a. The following command would be issued on an RS/6000 workstation:

**ls -la /***mountpoint*

The contents of the /trylfs file system should be listed on your screen in the form *filename.filetype* entered in lowercase.

   b. The following command would be issued on a PS/2 workstation:

**dir h:**

The contents of the /trylfs file system should be listed on your screen in the form *filename.filetype* entered in lowercase.

**Note**

NFS verification for OS/390 is now complete.

## Terminate the NFS verification

1. On the front-end processor, terminate **BFSSERV**.

   You can end BFSSERV by closing the front-end processor window. Close the front-end processor panel by :

   - Clicking on ***Close*** on the OS/2 pull down menu OR
   - Pressing 'F3' OR
   - Pressing 'ALT-F4'

2. From the host, reinitialize the OS/390 LAN Server server before making it available to the user community, using one of the following two commands.

**stop runlfs**

OR

**f runlfs,shutdown**

**Note**

You are ready to place OS/390 LAN Server in production.

# Startup/Shutdown Procedures

## Host Startup

The OS/390 operator can start OS/390 LAN Server by entering **start runlfs**.

## Host Shutdown

To stop OS/390 LAN Server, enter one of the following commands:

- To shut down OS/390 LAN Server from a TSO/E administrator, enter **shutdown**.
- From an OS/390 console, enter **stop runlfs**.

# Chapter 6. SNA Configuration Information

## SNA Configuration Using Extended Services

### Introduction

The problem this section solves is how to get SNA (LU6.2) connectivity between a PC with an OS/2 Operating System and its products and an OS/390 Host system and its products. When you see five (5) to seven (7) products using different terms for the same information, it can be very confusing knowing what to input for each term. This document attempts to explain what parameters have to be configured in each environment and how those parameters relate between the different products.

When configuring communications packages such as NS/2, CM/2 or Extended Services, a .NDF file is created which is the KEY to SNA(LU6.2) communications. This file can then be tailored to support numerous C/S products.

### Product Terms

- ES - Extended Services. IBM communications product
- CM/2 - Communications Manager/2. IBM communications product
- NS/2 - Networking Services/2. IBM communications product
- VTAM - Virtual Telecommunications Access Method
- SNA - Systems Network Architecture. IBM mainframe oriented network architecture
- LU6.2 - Special type of logical unit that supports Advanced Program-to-Program Communications (APPC)

## Software for SNA Connectivity

To configure OS/390 LAN Server to use SNA connectivity, you must have:

PC Software

1. Extended Services Release 1.0 installed on your OS/2 workstation
2. For OS/2 Version 1.32 workstations, APAR JR05162 must be installed to Extended Services.
3. For OS/2 Version 2.0 workstations, APAR JR06123 must be installed to Extended Services.
4. LAN Server 3.0 Advanced, used with OS/390 LAN Server

After this SNA configuration information is completed, it will create a **.NDF** to establish communications with the SNA network.

OS/390 Software

1. VTAM

## Preparing for a SNA Configuration

You need to have the following information before beginning the configuration.

| Information | Where you get the information |
|---|---|
| Independent LU | Defined by your local IS organization; must specify independent LU (Type 6.2) on the request. |
| Type 2.1 SNA Node | Your workstation should automatically use this when you use an independent LU (Type 6.2). Type 2.1 SNA node was previously called a PU Type 2.1. |
| PU | Defined by your local IS organization. |
| Node ID (hex) | Defined by your local IS organization; corresponds to VTAM IDBLK and IDNUM operands. |
| Network Name | Defined by your local IS organization. |
| LAN Destination Address | Defined by your local IS organization. |
| SNA Config File for Comm. Mgr. | Copy your current Communications Manager Configuration File to a new *.CFG name. Use this name when you make the SNA changes to Communications Manager. |
| OLSID | Located in \BFS\BFS.INI during OS/390 LAN Server installation; must match the OLSID of the OS/390 LAN Server server. (This is also equal to the VTAM APPLID for OS/390.) |
| FEP Name | Located in \BFS\BFS.INI during OS/390 LAN Server installation. |
| MODE Name | Name assigned to a set of session capabilities. For an LU, the name is installation dependent, but it is recommended that BFSLMOD be used for OS/390. This name must match your VTAM LOGMODE or DLOGMODE operand. |
| VTAM Definitions | Included in the Sample Files Appendix. |

## Extended Services SNA Configuration

1. Select the "Communications Manager" icon.
2. Double Click on **SNA Network Definitions Configurations** icon.

## Configuring Local Node Characteristics

1. Enter the name of your SNA Configuration File for the 'Enter node definitions (NDF) file name' field. This file should have the SAME name as your Communications Manager SNA Config File.
2. Select the **Open** pushbutton.
3. An informational panel may appear. You will only see the 'Creating basic SNA node information' panel if you have never configured any SNA parameters. If you see it, select **OK** and continue with 5 on page 137.
4. The panel 'SNA Network Definitions Selection' will appear if you **have** previously configured some SNA features.

   Highlight **Local Node Characteristics** and select **Configure**.

5. Fill in the parameters on the 'Local Node Characteristics' panel.
    a. **Network ID** = USIBMNY (You get this value from your local IS organization.)
    b. **Local Node Name** = the PU you get from your IS organization.
    c. **Node Type** = Network Node.
    d. **Local Node ID** = the hexadecimal ID you got from your local IS organization.
    e. **Local Node alias name** = the same as your *Local Node Name*.
    f. **Comment** is optional, but you may, for example, type *My SNA configuration*.
    g. De-select **Activate Attach Manager at start up** field (it will then be blank when de-selected).
    h. Click on **Verify and Return**.
6. You may get an 'Information Messages Logged' panel. If the text indicates that the file is considered to be successfully installed, you may ignore this message and click **OK**. If, however, the text indicates there were errors, then you must return to 5 to fill in the parameters in the 'Local Node Characteristics' panel.
7. When the 'Basic SNA Node Information Created' panel appears, click **OK**. You now have a basic SNA configuration for your workstation.

## Configuring Additional SNA Features

1. From the 'SNA Network Definitions Selection' panel, highlight **Additional SNA features** and click on **Configure**.
2. Select **View** and click on **Expand All**.
3. Double click on **Partner LUs**.
4. Fill in the parameters on the 'Changing a Partner LU' panel.
    a. **Fully qualified LU name** = the **Network ID** plus the VTAM APPLID. This will also be equal to the OLSID for OS/390.
    b. **Alias** = your alias name for the host.
    c. **Conversation Security**. Leave this field *Blank*.
    d. **Comment**. Optional.
    e. Click on **OK**.
5. You will return to the 'Additional SNA Features:' panel.

    Double click on **Local LUs**.
6. The 'Changing a Local LU' panel will appear. Fill in the fields as follows:
    a. **LU Name** = the Independent LU # you received from your local IS organization. Normally IS distributes Dependent LUs, not Independent LUs.
    b. **Alias** = any name, different than your Partner LU Alias.
    c. **NAU Address** = Independent LU.
    d. **Comment**. Optional.
    e. Click on **OK**.

7. You will return to the 'Additional SNA Features' panel.
8. Double click on **Conversation Security**. This will display the 'Creating Conversation Security' panel.
    a. Click on **Utilize User Profile Management**. This will cause an * to be put in the *User ID field*.
    b. Click on **Save**.
    c. Click on **OK**.
9. You will return to the 'Additional SNA Features:' panel.

    Double click on **CPI Communications Side Info**.
10. Fill in the parameters on the 'Changing a Side Information' panel.

    a. **Symbolic Destination Name** = the OLSID from your BFS.INI file.
    b. Click on **Fully qualified name**. Enter The **Network id** plus the VTAM APPLID which will be equal to your olsid for OS/390.
    c. **TP Name** = the OLSID from your BFS.INI file.
    d. **Security Type** = **Same**.
    e. **Mode Name** = **BFSLMOD** for OS/390 (these values are recommended), AVS or VTAM logon mode table.
    f. **Comment**. Optional.
    g. Click on **OK**.
11. You will again return to the 'Additional SNA Features:' panel.

    Double click on **Modes**.
12. Fill in the parameters for the 'Creating a Mode Definition' panel.

    a. **Mode name** = **BFSLMOD** for OS/390 is recommended, AVS or VTAM logon mode table.
    b. **Class of service** = #CONNECT. Leave this default. This may have to be defined under VTAM using CLAS of Service names. Refer to Appendix B for helpful VTAM manuals.
    c. **Mode Session Limit** = 4. Must be set to **4**.
    d. **Minimum Contention winners** = 4. Must be set to **4**.
    e. **Receive Pacing window** = 8. Must be set to **8**.
    f. Under *RU Size*, choose **Maximum RU size**. Set the Maximum RU size to **1024**.
    g. **Comment**. Optional.
    h. Click on **OK**.
13. You will return to the 'Additional SNA Features' panel.

    Select **File** and then click on **Verify**.
14. You may see a window 'Informational Messages Logged'. If the text indicates that the file is considered to be successfully verified, you may ignore the window and click on **OK**.

15. Select **File** and then click on **Exit** from the 'Additional SNA Features' panel.

## Configuring Connections

1. From the 'SNA Definitions Selection' panel, highlight **Connections** and click on **Configure**.
2. The 'SNA Connections' panel will appear.
   a. **Link Name** = LINK0001. Leave the default.
   b. **Partner network ID** = Network ID.
   c. **Partner node name** = VTAM APPLID name of the front-end processor. Must be the same as the OLSID for OS/390.
   d. **LAN Destination address** = LAN address you are connecting to.
   e. **Comment**. Optional.
   f. Click on **OK**.
3. Select **File** from the 'SNA Connections' panel, and then click on **Verify**.
4. When you are returned to the 'SNA Network Definitions Selection' panel, click on **Exit**.

