
This edition applies to

NetView File Transfer Program Server for AIX (5765-435)
NetView File Transfer Program Client for AIX (5622-242)

and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

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

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

IBM Deutschland Entwicklung GmbH
Information Development, Dept. 0446
Postfach 1380
71003 Boeblingen
Germany

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

© Copyright International Business Machines Corporation 1994. All rights reserved.
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.
Contents

Notices .......................................................... v
Trademark and Service Marks ................................. v

About This Book .............................................. vii
Abbreviations and Special Terms ............................ vii
Who Should Read This Book ................................. vii
How to Use This Book ........................................ viii
How to Read Syntax Diagrams ............................... viii

Chapter 1. Introducing NetView FTP for OS/2, DOS, and Windows Workstations ................................ 1

Chapter 2. Installing and Configuring NetView FTP AIX ........................................................ 7
Planning for NetView FTP AIX ................................ 8
Installing NetView FTP AIX .................................... 9
Installing and Using the Online Documentation ............ 10
Customizing NetView FTP AIX ................................ 11
    Creating a NetView FTP System User ID ................. 11
    Creating the NetView FTP System Environment ........... 11
    Adapting the NetView FTP Initialization and Request Definition Files ................................ 12
    Creating NetView FTP User Environments ................ 13
Summary of the NetView FTP Environment Variables and Files ........................................ 14
    NetView FTP Environment Variables ....................... 14
    NetView FTP System Files .................................. 15
Configuring NetView FTP Server AIX for Remote Communication ........................................ 16
    AIX Communication Device Configuration ................. 17
    Configure SNA Services/6000 .......................... 17
    Verifying Your SNA Services/6000 Configuration ........ 24
    Configure SNA Server/6000 ............................ 25
    Configure the Communication Paths ..................... 26

Chapter 3. Verifying Your Local Installation .................. 27
Starting the NetView FTP System Daemon ................. 27
Starting the NetView FTP Server Component ............... 28
Starting the NetView FTP Responder Component ........... 30
Starting a NetView FTP Client Environment .............. 33

Chapter 4. Tailoring the Initialization Parameters ......... 35
Overview of the Initialization Parameters .................. 36
Communication Protocol ..................................... 37
Create Directory ............................................. 37
Default Directory for Incoming Files ...................... 37
Default Directory for Outgoing Files ...................... 38
IP Server Workstation ID ................................... 38
Logical Unit Name .......................................... 39
Maximum Number of Clients ................................ 39
Maximum Number of Transfers ................................ 39
Network Identification ....................................... 40
Operation Mode .............................................. 40
Retry Attempts .............................................. 40
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNA Token Ring Link Station Profile — Caller</td>
<td>115</td>
</tr>
<tr>
<td>SNA LU6.2 Partner LU Profiles</td>
<td>115</td>
</tr>
<tr>
<td>SNA LU6.2 Partner LU Location Profile</td>
<td>116</td>
</tr>
<tr>
<td>SNA Services/6000</td>
<td>116</td>
</tr>
<tr>
<td>SNA Node Profile</td>
<td>116</td>
</tr>
<tr>
<td>SNA Control Point Profile</td>
<td>116</td>
</tr>
<tr>
<td>SNA Token Ring Logical Link Profile</td>
<td>116</td>
</tr>
<tr>
<td>SNA Token Ring Physical Link Profile</td>
<td>117</td>
</tr>
<tr>
<td>SNA Token Ring Attachment Profile — Listener</td>
<td>117</td>
</tr>
<tr>
<td>SNA Token Ring Attachment Profile — Caller</td>
<td>117</td>
</tr>
<tr>
<td>SNA LU6.2 Local LU Profile — Listener</td>
<td>118</td>
</tr>
<tr>
<td>SNA LU6.2 Local LU Profile — Caller</td>
<td>118</td>
</tr>
<tr>
<td>SNA LU6.2 Logical Connection Profile — Listener</td>
<td>118</td>
</tr>
<tr>
<td>SNA LU6.2 Logical Connection Profile — Caller</td>
<td>118</td>
</tr>
<tr>
<td>SNA LU6.2 Mode Profile — FTPBIND</td>
<td>119</td>
</tr>
<tr>
<td>SNA LU6.2 Mode List Profile</td>
<td>119</td>
</tr>
<tr>
<td>SNA LU6.2 TPN Profile</td>
<td>119</td>
</tr>
<tr>
<td>SNA LU6.2 TPN List Profile</td>
<td>120</td>
</tr>
<tr>
<td>SNA LU6.2 RTPN Profile</td>
<td>120</td>
</tr>
<tr>
<td>Server Group Table (srvgrp.tab) Entries</td>
<td>120</td>
</tr>
<tr>
<td>Monitoring Your SNA Activities</td>
<td>120</td>
</tr>
<tr>
<td><strong>Appendix E. Summary of Installed Files</strong></td>
<td>121</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td>123</td>
</tr>
<tr>
<td><strong>Bibliography</strong></td>
<td>137</td>
</tr>
<tr>
<td>The NetView FTP Library</td>
<td>137</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>139</td>
</tr>
</tbody>
</table>
Notices

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

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

Trademarks and Service Marks

The following terms, which are denoted by an asterisk (*) at their first occurrence in this publication, are trademarks or service marks of the IBM Corporation in the United States or other countries or both:

AIX AIX/6000 APPN
IBM MVS/ESA MVS/XA
NetView POWERserver POWERstation
RISC System/6000 SAA VTAM

The following term, denoted by a double asterisk (**) in this publication, is a trademark of another company:

Motif Open Software Foundation, Inc.
About This Book

This book describes the IBM* licensed programs NetView* File Transfer Program Server for AIX* and NetView File Transfer Program Client for AIX. This book describes how to install and use these NetView File Transfer Program products.

Abbreviations and Special Terms

Throughout this book, the following abbreviations are used:

NetView FTP NetView File Transfer Program (regardless of version number and operating system)

NetView FTP V2.2 MVS NetView File Transfer Program Version 2 Release 2 Modification Level 1 for MVS

NetView FTP Server AIX NetView File Transfer Program Server for AIX

NetView FTP Client AIX NetView File Transfer Program Client for AIX

NetView FTP AIX NetView File Transfer Program Server AIX and NetView File Transfer Program Client AIX

NetView FTP Client A NetView FTP Client AIX or the built-in client of a NetView FTP Server AIX program

NetView FTP host A system running NetView FTP V2.2 MVS

NetView FTP node A computer system running NetView FTP

NetView/6000 IBM AIX NetView/6000

AIX The AIX/6000* operating system

MVS The MVS/370, MVS/XA*, and MVS/ESA* operating systems.

Who Should Read This Book

This book is written for people who plan to use NetView FTP AIX to transfer files from a programmable workstation to other computer systems. This book assumes that you know how to create and work with the files you are about to transfer. You should also be familiar with the AIX/6000 operating system.

For the customization of NetView FTP AIX, you must have a good knowledge of AIX system administration. For the configuration of NetView FTP AIX, you must have a working knowledge of technical terms associated with Systems Network Architecture (SNA) environments.
How to Use This Book

To get to know NetView FTP AIX before installing or using it, read Chapter 1 first.

If you are already familiar with the NetView family of products and are about to install NetView FTP AIX, read Chapter 2.

If NetView FTP AIX is already installed, read Chapter 5 to get started.

You should also refer to the *NetView FTP Parameter Reference* for a description of the parameters mentioned in this book.

How to Read Syntax Diagrams

The syntax diagrams used in this manual are what is often called “railroad track syntax diagrams.” To use a diagram, follow a path from left to right, top to bottom, adding elements as you go. In these diagrams, all spaces and other characters are significant.

Each diagram begins with a double right arrowhead and ends with a right and left arrowhead pair. Lines beginning with single right arrowheads are continuation lines.

```
    ➤keyword=variable_value➤
```

Keywords are all in lowercase, but can be entered in uppercase or in lowercase. Variable values that you provide are shown in *italics* and are usually in lowercase. Where values are shown in uppercase, they should be entered as they appear.

In a choice of items, the default item is always shown above the main line:

```
    ➤keyword=default_value➤

    ➤keyword=other_value➤
```

Optional syntax elements are shown below the main line:

```
    ➤keyword=value➤
```
The following is a sample syntax diagram. It shows the expressions that you can form with the hello command.

Valid versions of the hello command are:

- hello
- hello name
- hello, how are you?
- hello name, how are you?

Note that the space before the name of person value is significant and that, if you do not code name at all, you still code the comma before how are you.

The key to using the syntax diagrams is to follow them mechanically.
Chapter 1. Introducing NetView FTP for OS/2, DOS, and Windows Workstations

NetView FTP Server AIX and NetView FTP Client AIX are members of the NetView FTP family of products. These products are also referred to as NetView FTP AIX when the information applies to both products.

NetView FTP AIX let users of programmable workstations transfer files quickly and reliably from or to other NetView FTP systems within local area networks (LANs) or wide area networks (WANs).

NetView FTP AIX:
- Provide high-speed file transfer
- Transfer files from one storage device to another without intermediate spooling
- Provide automatic restart of interrupted file transfers
- Offer a graphical user interface and a command-line interface.

NetView FTP AIX provide file-transfer functions at the workstation where they are installed. The NetView FTP Server for OS/2 has a "built-in" Client functionally equivalent to the NetView FTP Client for OS/2. Due to this built-in client, a NetView FTP Server for OS/2 can also be used as a stand-alone product for file transfers.

The NetView FTP Server for OS/2 product also serves as a gateway between NetView FTP Clients and other NetView FTP nodes in an SNA network. See Figure 1 on page 2.

In a LAN network with one or more NetView FTP clients there must be at least one workstation running a NetView FTP Server for OS/2. NetView FTP Server AIX communicates with NetView FTP Client AIX via Transmission Control Protocol/Internet Protocol (TCP/IP) protocols.

NetView FTP AIX consists of several components:

**System daemon**
- Provides common workstation-wide services that are required by the other components. The system daemon must be active before any other NetView FTP component can be started.

**Server component**
- Provides gateway and routing services for all attached NetView FTP clients through the SNA Services/6000 or the SNA Server/6000 product. The server component runs as a daemon process.

**Requester component**
- Provides services that enable users to request file transfer. This component contains the command-line and the graphical user interfaces through which users can set up file-transfer requests. The requester component is activated by each user individually.

**Responder component**
- Provides common responder services for your workstation. This component must be active to enable response to remotely initiated file transfers. The responder component also runs as a daemon process.
The server component is part of NetView FTP Server AIX only while all the system
daemon, the responder component, and the requester component are part of both
NetView FTP Server AIX and NetView FTP Client.
Figure 1 provides an overview of the NetView FTP products in the context of this
manual.

![Figure 1. Network with NetView FTP](image)

A file transfer can be initiated at any NetView FTP Client workstation, at a NetView
FTP Server workstation, or at a node with NetView FTP V2.2 MVS. The NetView
FTP system that initiates the file transfer is the requesting transfer node, while the
transfer partner is the responding transfer node.

In each file transfer, there is a sending file from which the data is read and a
receiving file to which the data is written. You use NetView FTP AIX by setting up
file-transfer requests. A request tells NetView FTP such things as:

- Whether to transfer a file to or from another system
- Which system to transfer the file to or from
- Which file is to be transferred from the sending system
- Where to store the file at the receiving system.

With NetView FTP AIX all file-transfer requests are combined from two sources:

- The input you enter using the command-line interface or the graphical user
  interface
- The request definition file (RDF).

In the user interfaces, you can assign values to required file-transfer parameters, or
you can specify override values for parameters included in the RDF.

The RDF is a text file that contains values for file-transfer parameters, usually those
that do not change very often. An RDF is not deleted after a file-transfer request
was created from it and can be reused. You can refer to an existing RDF by its
name when you submit a file-transfer request.
For more information about the parameters that can be included in the RDF and those that can be entered via the interfaces, refer to “Working with Request Definition Files” on page 69.

When you are using NetView FTP AIX, you can send files to or retrieve files from:

- A NetView FTP Client in an internet protocol (IP) network, either the same or another
- The built-in client of a NetView FTP Server
- A NetView FTP V2.2 MVS node.

Within the same network, NetView FTP transfers the file via the NetView FTP Server program (see 1 in Figure 2). In this case, however, NetView FTP Server AIX must be configured for SNA even if the TCP/IP protocol is used for the communication between NetView FTP Server AIX and NetView FTP Client AIX (refer to “Configuring NetView FTP Server AIX for Remote Communication” on page 16 for more information). In general you need at least two NetView FTP Server nodes to perform file transfers between the requesting and the responding transfer program.

Between two different networks, NetView FTP transfers the file via the NetView FTP Server program in the requester’s network and the NetView FTP Server program in the responder’s network (see 2 in Figure 2).

In transfers to and from NetView FTP V2.2 MVS, the server component of the NetView FTP Server AIX in the requester’s network communicates with the NetView FTP V2.2 MVS server (see 3 in Figure 2) in the responder’s network.
For file transfers between workstations, a responder component must have been started at the remote NetView FTP workstation. To address this responder component, you must specify in your request:

- The destination ID, which is the name of the connection profile that is defined for this connection in the SNA setup (keyword RMTNODE).
- The workstation ID, which is the IP address or the IP host name of the workstation running the responder component (keyword RMTWSTID).

For example, a file transfer from a NetView FTP Client in network A to a NetView FTP Client in network B as shown with 2 in Figure 2 works as follows:

- The NetView FTP Client program in network A is the requesting program, the NetView FTP Client program in network B is the responding program.
- The responder component of the NetView FTP Client in network B must be started.
- The file-transfer request submitted at the NetView FTP Client in network A must contain:
  - The destination ID of the NetView FTP Server AIX workstation in network B. The destination ID, which is the name of the connection profile that is defined for this connection in the SNA setup.
  - The workstation ID of the NetView FTP Client AIX workstation in network B.
• When the file transfer is performed, NetView FTP Server AIX passes the request to the NetView FTP Client that is identified with the workstation ID.

From theory to practice

After the installation and configuration of NetView FTP, have a look at the file-transfer examples in Chapter 5, “Getting Started” on page 45. This chapter also contains some hints and tips for the use of the file-transfer parameters.
Chapter 2. Installing and Configuring NetView FTP AIX

This chapter describes the installation and configuration of NetView FTP AIX.