**Note**

All of these SNA configuration menus create a .NDF file. If you make changes directly to this file by editing, you **MUST** verify using the Verify SNA Network Definitions Icon. After you verify it, you must verify the new configuration in Communications Manager. This is explained in the section *Changing the Communications Manager Configuration* under *Verifying Communications Manager (Picks up the verified .NDF file)* section.

## Checking Your SNA CONFIG Log File for Errors

1. Double click on the **Communications Manager** Icon.
2. Double click on **Display SNA Configuration Log** Icon.

   On the panel, enter the name of your SNA CONFIG file in the field. Click on **Open**.
3. Check for any error messages on the displayed 'SNA Configuration Log' panel.
   a. If you see error message **APN0534I**, ignore it. We don't want to auto-start the attach manager.
   b. Close the window.

## Important Addition to Your SNA Configuration (NDF) File

To edit the NDF file, change directories to \CMLIB\APPN. Then follow these steps:

1. Edit your SNA .NDF file so your SNA configuration knows which alias is the default alias.
2. The following line must be added in the **DEFINE_DEFAULTS** section after the **DEFAULT_MODE_NAME(BLANK)** parameter:

```
DEFAULT_LOCAL_LU_ALIAS(LOCALLUA)
```

**LocalLUA** must be eight characters in length. The value for the **LocalLUA** must match the alias defined for the Local LU Alias earlier. If the value for **LocalLUA** is less than 8 characters, you **must** pad the value with blanks. For example, if the **LocalLUA** is **LOCAL3**, this statement would be entered as:

```
DEFAULT_LOCAL_LU_ALIAS(LOCAL3  )   2 blanks are added so this
                                   field is 8 characters long.
```

3. After this line is added, **Save** and Exit this file.
4. Verify changes in Communications Manager. This is explained in the *Changing the Communications Manager Configuration*, under *Verifying Communications Manager* (Picks up the verified.NDF file) section.

## Verify SNA Changes to .NDF File

1. Double click on the **Verify SNA Network Definitions** icon.
2. Press **enter**.
3. You should see no errors on the displayed 'Verify SNA Network Definitions' panel. If you **do** see errors, go back to the previous page and check your syntax and information.
4. Press **enter**.
5. Next, go into Communications Manager and verify that the new .NDF file is being used.

---

## Changing the Communications Manager Configuration

You must have an existing Communications Manager .CFG file before starting this section.

Double Click on the **Communications Manager** Icon.

## Change Default Communications Manager CONFIG File to be Used.

1. From the Communications Manager Main Menu, select **Specify new Configuration File name default**.
2. Type in the name of your SNA CONFIG File. This file should be the one you created by copying your original Comm. Mgr. CONFIG File to this SNA CONFIG File name.
3. You might see the following popup message:

```
The Active LAN Configuration File PROTOCOL.INI is used
when configuring this workstation.
Changes will be saved in XXXXXX.INI after verification.
```

where XXXXXX.INI refers to your SNA CONFIG File for Comm. Mgr.

4. You want to select the first choice, since we want to use this configuration file on this machine.

## Changing Your Communications Manager SNA Configuration File.

1. From the Communications Manager Main Menu, select **Advanced**.
2. Then, select **Configuration**.
3. Enter the name of your Communications Manager SNA CONFIG File.
4. Click on **Enter**.
5. You might see the following screen:

```
                                Select Configuration Usage


   x   Select this option if you intend to use this configuration
       file on this workstation.


   _   Select this option if you DO NOT intend to use this configuration
       file on this workstation.

   Will have a Pop-up menu over the 2nd choice that says:

       The Active LAN Configuration File PROTOCOL.INI is used when
       configuring this workstation.
       Changes will be saved in XXXXXX.INI after verification.

   where XXXXXX.INI refers to your SNA CONFIG File for Comm. Mgr.
```

6. You want to select the first choice, since we want to use this configuration file on this machine.
7. Double click on **LAN adapter and Protocol support**. This creates a .INI file in the \IBMCOM subdirectory. The INI file will have the same name as your Communications Manager SNA CONFIG File.
8. Look under *Current Configuration* and check to see if you have **IBM OS/2 NETBIOS**. If you **don't**, go to step 9; otherwise go to step 10.
9. Go to *Protocols*. Click on **IBM OS/2 NETBIOS**. Click on **Add**. Make sure you see this added under *Current configuration*.
10. Click on **OK**.
11. Highlight *Configuration complete* and click on **OK**.

## Verifying Communications Manager (Picks Up Verified .NDF File)

1. Select **Verify** and then click on **Run Verify**.
   - If you see the following message:

     ```
     Verification of the configuration file complete.
     Minor inconsistencies found. Select Messages from
     the Communications Manager Menu.
     ```

     Click on **Enter**.
   - If you see the following message:

     ```
     To use this configuration, you must stop and
     restart your system and Communications Manager.
     ```

Click on **Enter**.

- Select **Exit**, and click on **Exit Communications Manager Configuration**.

2. Look at messages.
   - Select **Messages**. After you get to the actual messages, look for the following:

     Should see "End of configuration verification errors have occurred."
   - Select F7 to see previous message:

     Should see error message APN0534I.

     If you see a different error message, look up the error and fix the problem.
   - Select F7 to see previous message:

     Should see "Start of verification test for your configuration file".
3. Stop Communications Manager.
4. Shutdown and reboot your system.
5. Start Communications Manager. Start a session.
6. Do you get a terminal session? If **yes**, everything seems OK. If **no**, then talk to your IS people. Also, check the section on "*Common Communication Configuration Errors*".
7. If you get a blank terminal session, make sure IS has activated your PU# and LU#'s.

---

# SNA Configuration for CM/2

## Introduction

The problem this section solves is how to get SNA (LU6.2) connectivity between a PC with an OS/2 Operating System and its products and an OS/390 Host system and its products. When you see five (5) to seven (7) products using different terms for the same information, it can be very confusing knowing what to input for each term. This document attempts to explain what parameters have to be configured in each environment and how those parameters relate between the different products.

When configuring communications packages such as NS/2, CM/2 or Extended Services, a .NDF file is created which is the KEY to SNA(LU6.2) communications. This file can then be tailored to support numerous C/S products.

## Product Terms

- ES - Extended Services. IBM communications product
- CM/2 - Communications Manager/2. IBM communications product.
- NS/2 - Networking Services/2. IBM communications product
- NTS/2 - Network Transport Services/2. IBM product that contains the LAN Adapter and Protocol Support (LAPS) application
- VTAM - Virtual Telecommunications Access Method
- SNA - Systems Network Architecture. IBM mainframe oriented network architecture

- LU6.2 - Special type of logical unit that supports Advanced Program-to-Program Communications (APPC)

## Software for SNA Connectivity

To configure OS/390 LAN Server to use SNA connectivity, you must have:

PC Software

1. OS/2 Version 2.0 installed on your workstation
2. Network Transport Services/2 LAN Adapter and Protocol Support (LAPS)
3. Communications Manager/2 1.0
4. LAN Server 3.0 Advanced for OS/390 LAN Server
5. LAN Server 4.0 Advanced for OS/390 LAN Server

After this SNA configuration information is completed, it will create a **.NDF** to establish communications with the SNA network.

OS/390 Software

1. VTAM

## Preparing for a SNA Configuration

You need to have the following information before beginning the configuration.

| Information | Where you get the information |
|---|---|
| Independent LU | Defined by your local IS organization; must specify independent LU (Type 6.2) on the request. |
| Type 2.1 SNA Node | Your workstation should automatically use this when you use an independent LU (Type 6.2). Type 2.1 SNA node was previously called a PU Type 2.1. |
| PU | Defined by your local IS organization. |
| Node ID (hex) | Defined by your local IS organization; corresponds to VTAM IDBLK and IDNUM operands. |
| Network Name | Defined by your local IS organization. |
| LAN Destination Address | Defined by your local IS organization. |
| VTAM APPLID Name | VTAM (OS/390) administrator. |
| OLSID | Located in \BFS\BFS.INI during OS/390 LAN Server installation; must match the OLSID of the OS/390 LAN Server server. (This is also equal to the VTAM APPLID for OS/390.) |
| FEP Name | Located in user ID of the CPIC side information parameter in CM/2 and in \BFS\BFS.INI during OS/390 LAN Server installation. |
| MODE Name | Name assigned to a set of session capabilities. For an LU, the name is installation dependent, but it is recommended that the name BFSLMOD be used for OS/390. This name must match your VTAM LOGMODE or DLOGMODE operand. |
| VTAM Definitions | Included in the Sample Files Appendix. |

## Installing/Configuring NTS/2 LAPS

Communications Manager/2 will not run without LAPS installed.

Select the *OS/2 system* Icon; click on *Command prompts*, and then click on an *OS/2 Full screen* Icon.

After bringing up the *OS/2 Full screen* and placing the *LAPS Diskette* in the A: drive, type **A**:**LAPS** and select <**enter**>.

1. Click on **Install** from the 'LAN Adapter and Protocol Support' panel.
2. Type in *Drive Letter* of your Boot Drive and click on **OK**.
3. If you have Extended Services installed, you will see '*You have an earlier version of LAPS on your system. Do you want to upgrade it?*' Click on **Yes**.
4. On the 'Installation Complete' information message window, click on **OK**.
5. Next, you will return to the main panel for the 'LAN Adapter and Protocol Support'. Click on **Configure**.
6. Select **Configure LAN transports** and click on **Continue**.
7. The 'Configure Workstation' panel will be displayed. Check the current configuration. If it **doesn't** list *IBM OS/2 NETBIOS* and/or *IBM IEEE 802.2*, then go to step 8; otherwise click on **OK** and go to step 10.
8. Select *IBM OS/2 NETBIOS* and click on **Add**. You should then see this added to your current configuration.
9. Select *IBM IEEE 802.2*, if it's not part of your current configuration, and click on **Add**. You should then see this added to your current configuration.
10. Click on **OK**.
11. Next, you will again return to the main panel for the LAN Adapter and Protocol Support.

    Click on **Exit**.
12. Select your current **Boot** drive as the drive to update.
13. On the informational message window 'CONFIG.SYS Updated', click on **OK**.
14. The 'Exiting LAPS' panel will then be displayed. Click on **Exit**.
15. Remove the diskette, shutdown, and reboot your machine.

## CM/2 Setup/Installation for SNA

If configuring an existing Communications Manager Configuration File, proceed to the section '**Configure Existing Configuration for CM/2**'; otherwise continue.

## New Installations

Select the *OS/2 System* Icon; click on *Command Prompts*, and then click on an *OS/2 Full Screen* Icon.

After bringing up the OS/2 full screen and placing Disk 1 in the A: drive, type **A:CMSETUP** and select <**enter**>.

1. You will see an information screen that indicates temporary files are being copied to your startup drive and that they will be erased after the installation is complete.
2. Next you will see the panel 'Installation Notes'. Click on **Continue**. Refer to the section, '**Installing/Configuring NTS/2 LAN Adapter Protocol Support (LAPS)**' program, if LAPS is not installed and/or configured for NETBios and IBM IEEE 802.2.
3. On the 'Target Drive Selection' panel, highlight the drive that you want to install to and click **OK**.
4. If you have Extended Services or Communications Manager/2 installed currently, you will see a warning. The warning indicates that it is already installed and will be reinstalled.

   When you click **OK**, you will see another informational message indicating that product files are being removed. CM/2 removes the previous versions' files before reinstalling.
5. The 'Communications Manager Setup' panel will appear. Click on **Setup**. This will install and configure CM/2.
6. When the 'Insert Diskette' panel appears, remove diskette **1** and insert diskette **2**. Click on **OK**.
7. You will see a screen indicating that the files are being copied from diskette 2.
8. When the 'Insert Diskette' panel appears, remove diskette **2** and insert diskette **3**. Click on **OK**.
9. You will see a screen indicating that the files are being copied from diskette 3.
10. Go to “Configuring CM/2” to continue.

## Configure Existing Configuration for CM/2

1. Select the **Communications Manager/2** icon.
2. Double click on the **Communications Manager Setup** icon.
3. On the 'Communications Manger Setup' panel, click on **Setup**. This will configure CM/2.
4. Continue with “Configuring CM/2.”

## Configuring CM/2

1. On the 'Open Configuration' panel, enter the name of your SNA Configuration File and click on **OK**.
2. If this is a new configuration file, you will see a warning panel that indicates that configuration file specified was not found. To create the file, click on **Yes**.
3. You may see an informational panel appear asking if the configuration will be used for the workstation. Answer the question by clicking on **Yes**.
4. The 'Communications Manager Configuration Definition' panel will appear next. Highlight **Token_ring or other LAN types**, and double click on **APPC APIs:ehp2 to bring up the profile list sheet.**
5. On the 'Communications Manager Profile List Sheet' panel, double click on **DLC-Token-ring or other LAN types** to configure.

6. When the 'Token Ring or Other LAN Types DLC Adapter Parameters' panel appears, enter the PU name for the **C&SM LAN ID** field. The rest of the parameters should be OK as defaults.
7. Click on **OK** to return to the 'Communications Manager Profile List Sheet' panel.
8. Double click on **SNA local node characteristics** to configure.
9. Fill in the parameters on the 'Local Node Characteristics' panel.
    a. **Network ID** = USIBMNY (You get this value from your local IS organization.)
    b. **Local Node Name** = the PU you get from your local IS organization.
    c. **Node Type** = Network Node.
    d. **Local Node ID** = Leave the 1st 3 hex digits **05D**, and enter the 5 digit hexadecimal ID you got from your local IS organization.
    e. **Local Node alias name** = the same as your *Local Node Name* (use capital letters).
    f. **Comment**. Optional.
    g. De-select **Activate Attach Manager at start up** field; should be blank when de-selected.
    h. Click on **OK** to return.
10. You will again be returned to the 'Communications Manager Profile List Sheet' panel. Double click on **SNA connections** to configure.
11. On the 'Connections List' panel, both connections types will need to be LEN node or host to work. Click on **To LEN node** and continue with these steps. Otherwise, click on **To Host** connection, and continue with step 16 on page 147.
12. Click on **Create**.
13. On the 'Adapter List' panel:
    a. Highlight the type of connection you have. Usually this will be Token-ring.
    b. Enter the number of your adapter. If you have only one LAN card installed, this will be **0**.
    c. Click on **Continue**.
14. Fill in the parameters on the 'Create a Connection to a LEN node' panel.
    a. **Link Name** = LINK0001 (leave the default).
    b. **Partner network ID** = Network ID.
    c. **Partner node name** = VTAM APPLID.
    d. **LAN Destination address** = LAN address you are connecting to.
    e. **Comment**. Optional.
    f. Click on **OK**.
15. You will be returned to the 'Connection List' panel. Click on **Close**. To continue, skip the next section that would have been used to configure the host connection (the other choice), and refer to step 20 on page 147.

16. On the 'Connections List' panel, click on **To host** to configure a *To host* connection.

    Then click on **Create**.

17. On the 'Adapter List' panel:
    a. Highlight the type of connection you have. Usually this will be Token-ring.
    b. Enter the number of your adapter. If you have only one LAN card installed, this will be **0**.
    c. Click on **Continue**.
18. Fill in the parameters on the 'Create Connection to a Host' panel.

    a. **Link Name** = HOST0001 (leave the default).
    b. **LAN Destination address** = LAN address you are connecting to.
    c. **Partner network ID** = Network ID.
    d. **Partner node name** = VTAM APPLID for OS/390.
    e. **Local PU Name** = the PU you get from your local IS organization.
    f. **Node ID** = Leave the 1st 3 hex digits **05D**, and enter the 5 digit hexadecimal ID you got from your local IS organization.
    g. De-select **Use this host connection as your focal point**.
    h. De-select **APPN support** if it is check marked.
    i. **Comment**. Optional.
    j. Click on **OK**.
19. You will be returned to the 'Connection List' panel. Click on **Close** and continue.
20. You will then be returned to the 'Communications Manager Profile List Sheet' panel. Double click on **SNA features** to configure.
21. On the 'SNA Features List' panel, highlight **Local LUs** and click on **Create** to bring up the features list.
22. Fill in the parameters on the 'Create a Local LU' panel.
    a. **LU Name** = the Independent LU # you received from your local IS organization. Normally IS distributes Dependent LUs, not Independent LUs.
    b. **Alias** = any name, different than your Partner LU Alias.
    c. **NAU Address** = Independent LU.
    d. **Comment**. Optional.
    e. Click on **OK**.
23. You will be returned to the 'SNA Features List' panel. Highlight **Partner LUs**, and click on **Create**.
24. Fill in the parameters on the 'Create a Local LU' panel.
    a. **Fully qualified LU name** = the **Network ID** plus the VTAM APPLID.
    b. **Alias** = your alias name for the host. This name can be any name that is different than your Local LU alias name.

c. **Conversation Security**. Leave this field *Blank*.

d. **Dependent Partner LU**. Leave the fields here blank.

e. **Comment**. Optional.

f. Click on **OK**.

25. Highlight **Modes** on the 'SNA Features List' panel and click on **Create**.

26. Fill in the parameters on the 'Create a Mode Definition' panel.

    a. **Mode name** = **BFSLMOD** for OS/390 is recommended.

    b. **Class of service** = #CONNECT. Leave this default. This may have to be defined under VTAM using CLAS of Service names.

    c. **Mode Session Limit** = 4. Must be set to **4**.

    d. **Minimum Contention winners** = 4. Must be set to **4**.

    e. **Receive Pacing window** = 8. Must be set to **8**.

    f. Under *RU Size*, choose **Maximum RU size**. Set the Maximum RU size to **1024**.

    g. **Comment**. Optional.

    h. Click on **OK**.

27. Highlight **Conversation Security** on the 'SNA Features List' and click on **Create**.

28. On the 'Create Conversation Security' panel:

    a. Click on **Utilize User Profile Management**. This will cause an * to be put in the *User ID field*.

    b. Click on **Add**.

29. On the 'Create Conversation Security' panel, click on **OK**.

30. The 'SNA Features List' panel will again appear. Highlight **CPI Communications side information** and click on **Create**.

31. Fill in the parameters on the 'Create CPI Communications Side Information' panel.

    a. **Symbolic Destination Name** = the OLSID from your BFS.INI file.

    b. Click on **Fully qualified name**. Enter The **Network id** plus the **AVS Gateway name** or the VTAM APPLID for OS/390. (This will be equal to the OLSID for OS/390.)

    c. **TP Name** = the OLSID from your BFS.INI file.

    d. **Security Type** = **PGM**. OS/390 LAN Server doesn't support Security SAME.

    e. **Mode Name** = **BFSLMOD** for OS/390 is recommended for AVS or VTAM logon mode.

    f. **Comment**. Optional.

    g. Click on **Continue**.

32. On the 'Change CPI Communications Program Security' panel, enter:

    a. **User ID** = a valid User ID that has been defined to your host system for VM. For OS/390, this is your FEPNAME.

b. **Password** = a valid password for your user ID above. .