This chapter covers:

- Planning for NetView FTP AIX
- Installing NetView FTP AIX
- Installing and using the online documentation
- Customizing NetView FTP AIX
- Configuring NetView FTP Server AIX for remote communication.

It also gives a summary of the NetView FTP environment variables and files.

The tasks described in the following sections must be performed with root authority. The customization of NetView FTP AIX requires a good knowledge of AIX system administration. For the configuration of NetView FTP AIX, you must have a working knowledge of technical terms associated with SNA.

**Note:** You do not need to install both NetView FTP Server AIX and NetView FTP Client AIX on one workstation. In addition to the SNA gateway services, NetView FTP Server AIX offers the same functions as NetView FTP Client AIX.

The following hardware and software are prerequisites for NetView FTP AIX:

- Any RISC System/6000* POWERstation* or POWERserver*
- An 8 mm tape drive, a 1/4 inch tape drive, or a 3.5 inch diskette drive for local installation
- A communication adapter supported by:
  - IBM AIX SNA Services/6000 or IBM AIX SNA Server/6000
  - TCP/IP.
- IBM AIX for RISC System/6000 Version 3.2.5 (5756-030).

If the graphical user interface is to be used:

- A graphical display unit
- IBM AIXwindows Environment/6000 Version 1.2.4, X11R5 (5601-257).

NetView FTP Server AIX also requires one of the following:

- IBM AIX SNA Services/6000 Version 1.2 (5601-287)
Planning for NetView FTP AIX

Before installing NetView FTP for AIX, you must plan how NetView FTP is to be installed on the workstations in your local environment.

If you plan to transfer files only from one AIX workstation, that is, you do not have multiple workstations in your local network connected together, you must install NetView FTP Server AIX on that workstation. In this case, continue with “Installing NetView FTP AIX” on page 9.

If you have multiple workstations that serve as transferring nodes, you must decide on which workstation you want to install NetView FTP Server AIX and on which NetView FTP Client AIX. You need at least one NetView FTP Server AIX installation in your local network, otherwise the clients cannot be started.

Furthermore, you must determine how many parallel file transfers, that is, file transfers that run at the same time on one processing unit, a NetView FTP Server AIX must handle. Too many parallel file transfers on one NetView FTP Server AIX reduce the performance. Therefore, consider installing more than one server in your network.

Also take into account that not the number of connected workstations determines the transfer performance but the number of users that are transferring files at the same time.

**Note:** You can also transfer a file within the same IP network:
- Between two NetView FTP Client AIX programs via one workstation running NetView FTP Server AIX
- Between a NetView FTP Client AIX and a NetView FTP Server AIX.

Then, however, you must have access to the SNA network by using either the SNA Services/6000 product or the SNA Server/6000 product. Additionally, you must configure a U-shaped connection between two Token Ring adapters, so that NetView FTP Server AIX can establish two physical unit (PU) and two LU connections.

Before installing NetView FTP AIX, check that TCP/IP is configured correctly on your workstations. NetView FTP Server AIX and NetView FTP Client AIX communicate via TCP/IP sockets, which they cannot work when TCP/IP is not working properly.

To check your local configuration perform the following tasks:

1. Log on to the workstations that serve as clients and use the **ping** command to send echo requests (**ping**) to the server nodes with both the host name and the IP address. The clients must receive a response from the servers.

2. Log on to the server workstations and ping the client nodes with both the host name and the IP address.

All pings must receive a proper response. If you receive an error message, for example, **ping: unknown host abcd**, contact your TCP/IP administrator. In this case, you cannot work with NetView FTP because client and server cannot communicate.

If the pings were successful, continue with “Installing NetView FTP AIX” on page 9.
Installing NetView FTP AIX

This chapter explains how to install NetView FTP AIX on your workstation. NetView FTP Server AIX and NetView FTP Client AIX are shipped as software packages for use with the `installp` command. Both the client and the server package contain several product options that you can install. For example, if you only want to use the command-line interface of NetView FTP AIX, you need not install the graphical user interface. To determine which package and install options are on your distribution tape, do the following:

1. Log in as `root`.
2. Type `smit install` at the command prompt to get to the SMIT Software Installation Menu.
3. Choose `Install / Update Software`.
5. Enter the correct input device. If you are not sure about the input device, list the available devices and select the appropriate device.
6. If the installation media contains the server package, information similar to the following is displayed:

```
#-------------------------------------------------------
# Software packages                                      
#-------------------------------------------------------
1.1.0.0 NFTP                                             
  1.1.0.0 NetView FTP Server for AIX Base               
  1.1.0.0 NetView FTP Server User Interface             
  1.1.0.0 NetView FTP Smit Server Help Messages En_US   
  1.1.0.0 NetView FTP Server NetView/6000 Integration Files

1.1.0.0 ipfx.Runtime                                     
  1.1.0.0 IBM Presentation Facility/6000               
```

If the installation media contains the client package, information similar to the following is displayed:

```
#-------------------------------------------------------
# Software packages                                      
#-------------------------------------------------------
1.1.0.0 NFTP                                             
  1.1.0.0 NetView FTP Client for AIX Base               
  1.1.0.0 NetView FTP Client User Interface             
  1.1.0.0 NetView FTP Smit Client Help Messages En_US   
  1.1.0.0 NetView FTP Client NetView/6000 Integration Files

1.1.0.0 ipfx.Runtime                                     
  1.1.0.0 IBM Presentation Facility/6000               
```

The `ipfx.Runtime` package enables you to view the online documentation for NetView FTP. See “Installing and Using the Online Documentation” on page 10 for more information on this package.

7. Decide which options you want to install on which workstation. Note that you need not install the complete packages. You can install the base products first and the product options any time later.
The following section provides instructions on how to perform the installation:

1. After having listed the software on the installation media, select **Install / Update Selectable Software (Custom Install)** from the Install / Update Software menu.

2. Select **Install Software Products at Latest Available Level**.

3. Enter the input device. If you are not sure about the input device, list the available devices and select the appropriate device.

4. From the list of software to be installed, select the options you want to install. If you want to install the complete product package, select the ALL option.

After you have installed NetView FTP AIX successfully, you must customize the environment.

---

**Installing and Using the Online Documentation**

Check if the **ipfx** package is already installed on your system. You can do this using the `lslpp -l ipfx.Runtime` command.

The package is already installed when the following is displayed:

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path:/usr/lib/objrepos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipfx.Runtime</td>
<td>COMMITTED</td>
<td>IBM Presentation Facility/6000</td>
</tr>
</tbody>
</table>

Otherwise install the package as follows:

1. Log in as **root**.

2. Type `smit install`.

3. Select **Install / Update Software**.

4. Select **Install / Update Selectable Software (Custom Install)**.

5. Select **Install Software Products at Latest Available Level**.

6. Select the corresponding input device.

7. From the list of software to be installed select the **ipfx** package.

During the installation, the BOOKSHELF environment variable is set in `/etc/profile`. You must log out and log in again to activate this variable.

If the **ipfx** package was already installed on your system, you must set the BOOKSHELF variable in your `/etc/profile`:

```
export BOOKSHELF=/usr/lpp/nftp/etc:$BOOKSHELF
```

To use the online documentation, your Motif** Window Manager must be started.

Customizing NetView FTP AIX

To customize NetView FTP AIX you must:

- Create a NetView FTP system user ID
- Create the NetView FTP system environment
- Adapt the NetView FTP initialization and request-definition files
- Create NetView FTP user environments.

Creating a NetView FTP System User ID

1. Type `smit mkuser` and add a user with the name `nftp`. NetView FTP uses the home directory of this user as root entry for its own directories.

   You can use a different name. In that case, replace the name `nftp` in the following descriptions by the name you have used.

2. Make sure that the file system where the `nftp` user resides is large enough to handle NetView FTP requests. NetView FTP requires at least 64MB\(^1\) of free space in this file system. If there is not enough space, create a separate logical volume on which the `nftp` file system is mounted.

Creating the NetView FTP System Environment

To create the NetView FTP system environment do the following:

1. Type `smit nftp` at the command prompt to get to the SMIT menus for NetView FTP.

2. Select **Root Services**.

3. Select **Create NetView FTP system environment**.

4. A data entry panel is displayed. Specify the home directory of the NetView FTP system user. The default value is `/home/nftp`. NetView FTP creates several subdirectories in the NetView FTP home directory. These are:

   - `nftpwork` The directory containing common initialization and RDF files for all users on your AIX workstation.
   - `system` The directory containing the NetView FTP system files for the responder component and the system daemon.
   - `server` The directory containing the NetView FTP system files for the server component.
   
   In each of these directories the subdirectories `/basket`, `/data`, `/ini`, `/log`, and `/rdf` are created.

5. If you want the environment variable `NFTPSYSTEMDIR` to be included in the `/etc/profile` file, set this field to yes. During runtime NetView FTP uses the information in this variable to determine where the NetView FTP system user resides.

---

\(^1\) 1MB equals 1,048,576 bytes.
6. Before any NetView FTP system activities can take place, the NetView FTP system daemon must be running. Daemon processes are usually started during system startup. If you do not want to start the NetView FTP system daemon during startup, set this field to no. In this case you can start the NetView FTP system daemon manually at any time after system startup as described in Chapter 6, “Using NetView FTP for OS/2, DOS, and Windows Workstations” on page 61. If you select yes, the corresponding call statement is included in the file /etc/rc.tcpip.

7. The value in the last field determines whether the responder component is started during system startup. If you select yes, ensure that the NetView FTP system daemon and the NetView FTP server component are active before the responder component is started.

Adapting the NetView FTP Initialization and Request Definition Files

1. If you have installed NetView FTP Server AIX, you must customize the initialization file of the NetView FTP Server. If you have installed NetView FTP Client AIX, go to step 2.

There are two ways to customize the initialization file of the server:

a. Using SMIT:

1) Within the Root Services of the SMIT menu for NetView FTP select Start / Stop the NetView FTP Server.

2) Select Prepare NetView FTP Server initialization file.

3) Specify ibmnftp.ini and edit the server’s default initialization file. Note that you can use any other filename, but you must specify this filename during server startup.

b. Editing the initialization file directly:

1) Change to the directory /home/nftp/server/ini.

2) Edit the file ibmnftp.ini. This is the default initialization file for the NetView FTP Server.

Set the initialization parameters according to your system requirements. The NetView FTP initialization parameters are described in Chapter 4, “Tailoring the Initialization Parameters” on page 35.

2. To enable users on other NetView FTP nodes to send files to or to receive files from your workstation, the NetView FTP responder component must be active on your workstation. The NetView FTP responder component is running as a daemon process and accepts file-transfer requests on behalf of an AIX user on that workstation.

Note: If a NetView FTP responder component is started on a workstation, this workstation can be accessed from remote nodes. You can prevent this by not starting a NetView FTP responder component. Users on the workstation can still send or receive files, but users on other nodes have no access to this machine.
If you want to work with a NetView FTP responder component, you must customize the initialization file of the responder component. There are two ways to do that:

a. Using SMIT:

1) Within the **Root Services** of the SMIT menu for NetView FTP select **Start / Stop the NetView FTP Responder Component**.

2) Select **Prepare NetView FTP Responder Component initialization file**.

3) Specify `ibmnftp.ini` and edit the responder component’s default initialization file. Note that you can use any other filename, but you must specify this filename during the startup of the responder component.

b. Editing the initialization file directly:

1) Change to the directory `/home/nftp/system/ini`.

2) Edit the file `ibmnftp.ini`. This is the default initialization file for the NetView FTP responder component.

Set the initialization parameters according to your system requirements. The NetView FTP initialization parameters are described in Chapter 4, “Tailoring the Initialization Parameters” on page 35.

3. You can supply NetView FTP initialization files that can be used system-wide. If you want to do that, change to the directory `/home/nftp/nftpwork/ini` and create these files. All users who do not have a file with the same name in their private environments can work with these system-wide initialization files.

The file `ibmnftp.ini` is supplied as a sample. You can tailor this file according to your system requirements.

4. Additionally, you can provide predefined NetView FTP RDF files for your AIX users. If you want to do this, change to the directory `/home/nftp/nftpwork/rdf` and create the RDF files you want. A default RDF file with the name `default` is provided with the product. For a description of RDF parameters refer to the NetView FTP Parameter Reference.

**Note:** After the installation and customization you must restart the workstation, so that system-environment variables are known to the system. After the restart, create the NetView FTP user environments.

### Creating NetView FTP User Environments

After the NetView FTP system has been set up, users can set up their private NetView FTP environments. For this task, it is not necessary to have root authorization.

To create your own NetView FTP environment, do the following:

1. Log in with the user ID for which you want to create the NetView FTP Client environment.

2. Type `smit nftp` at the command prompt.

3. Select **User Services**.

4. Select **Create your NetView FTP environment**.
5. A data entry panel is displayed. Specify the directory where your NetView FTP subdirectories are to be placed. For example, if you work as user fred and you specify /home/fred/nftpwork, NetView FTP creates a directory /home/fred/nftpwork (if it does not already exist) plus the subdirectories basket, data, ini, log, and rdf.

NetView FTP also creates the files $HOME/nftpwork/ini/ibmnftp.ini and $HOME/nftpwork/rdf/default. Change them according to your needs.

6. When you create your own environment, you must tell NetView FTP where to find the corresponding directories and files. You do this by setting the environment variable NFTPWORKDIR. Here you can select whether this variable should be added to your .profile file.

You can also have multiple users share one client environment. To do that, you must ensure that the users who share the environment have write access to the directories pointed to by the variable NFTPWORKDIR.

For example:

1. Create a user nv_ftp_u.
2. Create a group nv_ftp_g.
3. The users fred and iris belong to group nv_ftp_g. The entry for group nv_ftp_g in the file /etc/group must be similar to the following:
   nv_ftp_g::!/200:nv_ftp_u,iris,fred
4. Log in as nv_ftp_u.
5. Set the file mask in a way that all members of group nv_ftp_g, that is, iris and fred, have write access to the files owned by nv_ftp_u.
6. Create the NetView FTP client environment as described at the beginning of this section.
7. If the client environment is created below /home/nv_ftp_u/nftpwork, iris and fred must specify the variable NFTPWORKDIR in their .profile file:
   export NFTPWORKDIR=/home/nv_ftp_u/nftpwork

   When user nv_ftp_u starts the client environment, iris and fred can use that environment, but they are not allowed to stop the environment. Only the owner (the user who starts the system) can stop the environment.