**Note:** If your password expires on the host, you must update it here.

**CM/2** Problem reported to CM/2 Product owners.

If your password expires, you can't just type over the old one. You need to click on **CPI Communications side information** in the features list. Highlight the current definition and change. Highlight **SAME** instead of **PGM** and click **OK**. Exit out of configuration to verify/save. Come all the way back to the SNA features list. Highlight **CPI Communications side information**; highlight **definition** and click on **change**. Select **PGM** instead of **SAME**; click on **Continue**, and retype the valid user ID and new password. Exit out of the menus to reverify.

33. This time when you are returned to the 'SNA Features List', click on **Close**.
34. Also, on the 'Communications Manager Profile List Sheet', click on **Close**.
35. When the 'OS/2 Communications Manager' window appears asking if you would like to invoke the FFST/2* message formatted to view the verify log, click **Yes** to see the verification log.
36. As long as the CONFIG message is APN0534I, it's ok.

    ```
    CONFIG   APN05341: The configuration contains local transaction program
      definitions or a default dir
    ```

37. If you see the following message,

    ```
    link name 'LINK0001', referenced by a dependant LU as a host link,
      specifies that the link does not allow SSCP sessions.
    ```

    make sure you have SOLICIT_SSCP_SESSION(YES), in your .NDF file. If it's set to NO, change it to yes. Add this change to your current CM/2 configuration. Follow the steps below if you are not installing for the first time:

    - Double click on the **Communications Manager** setup icon.
    - Click on **Setup**.
    - Click on **Close** to exit CM/2 setup.

38. Continue reading the message log; then close the message file.
39. When the 'OS/2 Communications Manager' window appears asking if you would like to return to the Communications Manager Configuration to change the settings, click on **NO** if the message file was OK.

## Important Addition to Your SNA Configuration (NDF) File

To edit the NDF file, change directories to \CMLIB. Then follow the steps below:

1. Edit your SNA .NDF file so your SNA configuration knows which alias is the default alias.
2. The following line must be added in the **DEFINE_DEFAULTS** section after the **DEFAULT_MODE_NAME(BLANK)** parameter:

   ```
   DEFAULT_LOCAL_LU_ALIAS(LOCALLUA)
   ```

   **LocalLUA** must be eight characters in length. The value for the **LocalLUA** must match the alias defined for the Local LU Alias earlier. If the value for **LocalLUA** is less than 8 characters, you **must** pad the value with blanks. For example, if the **LocalLUA** is **LOCALLU**, this statement would be entered as:

```
DEFAULT_LOCAL_LU_ALIAS(LOCALLU )   1 blank is added so this field
                                   is 8 characters long.
```

3. After this line is added, **Save** and **Exit this file**.
4. Add this change to your current configuration by following the steps below:
   - Double click on the **Communications Manager** setup icon.
   - Click on **Setup**.
   - Click on **Close** to exit CM/2 setup.

## Summary of Like Information

*Table 15. SNA Setup Information. SNA Parameters and Where They Must Match*

| Example Parameters | Parameter name | Parameter Location |
|---|---|---|
| LFSFEP7 | OLSID | BFS.INI |
| | Symbolic Destination Name | .NDF file |
| | TP name | .NDF file |
| | 2nd Part of Fully Qualified LU Name | .NDF file |
| | 2nd Part of Fully Qualified Name (CPIC side info) | .NDF file |
| | Partner Node Name | .NDF file |
| | APPLID | VTAM APPL def. file |
| | OLSID | LFS CONFIG (LFS Host Server) |
| MCCAMBRI (Valid Host User ID) | fep_name | BFS.INI |
| | User ID - CPIC side info (FepName) | .CFG |
| | FEPNAME (if ALLOWANY is not specified) | LFS CONFIG (LFS Host Server) |
| LOCAL3 | Local LU Alias | .NDF file |
| | Default_Local_LU_Alias | .NDF file |
| HOSTLU | Partner LU Alias | .NDF file |
| USIBMNY (Network ID) | Network ID | .NDF file |
| | 1st Part of Fully Qualified LU Name | .NDF file |
| | 1st Part of Fully Qualified Name (CPIC side info) | .NDF file |
| | Partner Network ID | .NDF file |
| N2NTPD#K (PU) | Local Node Name | .NDF file |
| | Local Node Alias | .NDF file |
| | PU name | VTAM SWNET |
| N2NTPDIK (Independent LU) | LU Name | .NDF file |
| | DLC profiles - C&SM LAN ID | .CFG file |
| | LU name | VTAM SWNET def file |
| 400000000290 (Lan Address) | Lan Destination Address | .NDF file |
| | Lan Destination Address (3270 emulation) | .CFG file |
| BFSLMOD | Mode name | .NDF file |
| | Create Mode name | .NDF file |
| | DLOGMOD | VTAM APPL |
| | DLOGMOD | VTAM SWNET def. file |
| 05D-27056 (Node ID) | Local Node ID | .NDF file |
| VTAM information provided; should be used by your host system administrator. | | |

# Appendix A. How to Run a CM/2 Trace

**CMTRACE** and **FMTTRACE** are the utilities used to run and format a CM/2 trace from the command line.

For SNA, use the following commands:

1. **CMTRACE start /API appc services /DATA ibmtrnet**, starts the trace.
2. **Start BFSSERV**, starts your application.
3. **Close BFSSERV**, stops the application, unless you have only 1 path connected for LFS.
4. **CMTRACE stop /API appc services /DATA ibmtrnet**, stops the trace.
5. **CMTRACE copy TEST.FIL**, Copies the trace information to a file.
6. **FMTTRACE /SDAPRH TEST.FIL**, formats the trace and creates a detailed trace with the extension **.DET** and a summary trace with the extension **.SUM**.

   The detailed trace usually contains the sense data and APPC errors and is easier to look at.

# Appendix B. Sample Files for SNA

## Definitions of .NDF File Parameters:

*Table 16 (Page 1 of 2). .NDF. Definitions of Some Important .NDF Parameters in Communications Manager that LAN Server Uses*

| SNA Configuration verbs | Parameter name | Example parameter | Parameter Definition |
|---|---|---|---|
| DEFINE_LOCAL_CP | FQ_CP_NAME | USIBMNY.N2NTPD#K | Specifies the fully qualified CP for the node. It is made up of the network ID concatenated with a period and the name of the CP (or PU in this case). |
| | CP_ALIAS | N2NTPD#K | Specifies the alias name by which TP name within the node can designate the CP as the Local LU on specific SNA configuration verbs. We usually make it equal to the PU. This parameter is CASE SENSITIVE. |
| | NAU_ADDRESS | INDEPENDENT_LU | Specifies that Network addressable unit (NAU) address is not to be used for terminal sessions. |
| | NODE_TYPE | NN | Specifies that the node provides APPN* network capability. Communications Manager provides many network node capabilities. We use NN, not EN. |
| | NODE_ID | X'05D27056' | For CM/2, you include the 05D; this has to be defined as 05D on VTAM using the IDBLK parameter. The last 5 digits are the Local Node Id you are using. |
| | HOST_FP_SUPPORT | YES | Specifies whether the host provides management services focal point support. We usually specify YES. |
| | HOST_FP_LINK_NAME | LINK0001 | Specifies the name of link that defines the link to the host. This parameter is not mandatory. Communications Manager will use the active SSCP-PU session if it exists. |
| DEFINE_LOGICAL_LINK | LINK_NAME | LINK0001 | 8 character name of the local logical link station. If less than 8 characters are used, you must pad with blanks. |
| | FQ_ADJACENT_CP_NAME | USIBMNY.N2I9AFEP | Specifies the fully qualified name for the CP in the adjacent node. This can be equivalent to your network id concatenated with a period to your VTAM APPLID. |
| | | USIBMNY.N2NT | Same as above, except concatenated with a period to your VTAM domain (?) name. |
| | ADJACENT_NODE_TYPE | LEN | Specifies that the adjacent mode is treated as a low entry networking (LEN) node. You should specify **CP_CP_SESSION_SUPPORT(NO):ehp2 when using this. With a LEN node, CP checking will be bypassed and you can use any CP name value to make the association between the DEFINE_PARTNER_LU_LOCATION and the DEFINE_LOGICAL_LINK verbs.** |
| | DESTINATION_ADDRESS | X'400000000290' | Specifies the destination address to be used by the local node to address the link station on the adjacent node. |
| | ACTIVATE_AT_STARTUP | NO | Specifies that this link will only be activated. |
| DEFINE_LOCAL_LU | LU_NAME | N2NTPDIK | Network name of the Local LU. This is the name of the LU as it is known throughout the network. |
| | LU_ALIAS | LOCALLU | Name used locally for the LU. This name is not sent outside the local node. |
| | NAU_ADDRESS | INDEPENDENT_LU | This is equal to zero and represents a NAU address that is not used. A LU type 6.2 is the only type of SNA LU that supports independent sessions. |
| DEFINE_PARTNER_LU | FQ_PARTNER_LU_NAME | USIBMNY.N2I9AFEP | Fully qualified network name for the partner lU. The name consists of the network id concatenated with the **partner_lu_name**. This is the name of the partner LU as it is known to the network. The partner_lu_name can be equal to the VTAM APPLID. |
| | PARTNER_LU_ALIAS | HOSTLU | The locally know name for the partner LU. This parameter is CASE SENSITIVE. |
| | PARTNER_LU_UNINTERPRETED_NAME | N2I9AFEP | Not needed when using Independent LU's, so LAN Server doesn't use this parameter. |
| | PARALLEL_SESSION_SUPPORT | YES | Specifies the partner LU. Supports more than one concurrent session to a Local LU. MUST have set to yes for LAN Server. |