### Summary of the NetView FTP Environment Variables and Files

This section gives an overview of the NetView FTP files and environment variables. If you do not want to use SMIT to customize your environment, you can use this overview as reference when customizing your workstation on your own.

#### NetView FTP Environment Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Purpose</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFTPSYSTEMDIR</td>
<td>Points to the home directory of the NetView FTP system user</td>
<td>/home/nftp</td>
</tr>
<tr>
<td>NFTPWORKDIR</td>
<td>Points to a NetView FTP Client environment directory</td>
<td>$HOME/nftpwork</td>
</tr>
</tbody>
</table>
NetView FTP System Files

\texttt{/usr/lpp/nftp}

NetView FTP installation directory.

\texttt{$NFTPSYSTEMDIR/nftpwork}$

The directory containing initialization and RDF files for all NetView FTP users.

\texttt{$NFTPSYSTEMDIR/system}$

The directory containing NetView FTP system files, especially for the NetView FTP responder component. This directory has the following subdirectories:

- \texttt{/basket} Basket directory of the NetView FTP responder component. When no complete file specification is given in the remote request, or the authenticated user is \texttt{anonymous}, the file is sent to this directory, unless a different directory was specified with the \texttt{INBASKET} initialization parameter.
- \texttt{/data} Internally used.
- \texttt{/ini} Directory containing the initialization files for the NetView FTP responder component.
- \texttt{/log} Directory containing the log and report files of the NetView FTP responder component and the system log.
- \texttt{/public} Directory from which \texttt{anonymous} users can receive files (no access authorization required), unless a different directory was specified with the \texttt{OUTBASKET} initialization parameter.
- \texttt{/rdf} Currently not used, but must exist.

\texttt{$NFTPSYSTEMDIR/server}$

The directory containing the system files for the NetView FTP server component. This directory has the following subdirectories:

- \texttt{/data} Data directory of the server component containing data files and the file \texttt{srvgrp.tab} that you must create when working with SNA Services/6000.
- \texttt{/ini} Directory containing the initialization files for the NetView FTP server component.
- \texttt{/log} Directory containing the log and report files for the NetView FTP server component.
- \texttt{/rdf} Currently not used, but must exist.
- \texttt{/basket} Currently not used, but must exist.

\texttt{$NFTPWORKDIR}$

The directory containing the NetView FTP user environment:

- \texttt{/basket} Basket directory of the NetView FTP user. When no complete file specification is given in the locally initiated request, NetView FTP uses the basket directory as source (send) or target (receive) directory, unless a different directory was specified with the \texttt{OUTBASKET} or \texttt{INBASKET} initialization parameter.
- \texttt{/data} Internal directory of NetView FTP.
/ini Directory containing the user-private initialization files. If you specify an initialization file that does not exist in the private ini directory, NetView FTP checks the system's ini directory $NFTPSYSTEMDIR/nftpwork/ini.

/log Directory containing the file-transfer log and report files for this specific user.

/rdf Directory containing the user-private RDF files. If you specify an RDF file that does not exist in the private RDF directory, NetView FTP checks the system's rdf directory $NFTPSYSTEMDIR/nftpwork/rdf.

If you have installed NetView FTP Server AIX, continue with “Configuring NetView FTP Server AIX for Remote Communication.” If you have installed NetView FTP Client AIX, continue with Chapter 3, “Verifying Your Local Installation” on page 27.

---

Configuring NetView FTP Server AIX for Remote Communication

The tasks described in the following sections must be performed with root authority. SMIT is used for the configuration tasks.

The panels and their parameters described in the following SMIT dialogs refer to a configuration for a Token-Ring connection. Panels for other types of connections may differ.

Panels may also differ according to SNA levels. Leave any parameter that is displayed but not described in this manual at its default value.

To configure NetView FTP Server AIX for remote communication you must:

- Determine the name of the LU that provides access to the SNA network
- Configure an AIX communication device
- Configure SNA Services/6000 or SNA Server/6000, depending on which of the products you have installed
- Configure the communication paths.

Note: The remote NetView FTP AIX nodes must be configured in the same way to allow for file transfers via the SNA network.

Appendix D, “Sample Profiles for APPC Configuration” on page 111 contains some sample profiles. These samples are provided with the product. You can import the samples and tailor them according to your requirements.
AIX Communication Device Configuration

This section describes the steps you must perform to add the device driver support for the Data Link Controls (DLC) of the specific SNA communication adapter that you are using.

1. Invoke SMIT.
2. Select **Devices** from the System Management menu.
3. Select **Communications** from the Devices menu.
4. Select **Token Ring** from the Communications menu.
5. Select **Services** from the Token Ring menu.
6. Select **Data Link Controls** from the Services menu.
7. Select the **Add a Token Ring Data Link Control** from the Data Link Controls menu.
8. The name of the data link control is displayed. Press ENTER to add the data link control to your configuration.
9. Return to the System Management menu.

Configure SNA Services/6000

You must configure profiles to define the following:

- SNA node
- SNA control point
- Physical unit attachment
- Data link control
- Logical units and associated profiles.

If you define profiles for connections to NetView FTP products on MVS systems, you need some MVS-specific information for some definitions. Ask the system administrator at the MVS node for the required information.

The starting point for configuring profiles to define the SNA network is the Advanced SNA Configuration menu. To get to this menu, do the following:

1. Invoke SMIT.
2. Select **Communications Applications and Services** from the System Management menu.
3. Select **SNA Services** from the Communications Applications and Services menu.
4. Select **Configure SNA Profiles** from the SNA Services menu.
5. Select **Advanced SNA Configuration** from the SNA Profiles menu.
Defining an SNA Node
Use the sample profile provided with SNA Services/6000. Do not modify the profile or add a new profile unless required by your installation.

Defining an SNA Control Point
1. Select Control Point from the Nodes menu to configure your SNA control point.

2. Select Add a Profile to define a new control point.

3. A data entry panel is displayed. Enter the following information:

   PROFILE name
   Enter the name of this profile.

   XID node ID
   Enter the exchange ID (XID) that identifies your physical unit (PU). The node ID must be supplied by the system administrator. It is an eight-digit hexadecimal number.

   The first three digits identify the product and should be 071 to indicate the RISC System/6000.

   For a connection to NetView FTP on MVS, these digits must be the same as in the IDBLK parameter in the VTAM* PU definition for the NetView FTP MVS server.

   The remaining five digits uniquely identify the product within the network. For a connection to NetView FTP on MVS, these numbers must be the same as in the IDNUM parameter in the VTAM PU definition for the NetView FTP MVS server.

   NETWORK name
   This is the network to which the NetView FTP AIX node is attached. This name is supplied by the system administrator.

   If you are attaching to a NetView FTP MVS node, this parameter must have the same value as the SSCPNAME parameter in the VTAM start statement of the NetView FTP MVS server.

   CONTROL POINT name
   This is the name of the local control point. This name is supplied by the system administrator.

4. Press ENTER.

5. Return to the Advanced SNA Configuration menu.

Defining a Physical Unit
1. Select Physical Units from the Advanced SNA Configuration menu.

2. Select Token Ring from the Physical Units menu.

   The Token Ring menu contains two options:
   - Token Ring Attachment
   - Token Ring Data Link Control.
3. Define the data link control:
   Use the sample profile provided with SNA Services/6000. Do not modify the Token Ring Logical Link and the Token Ring Physical Link profiles or add new profiles unless required.

4. Define the attachment:
   a. Select **Token Ring Attachment**.
   b. Select **Add a Profile**.
   c. A data entry screen is displayed. Enter the following information:

   **PROFILE name**
   Enter the name of the Token Ring Attachment Profile. An attachment represents the physical connection to a partner transfer program. An attachment can be referred to by one or more connection profiles.

   **CONTROL POINT profile name**
   Display the list of previously configured profiles, select a name, and press ENTER.

   **LOGICAL LINK profile name**
   Display the list of previously configured profiles, select a name, and press ENTER.

   **PHYSICAL LINK profile name**
   Display the list of previously configured profiles, select a name, and press ENTER.

d. The remaining fields vary according to the type of network to which this physical attachment gives access. You must provide physical addresses (for example, LAN addresses) and define the call type of the attachment.

e. Press ENTER to save the information.

f. Return to the Advanced SNA Configuration menu.

### Defining Logical Units and Associated Profiles

1. Select **Logical Units** from the Advanced SNA Configuration menu.

2. Select **LU6.2**. This gives access to all of the options for configuring LUs and their associated profiles:
   a. Define the local LU:

      1) Select **LU6.2 Local Logical Unit** from the LU6.2 menu.
      2) Select **Add a Profile** to define a local LU.
      3) A data entry panel is displayed. You must set the fields as follows:

      **PROFILE name**
      Enter a name to identify the local LU profile. Usually it is the same name as is used for the LU.

      **TPN LIST profile name**
      This field specifies the profile containing the list of local transaction programs.
**NETWORK name**
Enter the name of your network. This name is the same across the entire network. It must also be known at the remote node. If the remote node is a NetView FTP MVS system, this field must contain the same value as the NETID parameter in the VTAM start statement that is used at the MVS system.

**Local LU NAME**
Enter the name of the local LU. The LU name must be unique throughout the network and must be known at the remote node. If the remote node is NetView FTP MVS, this field must contain the same value as defined in the VTAM LU definition statement at the MVS system.

**INDEPENDENT LU?**
Set this field to **yes**.

The other fields need not be filled in as they only apply if INDEPENDENT LU is set to **no**.

4) Press ENTER to save the changes.
5) Return to the LU6.2 menu.

b. Define logical connections:

1) Select **LU6.2 Logical Connection**.
2) Select **Add a Profile**.
3) A data entry panel is displayed. Set the fields as follows:

**PROFILE name**
The name of the logical connections profile. Select a name by which the connection can be clearly identified.

**ATTACHMENT profile name**
The name of the profile that identifies the attachment (PU) that this connection uses (see step 4 of “Defining a Physical Unit”).

**Note:** More than one connection profile can refer to the same attachment by this profile name. That is, for communication with NetView FTP V2.2 MVS, you can have one attachment profile that defines the link to NetView FTP V2.2 MVS and one connection profile for each NetView FTP V2.2 MVS server that is defined as logical unit in VTAM.

**LOCAL LU profile name**
The name of the profile that identifies the local LU that this connection uses (see step 2a of “Defining a Physical Unit”).

**NETWORK name**
The name of the network of which this connection is a part. This name was defined when you configured your SNA node (see “Defining an SNA Node” on page 18).
REMOTE LU name
Enter the name of the remote LU to which this connection attaches. The name must be the same as that used at the remote site to refer to this LU. Ask the system administrator at the remote site for the name of the LU.

REMOTE TPN LIST profile name
Enter the name of the profile containing the list of allowed remote transaction programs (see step 2h on page 24).

MODE LIST profile name
Enter the name of the profile containing the list of allowed modes for use on this connection (see step 2d on page 22).

INTERFACE type
Select extended to indicate that NetView FTP uses the extended interface to SNA Services/6000.

SESSION CONCURRENCY
Select parallel to indicate that NetView FTP AIX makes use of parallel conversations on this connection when this is supported by the remote node.

c. Define a conversation mode:

1) Select LU6.2 Mode from the LU6.2 menu.
2) Select Add a Profile.
3) A data entry panel is displayed. Set the fields as follows:

PROFILE name
The name of the mode profile. Use FTPBIND.

MODE name
The name of the mode. Use FTPBIND. The same name must be configured at the remote site as well.

Maximum number of SESSIONS
This field specifies the maximum number of conversations that can exist simultaneously on a connection using this mode. Set this field to 32.

RECEIVE pacing
Set this field to 63.

SEND pacing
Set this field to 63.
Maximum RU SIZE

Set this field to a value between 256 and 3840. Increment by 32 bytes. The value you set for this field affects the performance. In general, the performance improves when you set a higher value for this field. Then, however, more system resources are consumed.

The value for Maximum RU SIZE relates to the settings made in the SNA Token Ring Logical Link Profile. For further information refer to the SNA Services/6000 manuals.

**Note:** For all NetView FTP environments, the default LU6.2 mode is FTPBIND. The values in this mode definition have been selected to allow for file transfers between all of the different environments (different operating systems, different machines), they have not been selected for high performance.

If you want to use a bigger RU size, increase the value of the RU size parameter in the FTPBIND mode definition or use either the NFTP1K profile or the NFTP2K profile, which are provided with the product.

It depends, however, on the session partner whether the RU size you specified is accepted.

4) Press ENTER to save the changes.

5) Return to the LU6.2 menu.

d. Add the modes to a mode list:

1) Select **LU6.2 Mode List** from the LU6.2 menu.

2) Choose **Add a Profile** to update the existing profile.

3) A data entry panel is displayed. Specify the name of the mode-list profile and the names of all conversation-mode profiles that you want to add to this mode list.

4) Press ENTER to save the changes.

5) Return to the LU6.2 menu.

e. Define the local transaction program names (TPN) by adding a profile for the sending and for the receiving transfer programs:

1) Select **LU6.2 Transaction Program Name (TPN)** from the LU6.2 menu.

2) Select **Add a Profile** to define a new profile.

3) Fill in the data fields as follows:

   **PROFILE name**
   Enter dvgftpb1.

   **TRANSACTION program name**
   Do not insert the NetView FTP transaction program name. Instead enter a value that can serve as placeholder.
PIP data?
Set the value of this field to yes.

If you set this field to no, NetView FTP Server AIX cannot receive any workstation IDs specified with the request keyword RMTWSTID. NetView FTP Server AIX then uses the TCP/IP host name as the default name for the responder component. So, no other responder components can be addressed.

For NetView FTP to work properly in this setup, the responder component must run on the same workstation as the server component.

If yes, SUBFIELDS
Set this field to 1.

CONVERSATION type
Set the value of this field to basic to indicate that basic conversations should be used.

SYNC level
Set the value of this field to confirm.

Full PATH to TPN executable
Enter /usr/bin/dvgcsac.exe for the NetView FTP TPN path.

MULTIPLE INSTANCES supported?
Set the value of this field to yes to allow multiple instances of the transaction program to run simultaneously.

User ID
Set this field to the user instance number of root.

The other fields have default values that you can leave unchanged.

4) Press ENTER to save the information.
5) Return to the LU6.2 menu.

f. Add the local TPNs to a local TPN List:
   1) Select LU6.2 Transaction Program Name List from the LU6.2 menu.
   2) Select Add a Profile to define a new group.
   3) Enter a profile name for the TPN group and the names of all TPN profiles you want to include in that list.
   4) Press ENTER to save the information.
   5) Return to the LU6.2 menu.

g. Define the remote TPN. Add a profile for the sending and for the receiving TP at the remote node:
   1) Select LU6.2 Remote Transaction Program Name (RTPN) from the LU6.2 menu.
   2) Select Add a profile to define a new profile.
3) Fill in the data fields as follows:

**PROFILE name**
Enter the profile name for the remote TP.

**Note:** Fill in the following fields exactly as specified.

**TRANSACTION program name**
Enter `rtpn` for the remote NetView FTP TP.

**PIP data ?**
Toggle the value of this field to `yes`.

If you set this field to `no`, NetView FTP Server AIX cannot receive any workstation IDs specified with the request keyword `RMTWSTID`. NetView FTP Server AIX then uses the TCP/IP host name as the default name for the responder component. So, no other responder components can be addressed.

For NetView FTP to work properly in this setup, the responder component must run on the same workstation as the server component.

**SYNC level**
Toggle the value of this field to `confirm`.

The other fields have default values that you can leave unchanged.

4) Press ENTER to save the information.

5) Return to the LU6.2 menu.

h. Add the remote TPNs to a remote TPN list:

1) Select **LU6.2 Remote Transaction Program Name List** from the LU6.2 menu.

2) Select **Add a Profile** to define a new group.

3) Enter the profile name for the RTPN list and the names of all remote TPs you want to include in this list.

4) Press ENTER to save the information.

5) Return to the LU6.2 menu.

**Verifying Your SNA Services/6000 Configuration**

You can use SMIT to perform basic consistency checks on your configuration. These checks help to spot typing errors in cross-references between profiles.

1. Go to the Advanced SNA Configuration menu in SMIT.

2. Select **Verify SNA Configuration Profiles** and wait for the response.

3. If there is an error, a warning message is issued. If the configuration is correct, the command status in the top left-hand corner of your screen shows OK.
Configure SNA Server/6000

SNA Server/6000 must be installed and the profiles needed for basic operations, such as SNA node, SNA control point, or data link control, must already be defined.

To run NetView FTP AIX with SNA Server/6000, you must configure the following:

- A local-transaction-program profile with the name `dvgftpb1`.
- Conversation mode profiles. You need at least one profile with the name `FTPBIND`. This is the default name NetView FTP uses. For any other conversation mode profile that you define you can choose whatever name you like.

The definitions you make in the mode profile have an effect on the performance, especially the value you select for the RU size.

In general, the performance improves when you set a higher value for this parameter. Then, however, more system resources are consumed.

The value for Maximum RU SIZE relates to the settings made in the SNA Data Link Control Profile. For further information refer to the SNA Server/6000 manuals.

**Note:** For all NetView FTP environments, the default conversation mode is `FTPBIND`. The values in this mode definition have been selected to allow for file transfers between all of the different environments (different operating systems, different machines), they have not been selected for high performance.

If you want to use a bigger RU size, increase the value of the RU size parameter in the FTPBIND mode definition or use one of the profiles NFTP1K, NFTP2K, NFTP4K, NFTP8K, NFTP16K, or NFTP32K, which are provided with the product. It depends, however, on the session partner whether the RU size you specified is accepted.

- A side information profile with the name `dvgftpsi`.
- A profile for a token-ring link station that defines the control characteristics that support calls from other nodes.

You can use the local control point as default LU. However, if you have defined a local LU for NetView FTP, you must define this local LU in the side information profile `dvgftpsi`.

To enable file transfers to and from remote locations, define the following profiles for every location:

- A link-station profile (SDLC, Ethernet, token ring, X.25, or APPN* connection network)
- A profile for the LU6.2 partner LU
- A profile for the partner LU6.2 location.
Configure the Communication Paths

If you have installed SNA Services/6000, you must have a server group table. For SNA Services/6000 it contains the names of all connection profiles that you want to use with NetView FTP and that are defined in the SNA configuration.

If you have installed SNA Server/6000, a server group table is optional. If no server group table is defined, you have to define a listening link station profile and a partner LU profile for those connections:

- On which you want to listen for remotely initiated file transfers
- Where locally initiated file transfers can be performed.

If a server group table is defined for SNA Server/6000, it must have one of the following contents:

- An asterisk (*); all remotely initiated requests are accepted.
- Partner LU alias names that are also specified in the SNA LU6.2 partner LU profiles. Remotely initiated requests are accepted only for those locations for which a partner LU alias exists.

In your request you can address the remote transfer partner by specifying either the fully qualified LU name (RMTLU) or the partner LU alias (RMTNODE) as defined in the partner LU profile.

Generate the file /home/nftp/server/data/srvgrp.tab. You can find a sample server group table in Appendix D, “Sample Profiles for APPC Configuration” on page 111.
Chapter 3. Verifying Your Local Installation

This chapter describes how to verify the local installation of NetView FTP Server AIX and NetView FTP Client AIX. It covers the following tasks:

1. Starting the NetView FTP system daemon (requires superuser authorization)
2. Starting the NetView FTP server component (requires superuser authorization)
3. Starting the NetView FTP responder component (requires superuser authorization)
4. Starting a NetView FTP client environment.

This chapter provides you with technical background and discusses possible error causes in your local network. Read this chapter carefully and compare the shown initialization and log files with those of your installation.

Starting the NetView FTP System Daemon

The NetView FTP system daemon is a background process that controls the NetView FTP resources on your local workstation. If the daemon is not running, nobody can work with NetView FTP on that workstation. So, an AIX system administrator can control the NetView FTP activities on this workstation by starting or stopping the NetView FTP system daemon.

To start the NetView FTP system daemon, type `nftpd start` at the command prompt. Information similar to the following is displayed:

```
***************
*             *
*  NetView File Transfer Program for Workstations  *
*  Command Line Interface                      *
*                                              *
*  Copyright International Business Machines Corp., 1994 *
*  Reproduction, use and transfer restricted.     *
*  See IBM Conditions of Use.                   *
*                                              *
***************

nftpd: Processing of < start > command completed!

Function successfully completed
Action : No action required
```

During the startup of the system daemon the following happens:

- The daemon process (`/usr/bin/dvgdem.exe`) itself is started. This process must be contained in the process table.
• Several system log files are initialized. These files are stored in NFTPSYSTEMDIR/system/log:
  – The system log file syslog.dat that stores all internal used system resources
  – The responder-component log and report files, log.dat and report.dat
  – The user-interface log file guimsg.dat that contains error messages written by the graphical user interface programs.

• Internal system semaphores are created to realize a controlled access of system resources.

If the start of the NetView FTP system daemon is not successful, do the following:

• Check if the daemon is already active. Search the process table for a process with the name dvgdem.exe by using the commands ps -ef | grep dvgdem.exe. If there is an entry, the daemon is already started.

• Check the log file /home/nftp/system/log/log.dat for a possible explanation. Probably your directory structure is not set up correctly. See “NetView FTP System Files” on page 15 for the directories that must exist.

• If you still cannot start the NetView FTP system daemon, purge the system environment.

  **Warning:** All environments (server, responder, client) can then be corrupted.

  To purge the system environment, type nftpd purge at the command prompt. After having purged the environment, you must restart all components.

After having started the daemon process, start the server component of NetView FTP.

### Starting the NetView FTP Server Component

Before starting the NetView FTP server component, check the following:

1. The initialization file of the server component must be configured. This file must reside in the directory /home/nftp/server/ini.


   If you have installed SNA Services/6000, the startup sequence for the server components of the local and the remote NetView FTP Server AIX depends on the type of attachment that is defined for the respective server. Make sure that the server that is defined as listener is started first.

3. The NetView FTP system daemon must be running.

To start the NetView FTP server component use the nftpd startsrv command. If the start of the server component was successful, a corresponding message is displayed.
After a successful startup you need not check the server log file. However, during verification display the file `log.dat` in the directory `/home/nftp/server/log` to verify that your log file looks similar to the one shown:

```
1994-/zerodot9-12 15:59:44; DVG01001:******************************************************
1994-/zerodot9-12 15:59:44; DVG00591: Parsing initialization parameter file /home/nftp/server/ini/ibmnftp.ini
1994-/zerodot9-12 15:59:44; DVG00931: The following default value(s) will be assumed:
1994-/zerodot9-12 15:59:44; DVG00941: ServerPort = < 5735 >
1994-/zerodot9-12 15:59:44; DVG00941: Protocol = < TCPIP >
1994-/zerodot9-12 15:59:44; DVG00941: Trace = < NO >
1994-/zerodot9-12 15:59:44; DVG00941: ModeName = < FTPBIND >
1994-/zerodot9-12 15:59:44; DVG00941: MaxClients = < 512 >
1994-/zerodot9-12 15:59:44; DVG00631: Initialization parameters:
1994-/zerodot9-12 15:59:44; DVG00941: MaxClients = < 512 >
1994-/zerodot9-12 15:59:44; DVG00941: MaxTransfers = < 16 >
1994-/zerodot9-12 15:59:44; DVG00941: ModeName = < FTPBIND >
1994-/zerodot9-12 15:59:44; DVG00941: ServerPort = < 5735 >
1994-/zerodot9-12 15:59:44; DVG00941: Protocol = < TCPIP >
1994-/zerodot9-12 15:59:45; DVG00461: Local workstation ID (TCP/IP hostname) = fred ; IP number = 1.234.5.67
1994-/zerodot9-12 15:59:45; DVG02001: NetView FTP Server for AIX is running with SNA Services/6/zerodot/zerodot Version 1.2
1994-/zerodot9-12 15:59:45; DVG01601: NetView FTP Server for AIX is listening for NetView FTP Clients using the communication protocol TCP/IP
1994-/zerodot9-12 15:59:45; DVG00401: NetView FTP Server for AIX successfully started
```

The server log shows the initialization parameters that are used during runtime. In the example the parameters are:

- **MAXCLIENTS = 512.** This parameter determines that a maximum of 512 clients can register to this server component.
- **MAXTRANSFERS = 16.** This parameter specifies that the server component can start a maximum of 16 parallel transfers.
- **MODENAME = FTPBIND.** That is the name of the SNA log mode.
- **SERVERPORT = 5735.** That is the default server port. A port, together with the host name or the IP address, specifies the destination of a TCP/IP application. You can change the server port, but then you must also change the initialization files of the NetView FTP Client.

**Note:** If you receive the error message `address already in use`, another application is using the same port number. In this case, change the port number of either the server component or the concurrent application.

- **PROTOCOL = TCPIP.** Currently the NetView FTP Server AIX supports only TCP/IP as protocol.
- **TRACE = NO.** When setting the trace indicator to YES, you get an expanded log output. Do this only in case of any problems, because tracing slows down the performance.

Furthermore, the log shows the local workstation IDs, the SNA services provider, and whether the startup was successful.

During the startup of the server component the following happens:

- Internal resources of the server component (shared memories and semaphore) are allocated. Their IDs are written to the file `/home/nftp/system/log/syslog.dat`.
- The server log file `/home/nftp/server/log/log.dat` is initialized.
Three processes are established:

1. The server component’s main process (/usr/bin/dvgcs.exe) that controls the established child processes.
2. The server component’s listen-for-clients (LC) process that controls the connections between the clients and the server component. The corresponding process name is /usr/bin/dvgcslc.exe.
3. The server component’s accept-conversations (AC) process that controls the connections between the server component and other SNA nodes. The corresponding process name is /usr/bin/dvgcsac.exe.

If the start of the NetView FTP server component is not successful, do the following:

- Check if the server component is already running. Search the process table for processes named dvgcs.exe, dvgcsac.exe, and dvgcslc.exe by using the commands `ps -ef | grep dvgcs*`. If there are entries, the NetView FTP server component is already started.
- Check the log file /home/nftp/server/log/log.dat for an explanation. Possible error causes are:
  - Invalid directory structure. See “NetView FTP System Files” on page 15 for the directories that must exist.
  - Invalid setup of the SNA communication subsystem. Contact your SNA administrator to have the subsystem set up correctly.
- If you still cannot start the NetView FTP server component, purge the system environment.

**Warning:** All environments (server, responder, client) can then be corrupted. Make sure that all NetView FTP system activities are stopped before you purge the system.

To purge the system environment, type `nftpd purge` at the command prompt. After having purged the environment, you must restart all components.

After having started the server component of NetView FTP, you can start the responder component of NetView FTP AIX.

---

**Starting the NetView FTP Responder Component**

After having started the NetView FTP server component, you can activate the responder component.

The NetView FTP responder component controls the remote access to a workstation. Without a responder component being started, a workstation cannot be accessed from any other node.

Before starting the responder component on a workstation, check the following:

- The NetView FTP system daemon must be active.
- The NetView FTP server component specified in the responder component’s initialization file must be started. If you specify IPSERVERWSTID=fred. in the responder component’s initialization file, the NetView FTP server component on workstation **fred** must be running.
Start the NetView FTP responder component by entering the `nftpd startresp` command. You receive a message telling you whether the command completed successfully.

Your log file `/home/nftp/system/log/log.dat` must be similar to this:

```
1994-09-12 17:04:03; DVG00451: NetView FTP for AIX ; Version 1.1.0 ; Maintenance Level < Tue Sep  6 13:49:29 1994 >
1994-09-12 17:04:25; DVG01001:******************************************************************************
1994-09-12 17:04:25; DVG00591: Parsing initialization parameter file /home/nftp/system/ini/ibmnftp.ini
1994-09-12 17:04:25; DVG00931: The following default value(s) will be assumed:
1994-09-12 17:04:25; DVG00941: Protocol = < TCPIP >
1994-09-12 17:04:25; DVG00941: Trace = < NO >
1994-09-12 17:04:25; DVG00941: Rootaccess = < NO >
1994-09-12 17:04:25; DVG00941: SecPar = < YES >
1994-09-12 17:04:25; DVG00941: ServerPort = < 5735 >
1994-09-12 17:04:25; DVG00631: Initialization parameters:
1994-09-12 17:04:25; DVG00941: IPServerWorkstationID = < fred >
1994-09-12 17:04:25; DVG00941: MaxTransfers = < 16 >
1994-09-12 17:04:25; DVG00941: CreateDirectory = < YES >
1994-09-12 17:04:25; DVG00941: Protocol = < TCPIP >
1994-09-12 17:04:25; DVG00941: Rootaccess = < NO >
1994-09-12 17:04:25; DVG00941: SecPar = < YES >
1994-09-12 17:04:25; DVG00941: ServerPort = < 5735 >
1994-09-12 17:04:25; DVG00941: Trace = < NO >
1994-09-12 17:04:25; DVG00461: Local workstation ID (TCP/IP hostname) = iris ; IP number = 1.234.5.24
1994-09-12 17:04:25; DVG00351: '1.234.5.24' is calling remote partner 'fred'
1994-09-12 17:04:26; DVG00351: '1.234.5.24' is calling remote partner 'fred'
1994-09-12 17:04:25; DVG00421: NetView FTP Responder < 1.234.5.24 > successfully started
1994-09-12 17:04:26; DVG01811: Directory access for incoming files of anonymous users limited to: /home/nftp/system/basket
1994-09-12 17:04:26; DVG01821: Public read access directory for anonymous users limited to: /home/nftp/system/public
```

The log file shows the initialization parameter for the responder component:

- **IPSERVERWSTID = fred.** That is the host name of the server component's workstation. You can also specify the IP address directly. In this case, the server component is running on workstation **fred**, the responder component is running on workstation **iris**. The NetView FTP server component on workstation **fred** is listening on the default port 5735. If responder component and server component are running on the same workstation, specify the local host name of the responder component and the server component.