*Table 16 (Page 2 of 2). .NDF. Definitions of Some Important .NDF Parameters in Communications Manager that LAN Server Uses*

| SNA Configuration verbs | Parameter name | Example parameter | Parameter Definition |
|---|---|---|---|
| DEFINE_PARTNER_LU_LOCATION | FQ_PARTNER_LU_NAME | USIBMNY.N2I9AFEP | Fully qualified network name for the partner LU. The name consists of the network id concatenated with the **partner_lu_name**. This is the name of the partner LU as it is known to the network. The partner_lu_name can be equal to the VTAM APPLID. |
| | FQ_OWNING_CP_NAME | USIBMNY.N2NT | Specifies the fully qualified name of the CP name of the node at which the partner LU is located. This name cannot be the same as the local CP. This name should equal the *fq_adjacent_cp_name* parameter defined under *DEFINE_LOGICAL_LINK*. |
| | LOCAL_NODE_NN_SERVER | YES | Specifies the local node acts as a NN server to the adjacent LEN node. |
| DEFINE_MODE | MODE_NAME | BFSLMOD | The mode name is used to designate the network properties for a group of sessions. This is the name of the mode as it is known throughout the network. This name must be padded if it is less than 8 characters. VTAM mode examples exist in the sample sections. |
| | MAX_RU_SIZE_UPPER_BOUND | 1024 | Specifies the upper bound for the maximum size of RU that can be sent and received on the session. The Max RU size used is negotiated between the local and partner LU's during session activation and will not exceed the value you have defined. |
| | RECEIVE_PACING_WINDOW | 8 | Specifies the session pacing window for sessions. |
| | PLU_MODE_SESSION_LIMIT | 4 | Specifies the maximum limit that a local LU is to use during its CNOS processing as the source LU for the mode name. LFS/ESA uses 4 sessions. |
| | MIN_CONWINNERS_SOURCE | 4 | Specifies the minimum number of contention winner sessions that the local LU is to use during CNOS processing as a source LU for the mode name. In LAN Server, the front-end processor uses all 4 sessions. |
| DEFINE_DEFAULTS | DEFAULT_LOCAL_LU_ALIAS | LOCALLU | Specifies the alias of the Local LU that is to serve as the default LU. The local CP is the default and LFS/ESA wants it equal to the Local LU. |
| DEFINE_CPIC_SIDE_INFO | SYMBOLIC_DESTINATION_NAME | N2I9AFEP | Specifies the symbolic name used by CPI-C applications to identify this definition. This is also equivalent to your VTAM APPLID. |
| | FQ_PARTNER_LU_NAME | USIBMNY.N2I9AFEP | Fully qualified network name for the partner LU. The name consists of the network id concatenated with the **partner_lu_name**. This is the name of the partner LU as it is known to the network. The partner_lu_name can be equal to the VTAM APPLID. |
| | MODE_NAME | BFSLMOD | The mode name designates the network properties for a group of sessions. This must be padded with blanks if less than 8 characters. Generally used for OS/390 LAN Server. |
| | TP_NAME | N2I9AFEP | Specifies the name of the partner TP to be used when a CPI-C application initiates a conversation specifying this side information entry. Equal to the OLSID for LAN Server. Equivalent to the VTAM APPLID. |
| START_ATTACH_MANAGER | N/A | | We don't require this parameter for LAN Server; we initiate the conversations from the PC to the Host. It is **OK**, if a previous application set this to **YES**. |
| CNOS | N/A | | May be used for other applications using SNA. |
| For detailed information on the .NDF parameters, refer to: *CM/2 System Management Programming Reference* or *ES for OS/2 Communications Manager System Programming Reference.* | | | |

# Front-End Processor Sample Files for CM/2.

The following sections provide sample SNACFG.NDF and BFS.INI files.

## Sample SNACFG.NDF File

```
DEFINE_LOCAL_CP  FQ_CP_NAME(USIBMNY.N2NTPD#K )
                 DESCRIPTION(My SNA Configuration)
                 CP_ALIAS(N2NTPD#K)
                 NAU_ADDRESS(INDEPENDENT_LU)
                 NODE_TYPE(NN)
                 NODE_ID(X'05D27056')
                 HOST_FP_SUPPORT(YES);

DEFINE_LOGICAL_LINK  LINK_NAME(LINK0001)
                     DESCRIPTION(VTAM APPC VTAMLST SNA application name)
                     FQ_ADJACENT_CP_NAME(USIBMNY.N2I9AFEP )
                     ADJACENT_NODE_TYPE(LEN)
                     DLC_NAME(IBMTRNET)
                     ADAPTER_NUMBER(0)
                     DESTINATION_ADDRESS(X'400000000290')
                     CP_CP_SESSION_SUPPORT(NO)
                     ACTIVATE_AT_STARTUP(NO)
                     LIMITED_RESOURCE(USE_ADAPTER_DEFINITION)
                     LINK_STATION_ROLE(USE_ADAPTER_DEFINITION)
                     SOLICIT_SSCP_SESSION(YES)
                     EFFECTIVE_CAPACITY(USE_ADAPTER_DEFINITION)
                     COST_PER_CONNECT_TIME(USE_ADAPTER_DEFINITION)
                     COST_PER_BYTE(USE_ADAPTER_DEFINITION)
                     SECURITY(USE_ADAPTER_DEFINITION)
                     PROPAGATION_DELAY(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_1(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_2(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_3(USE_ADAPTER_DEFINITION);

DEFINE_LOCAL_LU  LU_NAME(N2NTPDIK)
                 DESCRIPTION(My Independent LU)
                 LU_ALIAS(LOCALLU )
                 NAU_ADDRESS(INDEPENDENT_LU);

DEFINE_PARTNER_LU  FQ_PARTNER_LU_NAME(USIBMNY.N2I9AFEP )
                   DESCRIPTION(My Partner LU)
                   PARTNER_LU_ALIAS(HOSTLU)
                   PARTNER_LU_UNINTERPRETED_NAME(N2I9AFEP)
                   MAX_MC_LL_SEND_SIZE(32767)
                   CONV_SECURITY_VERIFICATION(NO)
                   PARALLEL_SESSION_SUPPORT(YES);

DEFINE_MODE  MODE_NAME(BFSLMOD )
             COS_NAME(#CONNECT)
             DEFAULT_RU_SIZE(NO)
             MAX_RU_SIZE_UPPER_BOUND(1024)
             RECEIVE_PACING_WINDOW(8)
             MAX_NEGOTIABLE_SESSION_LIMIT(32767)
             PLU_MODE_SESSION_LIMIT(4)
             MIN_CONWINNERS_SOURCE(4);

DEFINE_DEFAULTS  IMPLICIT_INBOUND_PLU_SUPPORT(YES)
                 DEFAULT_MODE_NAME(BLANK)
                 DEFAULT_LOCAL_LU_ALIAS(LOCALLU )
                 MAX_MC_LL_SEND_SIZE(32767)
                 DIRECTORY_FOR_INBOUND_ATTACHES(*)
                 DEFAULT_TP_OPERATION(NONQUEUED_AM_STARTED)
                 DEFAULT_TP_PROGRAM_TYPE(BACKGROUND)
```

```
                        DEFAULT_TP_CONV_SECURITY_RQD(NO)
                        MAX_HELD_ALERTS(10);

    DEFINE_CPIC_SIDE_INFO  SYMBOLIC_DESTINATION_NAME(N2I9AFEP)
                           DESCRIPTION(My CPIC side information for LFS)
                           FQ_PARTNER_LU_NAME(USIBMNY.N2I9AFEP )
                           MODE_NAME(BFSLMOD )
                           TP_NAME(N2I9AFEP);
```

## Sample BFS.INI File

```
;
;  OS/390 LAN Server - BFS.INI file for OS/390
;

BFS_LOG_FILE       = C:\BFS\BFS.LOG
CACHING            = on
FEP_NAME      = MCCAMBRI
OLSID         = N2I9AFEP
CONNECTION    = CM/2
```

# Front-End Processor Sample Files for Extended Services

The following section provides sample TEST.NDF, BFS.INI, ACPI.INI, and ACPI.DIR.