- **MAXTRANSFERS = 16.** The responder component can handle up to 16 parallel transfers.

- **CREATEDIRECTORY = YES.** If a nonexisting directory is specified in an incoming request, the directory is created by NetView FTP. If CREATEDIRECTORY is set to NO and the directory does not exist, the file transfer is rejected.

- **PROTOCOL = TCPIP.** The responder component uses TCPIP as protocol.

- **ROOTACCESS = NO.** If the receiving user ID is **root** and this parameter is set to NO, the file transfer is rejected.

**Warning:** User **root** is the owner of the AIX system files. When you set this parameter to YES, all files owned by **root** can be modified by file transfers.

- **SECPAR = YES.** If SECPAR is set to YES, the responder component can be accessed via the **anonymous** user ID. With this user ID, a user at a remote node can access a limited set of directories on your workstation.

- **TRACE = NO.** In case of any problems, set this parameter to YES to get an expanded log output.
The log file lists the local host name and IP address, the directories that can be accessed via **anonymous**, and messages for any errors that occurred during startup.

During the startup of the responder component, the following happens:

- Internal resources of the responder component (shared memory and semaphore) are allocated. Their IDs are written to the file `/home/nftp/system/log/syslog.dat`.

- The responder process `/usr/bin/dvgrsp.exe` is established. This process runs as a daemon process.

- The responder component tries to register to the remote server component with IPSERVERWSTID and SERVERPORT. If the server component is not started or is listening on another port, the responder start fails.

- The responder component creates a dynamic port that is stored in the server component’s responder table. Whenever a file-transfer request comes in for that responder component, the server component calls the responder component with this dynamic port number. Therefore, a responder component does not have a fixed well-known port.

- When a file-transfer request comes in, the responder component starts a new process and a transfer manager (`/usr/bin/dvgtm.exe`). This transfer manager handles the file transfer: It authenticates the caller, checks for file sizes, opens the files, and so on.

If the start of the responder component is not successful, do the following:

- Check if the responder component is already running. Search the process table for a process with the name `dvgrsp.exe`, using the commands `ps -ef | grep dvgrsp`. If there is an entry, the responder component is already started. You can stop the responder component with the `nftpd stoprsp` command and restart it afterwards. Note that file transfers that are active on this responder component are stopped as well.

- Check the log file `/home/nftp/system/log/log.dat` for an explanation. Possible error causes are:
  - Invalid directory structure. See “NetView FTP System Files” on page 15 for the directories that must exist.
  - Invalid entries for IPSERVERWSTID or SERVERPORT or both. Check if the NetView FTP server component is really running on the specified node and the specified port when it does not use the default port. Try to ping the workstation. If the ping is not successful, contact your TCP/IP administrator. Also, check the log file for further information.

- If you still cannot start the responder component, purge the system environment.

  **Warning**: All environments (server, responder, client) can then be corrupted. Make sure that all NetView FTP system activities are stopped before you purge the system.

  To purge the system environment, type `nftpd purge` at the command prompt. After having purged the environment, you must restart all components.
Starting a NetView FTP Client Environment

Before starting a NetView FTP Client AIX, check the following:

1. The client environment must exist and must have been customized.
2. The NetView FTP Server AIX specified in the client's initialization file must be running. Otherwise you cannot start the client environment.
3. Be aware of ownerships in AIX. If user fred starts the environment, fred becomes the owner of that environment. Only the owner can stop the environment. However, multiple users can share one environment, but these users must have write access for that environment.

The NetView FTP Client is started with the nftp start command. Note that you can specify an initialization file together with this command. This initialization file can reside in the private (NFTPWORK/ini) or the system environment (NFTPSYSTEMDIR/nftpwork/ini).

When you start the client, a message is displayed that tells you whether the command completed successfully.

You need not start the client environment explicitly. When you issue an nftp send or an nftp receive command and the client environment is not active, it is started then.

During client startup the following happens:

- Internal resources (semaphore and shared memory) are allocated.
- The initialization parameters are checked.
- The NetView FTP server component specified in the initialization file is called.

If the server component is not active, the NetView FTP Client cannot be started.

The following is an example of a log file that is written after a successful client start:

```
1994-09-13 10:01:21; DVG00001:******************************************************************************
1994-09-13 10:01:21; DVG00591: Parsing initialization parameter file /u/plo/nftpwork/ini/ibmnftp.ini
1994-09-13 10:01:21; DVG00931: The following default value(s) will be assumed:
1994-09-13 10:01:21; DVG00941: Protocol = < TCPIP >
1994-09-13 10:01:21; DVG00941: Trace = < NO >
1994-09-13 10:01:21; DVG00941: Rootaccess = < NO >
1994-09-13 10:01:21; DVG00941: SecPar = < YES >
1994-09-13 10:01:21; DVG00941: ServerPort = < 5735 >
1994-09-13 10:01:21; DVG00631: Initialization parameters:
1994-09-13 10:01:21; DVG00941: IPServerWstID = < fred >
1994-09-13 10:01:21; DVG00941: MaxTransfers = < 16 >
1994-09-13 10:01:21; DVG00941: CreateDirectory = < YES >
1994-09-13 10:01:21; DVG00941: OpMode = < ATTENDED >
1994-09-13 10:01:21; DVG00941: Protocol = < TCPIP >
1994-09-13 10:01:21; DVG00941: RetryAttempts = < 10 >
1994-09-13 10:01:21; DVG00941: RetryDelay = < 30 >
1994-09-13 10:01:21; DVG00941: Rootaccess = < NO >
1994-09-13 10:01:21; DVG00941: SecPar = < YES >
1994-09-13 10:01:21; DVG00941: ServerPort = < 5735 >
1994-09-13 10:01:21; DVG00941: Trace = < NO >
1994-09-13 10:01:21; DVG00461: Local workstation ID (TCP/IP hostname) = iris ; IP number = 1.234.5.24
1994-09-13 10:01:21; DVG00351: '1.234.5.24' is calling remote partner 'fred'
1994-09-13 10:01:21; DVG00401: NetView FTP Client for AIX successfully started
```
Some of the important initialization parameters are:

- **IPSERVERWSTID = fred.** The NetView FTP server component is running on workstation **fred.** The server component is listening on its default port 5735.

- **OPMODE = ATTENDED.** Messages that are created during the file transfer are written to standard output. If OpMode is set to unattended, the messages are written to the report file only.

- **RETRYATTEMPTS = 10.** If a recoverable error occurs during the file transfer, the transfer manager tries 10 times to recover from that error. After 10 unsuccessful attempts, the file transfer is rejected.

- **RETRYDELAY = 30.** This parameter specifies the wait time between two transfer attempts. In this case, the time interval is set to 30 seconds.

If you cannot start the client, do the following:

1. Check if the client is already active. You can directly transfer files.

2. The client cannot register to the server component. The reason can be:
   - The NetView FTP server component is not started. Start your server component.
   - The NetView FTP server component cannot handle any more clients. Consider increasing the value of the MAXCLIENTS parameter in the server component’s initialization file.
   - The NetView FTP server component is listening to another port. Change the client’s initialization file accordingly and restart the client.
   - Network problems. Try to ping the server. If you do not receive an echo, contact your TCP/IP administrator.

After having successfully started the server component, the responder component, and the client, you can work with NetView FTP AIX.
Initialization parameters define some aspects of how NetView FTP AIX works. They are contained in a file that is read during the startup of NetView FTP AIX. The default initialization (ini) file is called ibmnftp.ini, but you can have more than one initialization file to suit your needs. The initialization files are located in the ini subdirectory of the respective environment. The initial setup of the initialization parameter file is done during the installation (you are prompted for parameter values).

By changing the initialization parameters, you can modify some aspects of how NetView FTP AIX operates. You do not have to change the initial settings, but you can do so either during the installation or at any later time. If you want to change the initialization parameters after the installation, you can either edit the file ibmnftp.ini with an editor that can handle ASCII files or invoke the customization dialog in the graphical user interface.

Parameters are defined in the following form:

```
>>>keyword=--value
```

If you make changes, you must stop and restart NetView FTP AIX for the changes to take effect.
## Overview of the Initialization Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>NetView FTP Server AIX</th>
<th>NetView FTP Client AIX</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters Defining NetView FTP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LU Name</td>
<td>Mandatory</td>
<td>—</td>
</tr>
<tr>
<td>Network ID</td>
<td>Mandatory</td>
<td>—</td>
</tr>
<tr>
<td>Communication Protocol</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>IP Server Workstation ID</td>
<td>—</td>
<td>Mandatory</td>
</tr>
<tr>
<td>UMASK</td>
<td>Optional (responder component only)</td>
<td>Optional (responder component only)</td>
</tr>
<tr>
<td><strong>Parameters Controlling the Communication Subsystem</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNA Mode Name</td>
<td>Default</td>
<td>—</td>
</tr>
<tr>
<td><strong>Parameters Controlling Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Scope</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Root Access</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td><strong>Parameters Controlling Transfers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Directories</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Default Directory for Incoming Files</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Default Directory for Outgoing Files</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Maximum Number of Clients</td>
<td>Default</td>
<td>—</td>
</tr>
<tr>
<td>Maximum Number of Transfers</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Retry Attempts</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Retry Delay</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td><strong>Parameters Controlling Logging and Reporting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation Mode</td>
<td>Default</td>
<td>Default</td>
</tr>
<tr>
<td>Trace</td>
<td>Default</td>
<td>Default</td>
</tr>
</tbody>
</table>

**Notes:**
- **Mandatory**: You **must** specify a value for this parameter.
- **Default**: The transfer program uses a **default** value unless you specify a different value.
- **Optional**: You **can** specify a value for this parameter. If you do not, the transfer program does not provide a default value.
- **—**: Do not specify a value for this parameter.
Communication Protocol

Use this parameter to specify the communication method.

```
protocol = TCPIP
```

Where:

TCPIP Is the default value for NetView FTP AIX.

Create Directory

Use this parameter to specify whether NetView FTP AIX can create the directory specified for a receiving file if that directory does not already exist.

```
createdirectory = YES
```

Where:

YES Allows NetView FTP AIX to create directories.

NO Does not allow NetView FTP AIX to create directories.

Default Directory for Incoming Files

Use this parameter to specify a default directory for incoming files. Incoming files for which no path has been specified are stored in this directory. When you start a responder component, this directory and its subdirectories are also the only directories to which receiving files can be written by the anonymous user.

```
inbasket = NFTPSYSTEMDIR/system/basket
```

Where:

NFTPSYSTEMDIR/system/basket Is the directory for a responder component. NFTPSYSTEMDIR is the directory that is defined in the environment variable NFTPSYSTEMDIR.

NFTPWORK/basket Is the directory for a requester. NFTPWORK is the directory that is defined in the environment variable NFTPWORK.
Default Directory for Outgoing Files

Use this parameter to specify a default directory for outgoing files. If no path has been specified for an outgoing file, NetView FTP searches this directory for the file. When you start a responder component, this directory and its subdirectories are also the only directories from which files can be sent by the anonymous user.

Where:

**NFTPSYSTEMDIR/system/public**
Is the directory for a responder component. **NFTPSYSTEMDIR** is the directory that is defined in the environment variable NFTPSYSTEMDIR.

**NFTPWORK/basket**
Is the directory for a requester. **NFTPWORK** is the directory that is defined in the environment variable NFTPWORK.

IP Server Workstation ID

Use this parameter to specify the TCP/IP address or the IP host name of the server workstation. This address or nickname is used in the communication between NetView FTP Server and NetView FTP Client in an IP network.

Where:

**workstation-address**
Is a string of 7 to 15 characters.

The workstation address is the decimal representation of the Internet address of the NetView FTP Server workstation that serves the requesting NetView FTP Client. The address must be unique in the IP network.

The workstation address encodes both a network ID and a host ID. The host ID can represent a single host or a subnet with one or more hosts.

Enclose this value in single quotes (').

**workstation-nickname**
Is a string of up to 63 characters.

The workstation nickname is the nickname of the NetView FTP Server workstation that serves the requesting NetView FTP Client. This nickname must be defined in the name server.
Logical Unit Name

Use this parameter to specify the local LU that NetView FTP must use during transfer restart. This LU name must be defined in the SNA configuration of NetView FTP Server AIX and must be uppercase.

**Note:** This parameter applies to NetView FTP Server only.

```
lu_name
```

Where:

- **lu_name** is a string of up to 8 uppercase characters.

Maximum Number of Clients

This parameter applies to the NetView FTP Server only. Use this parameter to specify how many NetView FTP Client programs can be started and can transfer files via the NetView FTP Server. If you use the NetView FTP Server as a stand-alone product, specify 0 for this parameter.

```
maxclients
```

Where:

- **value** is a number from 0 to 512.

Maximum Number of Transfers

Use this parameter to specify how many transfers can run simultaneously on a NetView FTP system.

When you specify this parameter for a NetView FTP Server, the number specifies the maximum number of transfers that can run simultaneously on the NetView FTP Server workstation. These resources are shared among all NetView FTP Client programs connected to the NetView FTP Server.

When you specify this parameter for a NetView FTP Client, the number specifies the maximum number of transfers that a NetView FTP Client program can run simultaneously. Note that the number of simultaneous transfers on a NetView FTP Client workstation is also limited by the resources available on the NetView FTP Server workstation.

```
maxtransfers
```

Where:

- **number** is a number from 1 to 32.
Network Identification

Use this parameter to specify the SNA network ID of the NetView FTP Server AIX. This ID must be used during transfer restart.

The network ID must be defined in the SNA configuration of NetView FTP Server AIX and must be uppercase.

**Note:** This parameter applies to NetView FTP Server AIX only.

```
netid = net_id
```

Where:

- **net_id** is a string of up to 8 uppercase characters.

Operation Mode

Use this parameter to tell NetView FTP AIX the operation mode it is to run in.

```
opmode = UNATTENDED
```

You can specify one of the following values:

- **UNATTENDED** NetView FTP AIX writes report messages to the report collection file.
- **ATTENDED** NetView FTP AIX writes report messages to the screen as well as to the report collection file. If you specify \texttt{WAIT=\textsc{yes}} in your request, the file-transfer messages are displayed in the same window as the request-validation messages. Otherwise, a new window is opened.

A responding system always opens a new window to display the file-transfer messages.

**Note:** A responder component at an AIX system always runs in unattended mode.

Retry Attempts

Use this parameter to specify the number of times NetView FTP AIX retries automatic logon or attempts automatic transfer restarts. If the restart or retry is not successful after this number of attempts, NetView FTP AIX stops processing the file-transfer request.

```
retryattempts = number
```

Where:

- **number** is a number from 1 to 20.
Retry Delay

Use this parameter to specify how long NetView FTP AIX waits before making another automatic logon retry or automatic transfer restart.

```
  >>> retrydelay = time
```

Where:

- **time**
  Is a time interval in the range of 30 to 300 seconds.

Root Access

Use this parameter to specify whether a file-transfer request in which the user ID `root` is specified in the Access Security parameter is rejected. The user ID `root` has privileged access rights that overrule the installed security scheme.

```
  >>> rootaccess = NO
```

Where:

- **NO**
  The file-transfer request is rejected if the user ID `root` is specified in the Access Security parameter.
- **YES**
  The file-transfer request is not rejected if the user ID `root` is specified in the Access Security parameter.

Security Scope

Use this parameter to specify whether the security parameters in the file-transfer request can contain the user ID `anonymous`.

```
  >>> secpar = YES
```

Where:

- **YES**
  NetView FTP AIX requires a complete set of security parameters to be specified in the request. The security parameters are validated. The user ID `anonymous` is not accepted as security parameter.
- **NO**
  You can specify the user ID `anonymous` in the request. Although a password is required, it is not verified. With the user ID `anonymous`, write access is granted only to the `../basket` subdirectory, read access is granted only to the `../public` subdirectory of the responder component.
Where:

- **servername** is a string of up to 8 characters.

**Server Port**

Use this parameter to specify the IP port number of the NetView FTP Server at the workstation addressed by the IP Server Workstation ID that provides SNA connection for a NetView FTP Client.

Where:

- **portnumber** is a number from 5001 to 65535.

**SNA Mode Name**

Use this parameter to specify the SNA mode name that NetView FTP Server uses to allocate a conversation with its partner file-transfer program. The mode name is used to designate the network properties for a group of sessions. The SNA mode name is defined in the SNA conversation mode profile file (see “Defining Logical Units and Associated Profiles” on page 19). It must match a mode name configured at the node of the partner file-transfer program.

**Note:** This parameter applies only to a NetView FTP Server product that serves as an SNA gateway.

Where:

- **name** is an SNA mode name, up to 8 characters long, configured at the node of the partner file-transfer program.

**Trace**

Use this parameter to specify whether NetView FTP AIX has to write an internal trace.

Where:

- **trace** can be either `NO` or `YES`.
Where:

**NO**  No trace data is written to the log file.

**YES**  Trace data is written to the log file.

**Note:** Tracing can slow down the performance of your system.

---

**UMASK**

Use this parameter to set the file-mode creation mask of the NetView FTP responder component. This mask determines which bits of the standard file-mode creation mask are to be cleared for a file or directory when the NetView FTP responder component creates it. If you do not specify UMASK in the initialization file, the file-mode creation mask of the system is used.

\[
\text{UMASK} = \text{nnn}
\]

Where:

**nnn**  
Is a three-digit decimal number. The digits represent the octal values for the access modes that are assigned to the three permission groups: owner, group, other. You can assign a value of 1 to 7 to each permission group.

Figure 3 illustrates how to determine the numerical values for each level of access.

---

**Figure 3. Numerical Representation of Access Modes**

<table>
<thead>
<tr>
<th>Total Value</th>
<th>Read Permission</th>
<th>Write Permission</th>
<th>Execute Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Chapter 5. Getting Started

This chapter describes sample file transfers for users of NetView FTP AIX. The scenarios comprise:

1. Transferring files to and from NetView FTP AIX
2. Transferring files to and from NetView FTP host systems.

In the examples, the sample RDFs XBIN2BIN, BIN2BINX, and TXT2ESDS are used.

In the directory /usr/lpp/nftp/samples you find sample definition files that are provided with the product. Copy the sample RDFs XBIN2BIN, BIN2BINX, and TXT2ESDS from the sample rdf directory to the rdf directory of your private environment.

The notations used in the examples are:

- In commands, the values shown in lowercase italics represent values that you must replace with the appropriate values for your installation. For example, yourid is a placeholder for your own user ID.
- The RDFs contain some values for which you have to substitute the appropriate information. For example, in the statement RMTNODE = cpname replace cpname by a proper connection-profile name.

For sending and receiving files, you have the option to work with either the command-line interface or the graphical user interface. The steps for the command-line interface are marked with $ in the left margin. The steps for the graphical user interface are marked with GUI in the left margin.

Transferring Files to and from NetView FTP AIX

Before requesting a file transfer ensure that:

- At both the requesting (your) NetView FTP system and the responding (remote) NetView FTP system:
  1. The SNA services, that is, the NetView FTP server component, is active.
  2. A connection between both systems has been started.
  3. The server component of NetView FTP Server AIX is active.
- At the responding NetView FTP system, the responder component is active.

When setting up a file transfer to or from NetView FTP AIX, you must know the name of a connection profile that determines the connection to the remote server. This profile must be defined in the SNA setup of the NetView FTP Server AIX to which your client is attached.

You must also know the TCP/IP address or the IP host name of the remote workstation. Ask the system administrator at the remote location for this information.
The workstation ID can be found in the responder component’s message log file in the messages number DVG0042I and DVG0046I. For example:

DVG0042I: NetView FTP Responder < 1.234.5.180 > successfully started and connected to
Server with Luname < ABXYZCD.ZY440000 >
DVG0046I: Local workstation ID (TCP/IP hostname) = auriga ; IP number = 1.234.5.180

Example 1: Sending a File to NetView FTP AIX

You send a copy of the file NFTPTEST.EXE from the NetView FTP sample
directory /usr/lpp/nftp/samples/rdf to a user at a remote workstation. For this
equivalent, you have to know the path for the private basket directory of the user
specified in the Access Security parameter.

$ Enter the nftp send command at the command prompt as follows:
nftp send /r:XRIN2BIN /t:path/NFTPTEST.EXE /d:cpname /w:wstid /su:ruserid

Replace the values shown in lowercase italics as follows:

path With the path for the private basket directory of the remote user
unless you set ruserid to anonymous

cpname With the connection-profile name for the remote workstation

wstid With the TCP/IP address or the IP host name of the workstation
where the responding user resides.

ruserid With the user ID of a user at the remote workstation.

If you specify anonymous and the remote workstation permits transfers with the anonymous user ID, the file is stored in the basket directory of the remote NetView FTP system environment.

You are prompted for the access-security password.

With this command, you override the values specified in the RDF for the receiving
file ID (RFILEID), for the connection-profile name (RMTNODE), the remote
workstation ID (RMTWSTID), and the access security (RSECURP).

If you set the operation mode of NetView FTP to attended, the file-transfer
messages are displayed.

If the operation mode of NetView FTP is unattended, check the file report.dat for a
report of the file transfer. A sample file-transfer report that is written at the sending
system is shown in Figure 6 on page 49.
Invoke the NetView FTP Send window with the `nftpguis` command. The NetView File Transfer - Send window is displayed.

Select `XBIN2BIN` from the list of RDFs.

Fill in the fields as shown in Figure 4, replacing `path` with the path for the private `basket` directory of the remote user. Or, if you want to use the `anonymous` user ID as access-security parameter, delete `path`.

![NetView File Transfer - Send Window](image)

*Figure 4. Example 1: NetView File Transfer - Send Window*
Select the Remote... push button. The Remote Node Information window is displayed (see Figure 5).

![Remote Node Information Window]

Figure 5. Example 1: Remote Node Information Window

Replace cpname with the connection-profile name for the remote workstation. You can do this either by typing or by selecting the corresponding value from the list of destination IDs. Replace wstid with the ID of the workstation where the responding user resides.

Replace userid under Access Security with the user ID of a user at the remote workstation. If you specify anonymous and the remote workstation permits transfers with the anonymous user ID, the file is stored in the $HOME directory of the remote NetView FTP system environment.

In the password field of Access Security, you can either enter a password directly or, if you leave the field unchanged, have NetView FTP prompt you for the password when the file transfer starts.

Select the Transfer push button to send the file.

If the operation mode of NetView FTP is unattended, check the report file for a report of the file transfer.

Figure 6 on page 49 shows a sample file-transfer report written at the sending system.
Figure 6. Sample File-Transfer Report Written at the Sending System

Hints and Tips

End-of-Processing Options (REPOK, SEOPOK, REOPNO):

These options determine what NetView FTP does with the sending and the receiving file after a file transfer. For example, you can tell NetView FTP to delete the sending file after it has been successfully transferred to the remote system: SEOPOK=DELETE

If a message or the report file indicate that anything went wrong before or during the file transfer, refer to “Trouble Shooting” on page 101.
Example 2: Receiving a File from NetView FTP AIX

You receive a copy of the file NFTPTEST.EXE from the workstation to which you sent the file in example 1. The file is received to the default NetView FTP directory on your workstation and has the name NFTPTEST.EXE.

You have to know the path for the private basket directory of the user at the remote workstation. You can find this information in the report for the file transfer in example 1.

Edit the file BIN2BINX and change the control statements as follows:

- For the statement with the keyword SFILEID, replace rpath with the path for the private basket directory of the user at the remote workstation. For example: SFILEID=\home\mic\nftpwork\basket
- For the statement with the keyword RFILEID, either replace rpath by the path for your private basket directory or specify the file name (RFILEID=BIN2BINX.NFTPTEST.EXE).
- Replace cpname by the connection-profile name for the remote workstation.
- Replace wstid by the ID of the remote workstation.
- For the statement with the keyword SSECURP, replace suserid with the appropriate value.
- If you want NetView FTP AIX to send you a file-transfer report, add a statement RNOTIFY=userid. Replace userid in this statement with your own user ID.

Enter the nftp receive command at the command prompt as follows:

```
nftp receive /r:BIN2BINX
```

If you set the operation mode of NetView FTP to attended, the file-transfer messages are displayed.

If the operation mode of NetView FTP is unattended, check the file report.dat for a report of the file transfer. A sample file-transfer report that is written by the requester is shown in Figure 9 on page 53.

Check your basket directory for the file NFTPTEST.EXE. When you invoke NFTPTEST.EXE, the following should be displayed:

Thank you for using NetView FTP for Workstations!
Invoke the NetView FTP Receive window with the `nftpguir` command. The NetView File Transfer - Receive window is displayed.

Select BIN2BINX from the list of RDFs. NetView FTP changes the names of the sending and the receiving file as shown in Figure 7.

![NetView File Transfer - Receive Window](image)

*Figure 7. Example 2: NetView File Transfer - Receive Window*
Select the Remote... push button. The Remote Node Information window is displayed (see Figure 8).

![Remote Node Information Window](image)

**Figure 8. Example 2: Remote Node Information Window**

Select the Transfer push button to receive the file.

If the operation mode of NetView FTP is **unattended**, check the report file for a report of the file transfer.

Figure 9 on page 53 shows a sample file-transfer report written by the requester.

Check your **basket** directory for the file NFTPTEST.EXE. When you invoke NFTPTEST.EXE, the following should be displayed:

Thank you for using NetView FTP for Workstations!
Hints and Tips

Report Recipients (RNOTIFY, SNOTIFY):

These parameters determine the recipients of the file-transfer report at the sending and the receiving node.
If a message or the report file indicate that anything went wrong before or during the file transfer, refer to “Trouble Shooting” on page 101.

Transferring Files to and from NetView FTP MVS

Before requesting a file transfer ensure that:

1. At the requesting (your) NetView FTP system:
   a. The SNA services, that is, the NetView FTP server component, must be active.
   b. A connection between both systems must have been started.
   c. The server component of NetView FTP Server AIX must be active.
2. The server at the NetView FTP host system is active.
3. If a security program is active at the host system, there are valid access-security parameters for the host system (xSECURP).

When setting up a file transfer to or from a NetView FTP host system, you must know the name of a connection profile that determines the connection to the remote system. This profile must be defined in the SNA setup of the NetView FTP Server AIX to which your client is attached.

You do not need APPC Conversation Security parameters (SECAPPC) for transfers to and from host systems.

Example 3: Sending a File from Your Workstation to a NetView FTP Host System

You send a copy of the file TXT2ESDS from the RDF directory to a host location. the NetView FTP sample directory /usr/lpp/nftp/samples/rdf to an MVS system. The receiving file is an entry-sequenced VSAM data set (VSAM ESDS). This VSAM ESDS file can already exist. If you do not change the RSTATOPT statement in the RDF and the file does not exist already at the remote system, you create a new VSAM ESDS file. If you want to work with an already existing file, contact a person at the remote location for a file name you can use in this transfer.

After the file transfer, a report is to be sent to a user at the host system. You have to know a user ID to which the report can be sent.

Edit the file TXT2ESDS and modify the following statements:

- For the statement with the keyword RMTNODE, replace cpname with the correct connection-profile name.
- For the statement with the keyword RSECURP, replace mvsuser and mvsgroup by access security parameters that are valid at the MVS system. If the access-security parameters are not required, delete the statement.
- For the statement with the keyword RNOTIFY, replace mvsuser by the user ID of the person at the receiving MVS system who is to be notified about the file transfer, and mvssys by the node ID of the receiving MVS system.
• For the statement with the keyword RFILEID, replace either qualifier only or the entire file name, depending on the name of the VSAM ESDS file at the MVS system. Ask the person who created the file for the correct name.