## Sample SNACFG.NDF File

```
    DEFINE_LOCAL_CP  FQ_CP_NAME(USIBMNY.N2NTPC#W )
                     DESCRIPTION(My SNA Configuration)
                     CP_ALIAS(N2NTPC#W)
                     NAU_ADDRESS(INDEPENDENT_LU)
                     NODE_TYPE(NN)
                     NODE_ID(X'27056')
                     HOST_FP_SUPPORT(YES);

    DEFINE_LOGICAL_LINK  LINK_NAME(LINK0001)
                         DESCRIPTION(VTAM APPC VTAMLST SNA application name)
                         FQ_ADJACENT_CP_NAME(USIBMNY.N2I9AFEP )
                         ADJACENT_NODE_TYPE(LEN)
                         DLC_NAME(IBMTRNET)
                         ADAPTER_NUMBER(0)
                         DESTINATION_ADDRESS(X'400000000290')
                         CP_CP_SESSION_SUPPORT(NO)
                         ACTIVATE_AT_STARTUP(NO)
                         LIMITED_RESOURCE(USE_ADAPTER_DEFINITION)
                         LINK_STATION_ROLE(USE_ADAPTER_DEFINITION)
                         SOLICIT_SSCP_SESSION(NO)
                         EFFECTIVE_CAPACITY(USE_ADAPTER_DEFINITION)
                         COST_PER_CONNECT_TIME(USE_ADAPTER_DEFINITION)
                         COST_PER_BYTE(USE_ADAPTER_DEFINITION)
                         SECURITY(USE_ADAPTER_DEFINITION)
                         PROPAGATION_DELAY(USE_ADAPTER_DEFINITION)
                         USER_DEFINED_1(USE_ADAPTER_DEFINITION)
                         USER_DEFINED_2(USE_ADAPTER_DEFINITION)
                         USER_DEFINED_3(USE_ADAPTER_DEFINITION);
```

```
DEFINE_LOCAL_LU  LU_NAME(N2NTPCIW)
                 DESCRIPTION(My Independent LU)
                 LU_ALIAS(LOCALLU )
                 NAU_ADDRESS(INDEPENDENT_LU);

DEFINE_PARTNER_LU  FQ_PARTNER_LU_NAME(USIBMNY.N2I9AFEP )
                   DESCRIPTION(My Partner LU)
                   PARTNER_LU_ALIAS(HOSTLU)
                   PARTNER_LU_UNINTERPRETED_NAME(N2I9AFEP)
                   MAX_MC_LL_SEND_SIZE(32767)
                   CONV_SECURITY_VERIFICATION(NO)
                   PARALLEL_SESSION_SUPPORT(YES);

DEFINE_MODE  MODE_NAME(BFSLMOD )
             COS_NAME(#CONNECT)
             DEFAULT_RU_SIZE(NO)
             MAX_RU_SIZE_UPPER_BOUND(1024)
             RECEIVE_PACING_WINDOW(8)
             MAX_NEGOTIABLE_SESSION_LIMIT(32767)
             PLU_MODE_SESSION_LIMIT(4)
             MIN_CONWINNERS_SOURCE(4);

DEFINE_DEFAULTS  IMPLICIT_INBOUND_PLU_SUPPORT(YES)
                 DEFAULT_MODE_NAME(BLANK)
                 DEFAULT_LOCAL_LU_ALIAS(LOCALLU )
                 MAX_MC_LL_SEND_SIZE(32767)
                 DIRECTORY_FOR_INBOUND_ATTACHES(*)
                 DEFAULT_TP_OPERATION(NONQUEUED_AM_STARTED)
                 DEFAULT_TP_PROGRAM_TYPE(BACKGROUND)
                 DEFAULT_TP_CONV_SECURITY_RQD(NO)
                 MAX_HELD_ALERTS(10);

DEFINE_CPIC_SIDE_INFO  SYMBOLIC_DESTINATION_NAME(N2I9AFEP)
                       DESCRIPTION(My CPIC side information for LFS)
                       FQ_PARTNER_LU_NAME(USIBMNY.N2I9AFEP )
                       MODE_NAME(BFSLMOD )
                       TP_NAME(N2I9AFEP);
```

## Sample BFS.INI File

```
;
;  OS/390 LAN Server - BFS.INI file for OS/390
;

BFS_LOG_FILE       = C:\BFS\BFS.LOG
CACHING            = on
FEP_NAME      = MCCAMBRI
OLSID         = N2I9AFEP
CONNECTION    = PWSCS
```

## Sample ACPI.DIR File

```
; Installation verification destination
INSTVER *USERID.X INSTVER VMINT SAME
;My Host ID, being used for SNA
N2I9AFEP LOCAL3.HOSTLU N2I9AFEP APPC PGM MCCAMBRI MUSKIES
```

---

# OS/390 Sample Files

## Sample VTAM APPC VTAMLST - SNA Application Name

```
File name is SYS1.VTAMLST(BFSAPPLS)

*********************************************************************
BFSAPPL  VBUILD TYPE=APPL
*
N2I9AFEP APPL  ACBNAME=N2I9AFEP,                                      X
               APPC=YES,            ALLOW APPC COMMUNICATION          X
               SECACPT=CONV,        CONVERSATION SECURITY ALLOWED     X
               DSESLIM=4,           SESSION LIMIT                     X
               PARSESS=YES,         ALLOW PARALLEL SESSIONS           X
               MODETAB=BFSTAB,      LOGON MODE TABLE                  X
               DLOGMOD=BFSLMOD      LOGON MODE ENTRY
```

## Sample VTAM Logon Mode Definition File for LU6.2 Applications

If your system already has a VTAM Logon mode definition file, the information after MODETAB and before MODEEND below must be placed in that VTAM Logon mode definition file.

```
File name is BFSTAB.ASSEMBLE

*********************************************************************
BFSTAB   MODETAB
BFSLMOD  MODEENT LOGMODE=BFSLMOD,TYPE=0,FMPROF=X'13',TSPROF=X'07',    X
               PRIPROT=X'B0',SECPROT=X'B0',RUSIZES=X'F8F8',           X
               COMPROT=X'D0B1',ENCR=B'0000',                          X
               PSERVIC=X'060200000000000000000300'
         MODEEND
         END
```

## Sample VTAM Switch Major Node Definition File.

```
File name is SYS1.VTAMLST(SWNET)

*********************************************************************
WLFSPCS  VBUILD TYPE=SWNET,                                          X
               MAXGRP=01,               maximum number of GROUPNM    X
               MAXNO=10                 maximum number of unique DIALs
*
* FEP (PS/2) running OS/2 and Extended Services
N2NTPC#W PU    PUTYPE=2,                PU type 2                    X
               IDBLK=05D,               PU device type               X
               IDNUM=2705C,             PU identification number     X
               MAXPATH=2,                                            X
               DLOGMOD=BFSLMOD,         logon mode table entry       X
               MAXDATA=2012,            maximum data length          X
               ANS=CONT,                                             X
               IRETRY=YES,                                           X
               MAXOUT=7,                                             X
               PASSLIM=5,                                            X
               ISTATUS=ACTIVE
N2NTPCIW LU    LOCADDR=0                Independent LU
```

# Glossary

## A

**abend**. (1) See *Abnormal end of task*. (2) Synonym for *abnormal termination*.

**abnormal end of task (abend)**. Ending of a task before its completion because of an error condition that cannot be resolved by recovery facilities while the task is running.

**abnormal termination**. The ending of processing before planned termination. Synonymous with *abend*.

**ACBNAME**. An application program name specified in the ACBNAME parameter of a VTAM APPL statement. A VTAM APPLID is also sometimes referred to as an application control block name or ACBNAME. See *VTAM APPLID*.

**accounting**. In OS/390, recording information about system users and the resources they require.

**active file**. The most recent backup copy of a file stored within the repository. Such a file is exempt from deletion until an incremental backup detects that the user has either replaced the file with a newer version, or explicitly deleted the file from the workstation (either intentionally or unintentionally).

**address space**. (1) The range of addresses available to a computer program. (2) In OS/390, all virtual storage that a program can address.

**administration processor**. A term that refers to the logical part of the host OS/390 LAN Server server which processes and responds to administration commands.

**administrator**. A user who is registered to enter privileged commands.

**Advanced Interactive Executive (AIX)**. A UNIX-based operating system used on IBM PC/RT and Risc System/6000 computers. A comprehensive, multiuser, multitasking virtual memory operating system that supports a full range of IBM hardware systems. It provides a comprehensive set of UNIX tools, utilities, compilers and application development software; and it includes a wide range of enhancements to UNIX.

**Advanced Program-to-Program Communications (APPC)**. An implementation of the SNA/SDLC LU6.2 protocol that allows interconnected systems to communicate and share the processing of programs. With VTAM, APPC provides this communication within a single system, throughout a collection of systems, and throughout a SNA network.

**AIX**. See *Advanced Interactive Executive*.

**allocate**. To assign a resource, such as a disk or a diskette file, to perform a task.

**American National Standard Code for Information Interchange (ASCII)**. The standard code used for information interchange among data processing systems, data communication systems, and associated equipment. ASCII uses a coded character set consisting of 7-bit coded characters (8 bits including parity check). The ASCII set consists of control characters and graphic characters.

**ANY data set**. A data set that contains subdirectories in both mixed format and folded format.

**APF**. See *authorized program facility*.

**APPC**. See *Advanced Program-to-Program Communications*.

**ASCII**. See *American National Standard Code for Information Interchange (ASCII)*.

**asset**. A collection of data delivered to one or more clients.

**authentication**. Verifying the identity of a user or the user's eligibility to access an object. Authentication checks the user's password to be sure the user is authorized to access the object.

**authorized program facility (APF)**. A facility that permits identification of programs authorized to use restricted functions.

## B

**bandwidth**. The data transfer rate of a device.

**BASE LDS**. A BASE LDS is a linear data set that is formatted to support access controls which are specified for the connect point (i.e. the netname), and which apply to all subdirectories and files below the connect point.

**buffer**. A portion of storage used to hold input or output data temporarily.

**byte**. A unit of storage, consisting of eight adjacent binary digits that are operated on as a unit and constitute the smallest addressable character.

# C

**cache**. (1) A special-purpose buffer, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (2) A buffer that contains frequently accessed instructions and data; it reduces access time.

**caching**. Storing instructions and data in a cache.

**carriage return (CR)**. An ASCII character used with a line feed (LF) character to mark the end of a line for OS/2 and DOS workstations.

**channel**. A path in a system that connects a processor and main storage with an I/O device.

**Channel-To-Channel Adapter (CTCA)**. A hardware device that connects two channels on the same computing system or on different systems.

**CLAW (Common Link Access to Workstations)**. A communications protocol for a direct channel connection between the front-end processor and the OS/390 LAN Server host server using the MMC or ESCON adapter.

**client**. (1) A user. (2) A functional unit that receives shared services from a server. (3) (SAA*) A client function is the requesting half of a function distribution protocol pair. (4) (SAA) Refers to the entity on whose behalf work is done.

**CM/2**. See *Communications Manager/2*.

**code page**. (1) An assignment of graphic characters and control function meanings to all code points; for example, assignment of characters and meanings to 256 code points for an 8-bit code, assignment of characters and meanings to 128 code points for a 7-bit code. (2) A particular assignment of hexadecimal identifiers to graphic characters.