• For the statement with the keyword RVOLSER, replace volser with the volume serial number of the direct access storage device on which the newly created VSAM ESDS is to reside at the remote MVS system.

Enter the `nftp send` command:

```
nftp send /r:TXT2ESDS
```

If the access-security parameters were included in the RDF, you are now prompted for the access-security password. Enter the password. It is not displayed. Remember to type the password in capital letters.

If you set the operation mode of NetView FTP to `attended`, the file-transfer messages are displayed. If the operation mode of NetView FTP is `unattended`, check the file `report.dat` for a report of the file transfer.

Check the host system for the receiving file.
Invoke the NetView FTP Send window with the `nftpguis` command. The NetView File Transfer - Send window is displayed (see Figure 10).

![NetView File Transfer - Send Window](image)

*Figure 10. Example 3: NetView File Transfer - Send Window*

Select TXT2ESDS from the list of RDFs. The panel fields show the values you included in the RDF.

You can also edit the RDF by pressing the Edit push button.
Select the Remote... push button to check the information on the Remote Node Information window (see Figure 11).

![Remote Node Information Window](image)

Figure 11. Example 3: Remote Node Information Window

If you leave the password fields unchanged, NetView FTP prompts you for the passwords when the file transfer starts.

Select the Send push button to send the file.

If you set the operation mode of NetView FTP to **attended**, the file-transfer messages are displayed. If the operation mode of NetView FTP is **unattended**, check the report file. Figure 12 on page 58 shows a sample report file for sending to MVS.

Check the host system for the receiving file.
DVGO001I:ğerodot Initialization
DVGO002I:ğerodot Request started for request number 3 on 1994-09-29 at 10:55:13
DVGO003I:ğerodot Parsing request definition file /home/yweber/nftpwork/rdf/TXT2ESDS
DVGO004I:ğerodot The following default value(s) will be assumed:
  DVGO005I: RSTPNT = < CHKPT >
  DVGO006I: SCCSID = < 85 >
  DVGO007I: SEOPOK = < KEEP >
  DVGO008I: SEOF = < YES >
  DVGO009I: SEORCHAR = < LF >
DVGO010I: Transfer Parameters:
  DVGO011I: RMTNODE = < CLIBCIF4 >
  DVGO012I: COMPMODE = < ADAPT >
  DVGO013I: CONVERT = < YES >
  DVGO014I: RETRY = < YES >
  DVGO015I: RNOTIFY = < ( FRS , SDFMVS6 ) >
  DVGO016I: WAIT = < NO >
DVGO017I: Sending File Parameters:
  DVGO018I: SFILEID = < /usr/lpp/nftp/samples/rdf/TXT2ESDS >
  DVGO019I: SFHMODE = < RECORD >
  DVGO020I: SCCSID = < 85 >
  DVGO021I: SEOPOK = < KEEP >
  DVGO022I: SEORCHAR = < LF >
  DVGO023I: SEOF = < YES >
DVGO024I: Receiving File Parameters:
  DVGO025I: RFILEID = < FRS.EXAMPLE.XFERAIX.TXT2ESDS >
  DVGO026I: RFILEORG = < VSAM >
  DVGO027I: RSTATOPT = < MAYEXIST >
  DVGO028I: REOPOK = < KEEP >
  DVGO029I: REOPNO = < KEEP >
  DVGO030I: RVOLSER = < MUSRT3 >
  DVGO031I: RSECURP = < ( FRS , ***pwd*** ) >
  DVGO032I: RRECORD = < NONINDEXED >
DVGO101I:ğerodot Request name = TXT2ESDS
DVGO102I:ğerodot Request originator = auriga
DVGO103I:ğerodot Transfer direction: File will be sent
DVGO104I:ğerodot Locally initiated file transfer started on 1994-09-29 at 10:55:18 for request number 3
DVGO901I:ğerodot Sending file information:
DVGO111I:ğerodot ID of sending program = auriga
DVGO112I:ğerodot Sending file name = /usr/lpp/nftp/samples/rdf/TXT2ESDS
DVGO113I:ğerodot CCSID = 850
DVGO114I:ğerodot Size of file to be sent = 3670 bytes
DVGO115I:ğerodot Now processing file data...
DVGO311I:ğerodot ID of receiving program = KZAESA
DVGO301I:ğerodot Receiving file name = FRS.EXAMPLE.XFERAIX.TXT2ESDS
DVGO401I:ğerodot CCSID = 500
DVGO001I:ğerodot Size of file to be sent = 3670 bytes
DVGO301I:ğerodot Total number of bytes sent = 3670
DVGO301I:ğerodot Transmission time = 1 sec; transmission rate = 3670 bytes/sec
DVGO351I:ğerodot File transfer 3 ended on 1994-09-29 at 10:55:22 with return code 0
DVGO101I:ğerodot المسلمين

Figure 12. Sample File-Transfer Report for Sending a File
**Hints and Tips**

### Character Data Conversion (CONVERT)
- **YES** Convert the file’s character data according to the CCSIDs specified in the parameters xCCSID.
- **NO** Do not convert the file’s character data.

### File Status Option (RSTATOPT)
- **ME** MUSTEXIST—the receiving file must already exist at the receiving system before the file transfer starts. If it does not already exist, the file transfer ends with an error.
- **MAY** MAYEXIST—the receiving file may or may not already exist at the receiving system before the file transfer starts. If it does not already exist, the file is generated. If it does already exist, the contents of the sending file replace the contents of the existing file.
- **MNE** MUSTNOTEXIST—the receiving file must not exist at the receiving system before the file transfer starts. If it does already exist, the file transfer ends with an error.

**Tip:** If the file transfer ends with an allocation error, check the file status option you used.

If a message or the report file indicate that anything went wrong before or during the file transfer, refer to “Trouble Shooting” on page 101.
Chapter 6. Using NetView FTP for OS/2, DOS, and Windows Workstations

Both, NetView FTP Server AIX and NetView FTP Client AIX provide:

- Requester service for sending files to or receiving files from a remote node
- Responder service for accepting file-transfer requests initiated at a remote node.

NetView FTP Server AIX additionally provides SNA gateway services to the SNA network via either the SNA Server/6000 product or the SNA Services/6000 product (NetView FTP server component).

After NetView FTP AIX has been successfully started, you can invoke these services via the command-line interface, the graphical user interface, or the SMIT menu entries for NetView FTP.

This chapter describes how to use the interfaces and menu entries. The NetView FTP commands mentioned in this chapter are described in detail in Appendix A, “Command Reference” on page 89.

Using the Command-Line Interface

Via the command-line interface, you can:

- Start and stop NetView FTP/2
- Send files to other nodes
- Receive files from other nodes.

Starting the System from the Command Line

Before you can start any services of NetView FTP AIX, the NetView FTP AIX system daemon must be active. The NetView FTP AIX system daemon can be started at system startup by including the `nftpd start` command in the `/etc/rc.tcpip` file. Or, it can be started at any time after system startup by the superuser with the `nftpd start` command.

Next, the server component of NetView FTP Server AIX must be started:

- If the `nftpd startsrv` command is included in the `/etc/rc.tcpip` file after the `nftpd start` command, the server component is activated during system startup.
- The superuser issues the `nftpd startsrv` command.

Note: You need superuser authorization to start the NetView FTP system daemon or the NetView FTP server component.

To enable NetView FTP AIX to accept remotely initiated file-transfer requests, you have to start the NetView FTP responder component.

To start a NetView FTP responder component you can:

- Issue the `nftpd startrsp` command
- Include the `nftpd startrsp` command in the file `/etc/rc.tcpip` which is processed during login to the operating system.
You can disable the responder component of NetView FTP with the `nftpd stoprsp` command.

**Note:** You need superuser authorization to start the NetView FTP responder component.

If you do not explicitly stop the responder component, it terminates when you stop NetView FTP AIX.

Then you can start a NetView FTP AIX requester service on your workstation by:

- Issuing the `nftp start` command
- Including the `nftp start` command in the `.profile` file that is processed during login to the operating system.

During startup, NetView FTP AIX is initialized with the settings specified in the initialization file.

You can use NetView FTP AIX as soon as the NetView FTP Server and NetView FTP Client programs have been started successfully.

### Sending Files Using the Command-Line Interface

To send a file, invoke the command-line interface by entering the `nftp send` command at the command prompt.

With the `nftp send` command, you can:

- Use a default RDF
- Specify an RDF that contains all NetView FTP parameters needed for this transfer
- Specify values for one or more of the most important NetView FTP parameters, using defaults for all others
- Specify values for one or more of the most important NetView FTP parameters, overriding the values specified in an RDF.

RDFs are described in “Working with Request Definition Files” on page 69.

The `nftp send` command also starts the NetView FTP Client/2 if it had not been started before.

### Receiving Files Using the Command-Line Interface

When you want to receive a file, invoke the command-line interface by entering the `nftp receive` command at the command prompt.

With the `nftp receive` command, you can:

- Use a default RDF
- Specify an RDF that contains all NetView FTP parameters needed for this transfer
- Specify values for one or more of the most important NetView FTP parameters, using defaults for all others
Specify values for one or more of the most important NetView FTP parameters, overriding the values specified in an RDF.

The `nftp receive` command also starts the NetView FTP Client/2 if it had not been started before.

**Stopping the System from the Command Line**
When you no longer need NetView FTP AIX, stop it as follows:
- The requester services of NetView FTP AIX with the `nftp stop` command
- The responder component of NetView FTP AIX with the `nftpd stoprsp` command
- The server component of NetView FTP Server AIX with the `nftpd stopsrv` command
- The NetView FTP AIX system daemon with the `nftpd stop` command.

If you do not explicitly stop NetView FTP AIX, it is stopped when the operating system is shut down.

*Note:* You need superuser authorization to stop the NetView FTP system daemon, the NetView FTP server component, or the NetView FTP responder component.

**Using the Graphical User Interface**
Via the graphical user interface, you can:
- Work with the root services of NetView FTP if you have root authorization:
  - Start and stop the NetView FTP system daemon
  - Start and stop the NetView FTP server component
  - Start and stop the NetView FTP responder component.
- Work with the user services of NetView FTP:
  - Start and stop the requester services of NetView FTP.
- Check the status of the NetView FTP system
- Send files to other nodes
- Receive files from other nodes.

*Note:* The Motif Window Manager must be started before you can work with the graphical user interface of NetView FTP AIX.

**Working with the NetView FTP Root Services**
If you have superuser authorization, you can work with the NetView FTP root services. These services include:
- Starting and stopping the NetView FTP system daemon
- Starting and stopping the NetView FTP server component
- Starting and stopping the NetView FTP responder component.

Invoke the window for the NetView FTP Root Services (as shown in Figure 13) with the `nftp gui` command.
The status fields show whether a NetView FTP component is active or inactive and how many file transfers are currently running on the system.

You can start or stop each NetView FTP component with the respective Start or Stop push button. Additionally, you can browse the log file of each NetView FTP component by selecting the View Log push button. For the NetView FTP responder component, you can also browse the report file by selecting the View Report push button.

When you select to stop the NetView FTP system daemon while there are still file transfers active, you must confirm that you really want to stop the system. All active file transfers are interrupted.
Checking the NetView FTP System Status

If you do not have superuser authorization, you can display the NetView FTP system status with the NetView FTP Status Panel. This includes the status of the:

- NetView FTP system daemon
- NetView FTP server component
- NetView FTP responder component.

Invoke the window for the NetView FTP Status Panel (as shown in Figure 14) with the `nftpguic` command.

![NetView FTP Status Panel](image)

*Figure 14. NetView FTP Status Panel*

Use the NetView FTP Status Panel to check whether the NetView FTP system daemon, the NetView FTP server component, and the NetView FTP responder component are active, before you start the NetView FTP requester services.

Additionally, you can browse the log and report files of the NetView FTP responder component by selecting the View Log or the View Report push button.
Working with the NetView FTP User Services

To work with the requester services of NetView FTP AIX, you can use the NetView FTP User Services window. Invoke this window (as shown in Figure 15) with the `nftpguid` command.

![NetView FTP User Services window](image)

**Figure 15. NetView FTP User Services**

In this window, you can:

- Check the status of the NetView FTP requester services (Client System)
- Start and stop the client system
- Browse your log and report files
- Invoke the NetView FTP Send window
- Invoke the NetView FTP Receive window.

**Note:** You can start the requester services of NetView FTP only if the NetView FTP system daemon, the NetView FTP server component, and the NetView FTP responder component are active. You can check this via the NetView FTP Status Panel (as described in “Checking the NetView FTP System Status” on page 65).
Sending Files to a Remote Node

When you want to send a file to a remote note, you can invoke the graphical user interface by:

- Entering the `nftpguis` command at the command prompt
- Selecting the Send push button on the NetView FTP User Services window.

The window shown in Figure 16 appears.

![NetView File Transfer - Send](image)

*Figure 16. NetView File Transfer - Send*

In this window, you can select an RDF from a list of private RDFs or of system RDFs. Use the View... push button to browse the selected RDF. Additionally, you can enter names for the sending and the receiving files to override the ones specified in the RDF. Instead of entering a name for the sending file you can also invoke a file list with the File list... push button and select a file from this list.
If you want to change the specifications for the remote node, select the Remote... push button to open the Remote Node Information window (Figure 17).

![Remote Node Information](image)

*Figure 17. Remote Node Information*

In this window, you can select a destination ID and override values for the security parameters and the workstation ID.

Select the Send push button to send the file.

**Receiving Files from a Remote Node**

To receive a file from a remote node, you can invoke the graphical user interface by:

- Entering the `nftpguir` command at the command prompt
- Selecting the Receive push button on the NetView FTP User Services window.
Using the SMIT Menu Entries for NetView FTP

To work with NetView FTP, you can also use NetView FTP menu entries provided by SMIT. Invoke the NetView FTP menu either by selecting **NetView FTP AIX** from the SMIT menu Communications Applications and Services or by invoking SMIT with the option **nftp**.

The NetView FTP menu provides the menu items User Services and Root Services. From the Root Services menu you can select:

- **Start / Stop the NetView FTP System**
- **Start / Stop the Responder Component**
- **Start / Stop the Server Component**.