**code point**. A 1-byte code representing one of 256 potential characters.

**commit**. Permanently changing a resource (such as a file).

**Communications Manager/2**. A function of the OS/2 program that lets a workstation connect to a host computer and use the host resources as well as the resources of other personal computers to which the workstation is attached, either directly or through a host system.

**connect**. Establishing a path to communicate with another address space or with the user's own address space.

**connectivity**. The way that computing elements interconnect. The capability of a system or device to be attached to other systems without modification.

**control block**. A storage area used by a computer program to hold control information.

**control file**. A file that is interpreted and directs the flow of a certain process through specific steps. For example, the control file could contain installation steps, default addresses, PTF prerequisite lists, and many other necessary items.

**CTCA**. See *Channel-To-Channel Adapter*.

# D

**DASD**. Direct access storage device; in general, a disk.

**DASD striping**. The use of multiple DASD devices as a single logical volume.

**data set**. A unit of information that can be stored and retrieved. A data set is organized in one of several arrangements. The two types of data sets most often used with TSO/E are a sequential data set and a partitioned data set. See *sequential data set* and *partitioned data set*.

**DBCS**. See *Double-Byte Character Set*.

**device driver**. (1) A file that contains the code needed to attach to and use a device. (2) A collection of subroutines that control the interface between I/O device adapters and a processor.

**diskette**. A diskette is a specific instance of workstation removable media. Other examples might include CD-ROM or optical volumes. Removable media is any volume that can contain a file system that can be removed during regular system operation.

**DOS (Disk Operating System)**. An operating system used in IBM PC, PS/2, and compatible computers.

**dotted decimal notation**. A TCP/IP convention for representing 32-bit internet addresses. Under this convention, the address is written as four decimal integers separated by dots. Each integer represents one byte of the internet address. For example, an internet address of:

```
00000111 10000000 00000101 11111111
```

is represented in dotted decimal notation as:

```
7.128.5.255
```

**Double-Byte Character Set (DBCS)**. A set of characters in which each character is represented by two bytes. Languages such as Japanese, Chinese, and

Korean, which contain more symbols than can be represented by 256 code points, require double-byte character sets. Because each character requires two bytes, the typing, display, and printing of DBCS characters requires hardware and programs that support DBCS. Contrast with *Single-Byte Character Set*.

**drive**. A piece of hardware used to read or write recording media such as disks, tapes, diskettes, and optical media.

# E

**EBCDIC**. See *Extended Binary-Coded Decimal Interchange Code*.

**ES**. See *Extended Services*.

**ESCON**. Enterprise systems connection. A fiber optic channel connection.

**ESCON adapter**. The IBM ESCON adapter card allows attachment of a 3172-3 Interconnect Controller directly to the ESCON channel of an ES/9000 server. The CLAW communications method is used with this adapter.

**Ethernet**. See *IEEE 802.3*.

**export**. To write data from a database or file system to an external file or medium.

**Extended Binary-Coded Decimal Interchange Code**. A coded character set consisting of 8-bit coded characters.

**EXTENDED LDS**. An EXTENDED LDS is a linear data set that is formatted to support access controls that can be specified for each directory, subdirectory, and file.

**Extended Services**. This is an IBM communications product.

# F

**file system**. For NFS clients, the collection of files and file management structures on a physical or logical mass storage device, such as a diskette or minidisk.

**folded directory (FOLD directory)**. On an OS/390 LAN Server workstation format minidisk, a directory that supports only uppercase names. Folded directories are normally used for OS/2 and DOS compatibility.

**Front-End Processor**. A LAN server workstation running OS/390 LAN Server, through which LAN workstation users can access files stored on an OS/390 system.

# G

**gigabyte (GB)**. (1) One billion ($10^9$) bytes. (2) When referring to memory capacity, 1 073 741 824 in decimal notation.

# H

**High Performance File System (HPFS)**. A file system introduced with OS/2 Extended Edition Version 1.2.

# I

**IEEE 802.3**. A standard that describes the carrier sense multiple access with collision detection network. The network's protocol requires carrier sense and a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again. IEEE 802.3 is commonly known as Ethernet.

**import**. To read data from an external source into a database or file system.

**inactive file**. A backup copy that was made obsolete by a more recent copy of the file, or by deletion of the file on the workstation.

**incremental backup**. In OS/390 LAN Server, a function that automatically backs up workstation files that were modified since the time their active copy was stored in the repository, or for which no copy exists in the repository.

**initialization**. Preparation of a system, device, or program for operation.

**Internet Protocol (IP)**. The TCP/IP layer between the higher level host-to-host protocol and the local network protocols. IP uses local area network protocols to carry packets, in the form of datagrams, to the next gateway, router, or destination host.

# J

**job**. A unit of work defined by a user that is to be accomplished by a computer.

**Job Control Language (JCL)**. A control language used to identify a job to an operating system and to describe the job's requirements.

# K

**kanji**. A graphic character set consisting of symbols used in Japanese ideographic alphabets. Each character is represented by two bytes.

**KB**. See *kilobyte*.

**kilobyte (KB)**. 1024 bytes.

# L

**LAN**. See *Local Area Network*.

**LAN Server**. A LAN server provides services to a local area network.

**LDS**. See *Linear Data Set*.

**Linear Data Set (LDS)**. In OS/390, a VSAM data set addressable by byte address, as opposed to cylinder or record location.

**line feed (LF)**. An ASCII character used with a carriage return character to mark the end of a line for OS/2 and DOS workstations.

**link**. A connection, or ability to communicate, between two adjacent nodes in a network.

**local**. Two entities (for example, a user and a server) are said to be local to each other if they belong to the same node within a SNA system. Contrast with *remote*.

**Local Area Network (LAN)**. A collection of workstations connected through a set of interface hardware (such as a Token Ring interface or an Ethernet interface) and software (such as the OS/2 Communications Manager) so that they can send messages and share data.

**logical unit (LU)**. An entity addressable within a SNA-defined network, similar to a node within an OS/390 network. LUs are categorized by the types of communication they support.

**logical unit name (LU name)**. A symbolic name given to a particular LU in a SNA-defined network.

**logon mode table**. A table that contains information used by VTAM to determine the rules to be used by two communications programs. A program may be an application or code that handles a terminal for an end user.

**LU6.2**. This is a special type of logical unit that supports Advanced Program-to-Program Communications (APPC).

# M

**MB**. See *megabyte*.

**megabyte (MB)**. 1 048 576 bytes.

**minimum truncation**. The shortest form of a command name, operand, or option that can be keyed in and still be recognized by OS/390. For example, AC is the minimum truncation for the ACCOUNT command, while the letter A is the minimum truncation for the AUDIT command.

**mixed directory (MIX directory)**. On an OS/390 LAN Server workstation format data set, a directory that supports mixed case names.

**MMC**. The IBM PS/2 Micro Channel to Mainframe Connection (MMC) card, which allows workstations to directly attach to S/370 and S/390 channels.

**module**. (1) A unit of a software product that is discretely and separately identifiable with respect to modifying, compiling, and merging with other units, or with respect to loading and execution. For example, the input to, or output from, a compiler, the assembler, the linkage editor, or an exec routine. (2) A nonrelocatable file whose external references have been resolved.

**mount**. To make a data medium, such as a tape reel, ready to use. This can be done manually or by an automated process.

**multiprogramming**. (1) A mode of operation that provides for interleaved execution of two or more computer programs by a single processor. (2) Pertaining to concurrent execution of two or more computer programs by a computer. (3) The processing of two or more programs at the same time.

**MVSNFS**. An NFS server provided as an optional feature of the IBM program offering TCP/IP Version 2 for MVS.

# N

**network**. Any set of two or more computers, workstations, or printers linked in such a way as to let data be transmitted between them.

**Network File System (NFS)**. A set of files serving RPC protocols defined by Internet RFC 1094. This set of protocols is widely used in TCP/IP operating environments. NFS is a trademark of Sun Microsystems, Inc.

**NFS**. See *Network File System*.

**NFS format data**. Files or directories written to OS/390 LAN Server DASD from an NFS client.

**node**. (1) A single processor or a group of processors in a teleprocessing network. (2) A computer, workstation, or printer, when it is participating in a network.

**nucleus**. The part of OS/390 resident in main storage.

# O

**OS/2 format data**. Data sets or directories written to OS/390 LAN Server DASD from an OS/2 LAN Server requester.

**OS/2 operating system**. An operating system used in IBM PC/AT, PS/2, and compatible computers. OS/2 is one of the client environments supported by OS/390 LAN Server.

# P

**page**. (1) The portion of a panel that is shown on a display surface at one time. (2) To move back and forth among the pages of a multiple-page panel.

**parameter**. A variable that is given a constant value for a specified application and that may denote the application.

**partitioned data set**. A subdivided unit that is divided into separately named, independent partitions called members, each of which can contain data. A partitioned data set has a directory that contains information about each member. See *data set*.

**password**. In computer security, a string of characters known to the computer system and a user, who must specify it to gain full or limited access to a system and to the data stored within it.

**path**. (1) In a network, any route between any two nodes. A path may include more than one branch. (2) In APPC/VM, a connection between two application programs that are on the same or different systems. Paths have names assigned to them.

**problem determination**. The process of identifying the source of a problem; for example, a program component, a machine, telecommunication facilities, user or contractor-installed programs or equipment, an environmental problem such as a power loss, or a user error.

**product**. Any separately installable software program, whether supplied by IBM or otherwise, distinct from others and recognizable by a unique identification code. The product identification code is unique to a given product, but does not identify the release level of that product.

**prompt**. A displayed message that describes required input or gives operational information.

**protocol**. A set of rules for communication that are mutually understood and followed by two communicating stations or processes. The protocol specifies actions that can be taken by a station when it receives a transmission or detects an error condition.

**PTF**. Program temporary fix.

# Q

**queue**. (1) A list constructed and maintained so that the next data element to be retrieved is the one stored first. (2) A line or list of items waiting to be processed; for example, work to be performed or messages to be displayed.

**Note:** This method is characterized as first-in-first-out (FIFO).

# R

**RACF**. See *Resource Access Control Facility*

**read-only access**. An access mode associated with an OS/390 data set that lets a user read, but not write or update, any file on the disk, or SFS directory, or data set.

**remote**. Two entities (for example, a user and a server) are said to be remote to each other if they belong to different nodes within a SNA network. Contrast with *local*.

**Remote Procedure Call (RPC)**. A programming interface that calls subroutines to be processed on a different type of machine. NFS is implemented on RPC architecture.

**requester**. The program that relays a request to another computer. The workstation that runs the requester program may also be referred to as a requester. Contrast with *server*.

**resource**. A program, a data file, a specific set of files, a device, or any other entity or a set of entities that the user can uniquely identify for application program processing.

**Resource Access Control Facility (RACF)**. An IBM product that controls access to resources. These resources can be data, programs, or user defined entities.

**resource ID**. A one-to-eight character name that identifies a resource.

**restore**. A function that allows users to return a copy of a file which was sent to a server storage pool using the backup function to the workstation. The backup copy of the file in the storage pool is not affected.

**route**. A connection to another system by a logical link and one or more intermediate systems. In TSAF, many links and possible intermediate systems that allow the connection of one system to another.

**RPC**. Remote Procedure Call

# S

**SAA architecture**. See *Systems Application Architecture**.

**SBCS**. See *Single-Byte Character Set*.

**SCRIPT/VS**. A component of the IBM Document Composition Facility program product available from IBM for a license fee.

**sequential data set**. A single unit of data arranged in a sequence, from top to bottom, or from beginning to end. See *data set*.

**server**. (1) A functional unit that provides shared services to workstations and workstation group clients over networks; for example, a file server. Contrast with *requester* and *client*. (2) A special kind of application that provides a defined set of services to multiple users or applications. (3) A system in a network that handles the requests of a system at another location, called a client-server. (4) Provides the services of a distributed function protocol pair. (5) (SAA) Refers to the entity that provides services.

**Server Message Block (SMB)**. A set of data structures called Server Message Blocks (SMBs) that are passed over a session established between a requester and a server, and a set of rules governing the sending of these data structures. The four general types of SMBs are session control, file access, print server, and messages.

**service**. Changing a product or adding product updates after installation.

**session**. The SNA term for a connection between two LUs. The LUs involved allocate conversations across sessions.

**sever**. To end communications.

**Single-Byte Character Set (SBCS)**. A set of characters in which each character is represented by a one-byte code. Contrast with *Double-Byte Character Set*.

**SMB**. See *Server Message Block*.

**SMB Processor**. This term refers to the logical part of the host File Services server that interprets, processes, and responds to SMB requests from LAN workstations.

**SMB Protocol**. The set of rules governing the sending of the data structures called Server Message Blocks (SMBs). See *Server Message Block*.

**SMF**. See *system management facilities*.

**SNA**. See *Systems Network Architecture*.

**storage pool**. A collection of virtual storage, all of which has the same characteristics.

**subsystem**. A secondary or subordinate system, usually capable of operating independent of, or asynchronously with, a controlling system.

**Supervisor Call Instruction (SVC)**. An instruction that interrupts a program being run and passes control to the supervisor for a specific service identified by the instruction.

**SVC**. See *Supervisor Call Instruction*.

**syntax**. The rules for the construction of a command or program.

**Systems Application Architecture (SAA)**. A set of software interfaces, conventions, and protocols that provide a framework for designing and developing applications with cross-system consistency.

**system management facilities (SMF)**. An optional control program feature of the OS/390 operating system that provides the means for gathering and recording information that can be used to evaluate system usage.

**stream**. A logical flow of asset data to a single client.

**Systems Network Architecture (SNA)**. The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks.

# T

**token**. OS/390 LAN Server Access Token grants access to a specific protected file to a client with general access privileges that otherwise could not view the file.

**throughput**. (1) A measure of the amount of work

performed by a computer system over a period of time; for example, number of jobs per day. (2) In data communication, the total traffic between stations per unit of time.

**time stamp**. A record containing the time-of-day clock value stored in its internal 32-bit binary format.

**trace**. To record events occurring in a program, usually for debugging purposes.

**Transmissions Control Protocol (TCP)**. The TCP/IP layer that provides reliable process-to-process data stream delivery between nodes in interconnected computer networks. TCP assumes that IP (Internet Protocol) is the underlying protocol.

**Transmissions Control Protocol/Internet Protocol (TCP/IP)**. A set of protocols designed to allow communication between networks regardless of the technologies implemented in each network.

**transparent**. The addition of function or capability that does not change the way the user works with the system. The user is not required to add new software or other facilities to the existing environment in order to use the new function or capability.

# U

**UDP**. See *User Datagram Protocol*.

**UNIX**. A portable operating system developed by Bell Laboratories**. UNIX has been widely accepted as a development and end user computing environment, especially in the education and scientific communities. UNIX is a trademark of UNIX System Laboratories.

**UNIX group identifier (gid)**. A numeric value used to identify a group of users on a UNIX system. This value is assigned by the administrator of the UNIX system.

**UNIX style permissions**. A method used by UNIX systems to control user access to files and directories based on the UNIX user identifier and the UNIX group identifier.

**UNIX user identifier (uid)**. A numeric value used to identify a unique user on a UNIX system. This value is assigned by the administrator of the UNIX system.

**user**. (1) Anyone who requires the services of a computing system. (2) Person, machine, or node.

**User Datagram Protocol (UDP)**. In TCP/IP, a packet-level protocol built directly on the Internet protocol layer. UDP is used for application-to-application programs between TCP/IP host systems.

# V

**Virtual Storage Access Method (VSAM)**. An access method for indexed or sequential processing of fixed and variable-length records on direct access devices. The records in a VSAM data set can be organized in logical sequence by means of a key field (key sequence), in the physical sequence in which they are written on the data set or file (entry-sequence), or by means of relative-record number.

**Virtual Telecommunications Access Method (VTAM)**. An IBM software product that controls communication and the flow of data in a computer network. It provides single-domain, multiple-domain, and multiple-network capability. Virtual Telecommunications Access Method runs under OS/390 and other operating systems.

**volume**. The portion of a single unit of storage mounted and demounted as a unit (for example, a tape reel), or accessible to a single read/write mechanism. In OS/390 LAN Server, a volume can be a physical volume, volume partition, file system, or a VSAM data set, depending upon the host operating system and the use of the volume.

**VSAM**. See *Virtual Storage Access Method*.

**VTAM**. See *Virtual Telecommunications Access Method*

**VTAM APPLID**. A name for a list of parameters that describes to VTAM the rules an application will use to govern communications with other applications. A VTAM APPLID is also sometimes referred to as an application control block name or ACBNAME.

# W

**wildcard**. A pattern-matching character.

**window**. A portion of a computer screen, usually framed, used by a single program to present information or interact with the user.

**workstation**. Generally, a workstation is a computer with its own processing hardware, designed for use by an individual (or sometimes a small group).

**workstation format data set**. A data set that supports workstation data in its native format, including hierarchical directories, long names, hard and symbolic links, extended attributes, and so forth.

# 3

**3088**. Refers to the IBM 3088 Multisystem Communications Unit, Models 1 and 2.

**3380**. Refers to the IBM 3380 Direct Access Storage Device.

# 9

**9370**. Refers to a series of small IBM System/370 processors.

# Index

## Numerics



## A



## B



## C



## D

## E



## F



## G



## H



## I



## J



## K



## L



## M

# N



# O



# P



# Q



# R



# S

## T



## U



## V



## W

# Communicating Your Comments to IBM

OS/390
LAN Server
Installation Guide

Publication No. GC28-1733-03

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

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

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

If you are mailing an RCF from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:
  - FAX: (International Access Code)+1+914+432-9405
- If you prefer to send comments electronically, use this network ID:
  - IBMLink: (United States customers only): KGNVMC(MHVRCFS)
  - IBM Mail Exchange: USIB6TC9 at IBMMAIL
  - Internet e-mail: mhvrcfs@vnet.ibm.com
  - World Wide Web: http://www.s390.ibm.com/os390

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

Optionally, if you include your telephone number, we will be able to respond to your comments by phone.

# Reader's Comments — We'd Like to Hear from You

**OS/390**
**LAN Server**
**Installation Guide**

**Publication No. GC28-1733-03**

You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

**Note:** Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.

Today's date: _____

What is your occupation?

Newsletter number of latest Technical Newsletter (if any) concerning this publication:

How did you use this publication?

| | | | |
|---|---|---|---|
| [ ] | As an introduction | [ ] | As a text (student) |
| [ ] | As a reference manual | [ ] | As a text (instructor) |
| [ ] | For another purpose (explain) | | |

Is there anything you especially like or dislike about the organization, presentation, or writing in this manual? Helpful comments include general usefulness of the book; possible additions, deletions, and clarifications; specific errors and omissions.

Page Number: Comment:

Name

Address

Company or Organization

Phone No.

**Reader's Comments — We'd Like to Hear from You**
GC28-1733-03

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

# BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie NY 12601-5400

Fold and Tape | **Please do not staple** | Fold and Tape



Cut or Fold
Along Line

File Number: S370/S390-34
Program Number: 5647-A01

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC28-1733-03