From the User Services menu you can select:

- **Start / Stop NetView FTP Client**
- **Transfer Files**.

Working with Request Definition Files

The RDF contains file-transfer parameters and their values. You can add or change control statements by editing the file.

The following rules apply when you code NetView FTP AIX control statements:

**Format**

When you change the sample RDFs provided with the product or create your own RDFs, enter the control statements in the format:

```
/SM590000/SM590000──keyword──=──
                                          ───value
                                       ────────/SM590000/SM630000
```

**Sequence**

You can code NetView FTP AIX control statements in any sequence.

**Columns**

NetView FTP AIX control statements need not begin in column one.

**Lines**

Do not code more than one NetView FTP AIX control statement on one line. A plus sign (+) at the end of a line extends a NetView FTP AIX control statement to the following line.

**Comments**

A comment begins with a slash and an asterisk (/*) and ends with an asterisk and a slash (*/).

**Values**

A value sometimes consists of a list of items. These items must be separated by commas, and the value must be enclosed in parentheses.

A value containing nonalphanumeric characters **must** be enclosed within double quotes (").

If you code a NetView FTP AIX control statement incorrectly, NetView FTP AIX rejects the request and issues an error message. In the RDF, you can assign
values to all NetView FTP file-transfer parameters, but there are a few parameters that can also be given values via the interfaces.

These parameters are:

- File ID for the sending file
- File ID for the receiving file
- Destination ID
- Workstation ID
- File access security.

Parameter values you assign via the interface override those specified in the RDF.

If you do not assign a value to a NetView FTP file-transfer parameter and a default value is available for this parameter, NetView FTP AIX uses this value. For more information on the NetView FTP parameters and their values, refer to the NetView FTP Parameter Reference.

If you do not specify an RDF when setting up a file-transfer request, the default RDF is used. Sample RDFs are provided with the product (see also Appendix C, “Sample Request Definition Files” on page 107).
Chapter 7. Learning More about NetView FTP for OS/2, DOS, and Windows Workstations

This chapter contains more information about NetView FTP AIX. It describes:

- How NetView FTP AIX handles files
- Logging and reporting
- Data compression
- Character data conversion
- Error recovery
- Security
- Transferring files on networks.

All parameters referenced in this chapter are described in detail in the NetView FTP Parameter Reference.

How NetView FTP for OS/2, DOS, and Windows Workstations Handles Files

This section describes the file systems and types that NetView FTP AIX supports and the different file handling modes NetView FTP AIX offers. It also explains how NetView FTP AIX allocates files and the file attributes it supports.

Supported File Types on Workstations

NetView FTP AIX can transfer regular files as well as directories and special files.

Supported File Types on Hosts

NetView FTP AIX can transfer workstation files to or from the following types of files at an MVS system:

- VSAM ESDS
- VSAM KSDS
- VSAM LDS
- Physical sequential stored on DASD
- Physical sequential stored on labeled tape
- Physical sequential stored on unlabeled tape
- Single PDS member without directory information.

File-Handling Modes

In AIX a file is regarded as a consecutive stream of bytes, but some application might need another mode for handling a file. To cope with this difference, NetView FTP AIX offers a record-oriented file handling mode and a byte-oriented file handling mode. You select the appropriate mode via the File Handling Mode parameter.
**Record-Oriented File Handling**
A file’s data can be structured into strings of bytes, called *records*. Each record is delimited by a *record delimiter* such as the carriage return/line feed (CRLF) character combination. Typical examples of record-oriented files are REXX command files or program source code.

Some applications, for example, database programs, process files with a record-oriented format but without record delimiters. These are files with records of fixed length. The length of the records is known only to the application that created the file. Therefore, NetView FTP AIX processes these files as if they had a byte-oriented file format.

In record-oriented file handling mode, NetView FTP AIX does not regard the record delimiters as part of a file’s data. Consequently, NetView FTP AIX at the sending node removes the record delimiters from the sending file’s data. However, it sends the data to the transfer program at the receiving node in a way that the boundaries of the records are recognizable. At the receiving node, NetView FTP AIX adds record delimiters to the received records. NetView FTP AIX uses the operating system’s default control characters as record delimiters.

In addition, you can specify for the sending file whether NetView FTP AIX should treat the ASCII *end-of-file character* as a signal for the end of the file. The records up to the end-of-file character are transferred and the end-of-file character is removed from the file’s data. You can also specify whether NetView FTP AIX should append the end-of-file character to the end of the receiving file.

Furthermore, you can tell NetView FTP AIX which record delimiters have been written at the time the sending file was created. These can be the sequences CRLF (carriage return/line feed), CR (carriage return), or LF (line feed). If you do not specify a record delimiter, NetView FTP AIX uses LF as the default.

The Record Delimiter parameter and the End-of-File Option are described in the *NetView FTP Parameter Reference*.

**Byte-Oriented File Handling**
A file can also be unstructured, that is, it is a consecutive stream of bytes. Typical examples of byte-oriented files are binary files like executable program files or various kinds of graphical files (.cgm files and others).

In byte-oriented file handling mode, NetView FTP AIX neither removes record delimiters from the file nor adds them to the file.

**Combinations of File Handling Modes**
For a given file transfer, the file handling mode used by the sending transfer program can be the same as or different from the one used by the receiving transfer program. The following sections describe the valid combinations of file handling modes for NetView FTP AIX and its communication partners.
**File Transfers between NetView FTP AIX and OS/2 Workstations:** Figure 18 illustrates which combinations of file handling modes are valid in transfers between systems where NetView FTP AIX is installed.

In general, in transfers between workstations, NetView FTP AIX handles the sending and the receiving files in byte-oriented mode. Any record delimiters contained in the file remain unchanged. For some scenarios, however, it may be necessary to change the record delimiters when transferring a file. Therefore, NetView FTP AIX can handle both files in record-oriented mode when transferring a file to or from another NetView FTP AIX.

**File Transfers between a Workstation and a Host:** Figure 19 illustrates which combinations of file handling modes are valid in transfers between NetView FTP AIX and a NetView FTP host node.

Refer to the NetView FTP Parameter Reference Appendix C: Relationships between Sending File and Receiving File Attributes.
Allocation and Creation of Files

This section describes how NetView FTP AIX handles the allocation of space, the access to files, and which file names, file status and process options, and file access mode attributes NetView FTP AIX supports.

Space Allocation
Space allocation is not necessary, because NetView FTP AIX creates and enlarges files dynamically. When running at the sending system, NetView FTP AIX determines the size of the sending file and sends this information to the receiving system.

File Access
When NetView FTP AIX reads a file, other programs can read the file as well, but no other program is allowed to write to the file. When NetView FTP AIX writes to a file, no other programs can read from or write to the file. If a file is already in use by another program when NetView FTP AIX is about to process it, NetView FTP AIX regards this as a temporary error. This also applies when only parts of the file have been locked.

File Names
NetView FTP AIX supports file names that conform to the rules of the operating systems and, if applicable, the file system the files are organized in. In a file transfer request, you must specify the sending file name only, the specification of a receiving file name is optional. If you do not specify a receiving file name, the transfer program at the receiving system creates one according to the rules described in the Appendix on file naming conventions in the NetView FTP Parameter Reference.

The following reserved device names cannot be used as proper file or directory names:

stdin stdout stderr

If one of these names is used as either sending or receiving file ID, NetView FTP AIX tries to use that file handle as input or output device. This allows you to use NetView FTP AIX as a filter. If NetView FTP AIX runs in ATTENDED mode, the program writes messages to stdout. So you can use stderr to capture file data (with the Korn shell, the stderr output redirection is done with 2> ).

If you have superuser authorization, you can use special file names such as /dev/lp0. NetView FTP AIX then uses the respective device. For example, RFILEID=/dev/lp0 prints the incoming data on a locally attached printer (if it is configured correctly).

To write to raw devices such as tapes (/dev/rmt0) you can use a post-transfer script that you specify in the RDF (keyword xPTJOBOK).
File Status and Processing Options

The file status and processing options are commonly defined for all members of the NetView FTP family of products. The options for files handled by NetView FTP AIX are:

1. **File Status Option**
   
   With the file status option, you specify whether a file must, must not, or may already exist at the receiving system before the transfer.

2. **File Processing Option**
   
   With the file processing option, you specify whether NetView FTP AIX is to replace a receiving file’s data or to append to it.

3. **End-of-Processing Option**
   
   With the end-of-processing option, you specify whether NetView FTP AIX should keep or delete a file after the transfer. The effect of the end-of-processing option depends on the result of the file transfer.

File Access Mode Attributes

In your request you can specify the file access mode for a new AIX file. Additionally, you can change the currently active file access mode if the receiving file does already exist and the access security user ID in your request identifies the owner of the file. If you do not specify a file access mode for a new AIX file (either with File Access Mode parameter in your file-transfer request or with the UMASK initialization parameter), NetView FTP AIX uses the default access mode of the receiving system. If you specify a file access mode for a non-AIX file, the file transfer fails.

Logging and Reporting

NetView FTP AIX provides several log and report files:

- A user log file and a user report file.
  
  The user log file and the user report file are stored in the `.log` directory of the NetView FTP user environment.

- A responder-component log file and a responder-component report file.

  The responder-component log file and the responder-component report file are stored in the `.log` directory of the NetView FTP system environment.

- A server log file and a server report file.

  The server log file and the server report file are stored in the `.log` directory of the NetView FTP server environment.

- User-interface log files.

  The user-interface log files contain error messages written by the graphical user interface programs. These log files are called `guimsg.dat` and are stored in the `.log` directory of the respective environment.
A NetView FTP AIX system log file.

This log file is available for the system administrator only. It contains messages related to accounting, performance, and exceptional conditions, such as internal program errors or security violations.

The NetView FTP AIX system log file is stored in the ./log directory of the NetView FTP system environment.

NetView FTP AIX records informational and error messages not related to a particular file transfer in the log file. The name of the log file is log.dat.

Informational and error messages related to a particular file transfer are recorded in the report file. The report file contains information about all file transfers that were performed since NetView FTP AIX was started. This includes the sending and receiving file specification, messages about file transfer errors (if applicable), statistical information, and the file-transfer return code. The name of the report file is report.dat.

When NetView FTP AIX is newly started, the contents of the existing log and report files are saved in files called guimsg.old, log.old, and report.old, and the files guimsg.old, log.dat, and report.dat are overridden. Figure 20 on page 77 shows an example of a report collection file.
DVG0045I: NetView FTP for AIX; Version 1.1.0; Maintenance Level < Mon Sep 26 15:27:01 1994 >

DVG0058I: Processing started for request number 1 on 1994-09-29 at 10:50:56

DVG0060I: Parsing request definition file /home/yweber/nftpwork/rdf/default

DVG0093I: The following default value(s) will be assumed:
DVG0094I: CONVERT = < NO >
DVG0094I: RETRY = < YES >
DVG0094I: RSTPNT = < CHKPT >
DVG0094I: WAIT = < NO >
DVG0094I: SEPOK = < KEEP >
DVG0094I: SFHMODE = < STREAM >
DVG0097I: Transfer Parameters:
DVG0094I: RMTNODE = < CLIBCWEG >
DVG0094I: RMTWSTID = < wega >
DVG0094I: COMPMODE = < NONE >
DVG0094I: CONVERT = < NO >
DVG0094I: RETRY = < YES >
DVG0094I: RSTPNT = < CHKPT >
DVG0094I: WAIT = < NO >
DVG0098I: Sending File Parameters:
DVG0094I: SFILEID = < /u/yweber/nftpwork/rdf/default >
DVG0094I: SFHMODE = < STREAM >
DVG0094I: SEPOK = < KEEP >
DVG0099I: Receiving File Parameters:
DVG0094I: RFILEID = < /u/mic/nftpwork/basket/target.dat >
DVG0094I: RSTATOPT = < MAYEXIST >
DVG0094I: RSECURP = < ( mic , ***pwd*** ) >

DVG0100I:*****************************************

DVG0318I: Request name = default
DVG0319I: Request originator = auriga
DVG0321I: Transfer direction: File will be sent
DVG0301I: Locally initiated file transfer started on 1994-09-29 at 10:51:01 for request number 1
DVG0001I:--------
DVG0311I: Sending file information:
DVG0320I: ID of sending program = auriga
DVG0308I: Sending file name = /u/yweber/nftpwork/rdf/default
DVG0001I:--------
DVG0322I: Receiving file information:
DVG0321I: ID of receiving program = wega
DVG0309I: Receiving file name = /u/mic/nftpwork/basket/target.dat
DVG0001I:--------
DVG0322I: Size of file to be sent = 3968 bytes
DVG0308I: Now processing file data...
DVG0311I: Total number of bytes sent = 3968
DVG0310I: Transmission time = 1 sec; transmission rate = 3968 bytes/sec
DVG0358I: File transfer 1 ended on 1994-09-29 at 10:51:02 with return code 0
DVG0100I:*****************************************

Figure 20. Report Collection File of NetView FTP AIX

User Interface Reporting

The user interfaces of NetView FTP AIX issue one of the following:

- A message indicating that the file-transfer request is accepted
- A message indicating that the file-transfer request is rejected
- A message indicating the outcome of the file-transfer request, if the file-transfer request had been accepted and the file transfer was performed synchronously, that is, if you specified WAIT=YES in the request.
Message Format
The format of a message of NetView FTP AIX is \textit{DVGnnna}, where:

- \textit{DVG} identifies NetView FTP AIX.
- \textit{nnnn} is the message number.
- \textit{a} is the action code indicating the message severity as follows:
  - \textit{I} Information only, processing continues.
  - \textit{W} Warning only, processing continues.
  - \textit{E} An error condition has been detected that prevents normal completion of a function. The file transfer is unsuccessful.
  - \textit{T} NetView FTP AIX has been terminated, because an unrecoverable error has occurred.

User Notification
If a file is received by a NetView FTP AIX program and you specified a valid user ID other than \textit{anonymous} in your request, this user is notified about the end of the file transfer and receives a file-transfer report.

Data Compression
To reduce the amount of data needed to transfer a file, you can tell NetView FTP AIX to compress the data just before sending it and to decompress the data just after it has been received. You can select either no compression or \textit{adaptive} compression with the Compression parameter. This parameter is described in detail in the \textit{NetView FTP Parameter Reference}.

Character Data Conversion
NetView FTP AIX supports character data conversion based on the character data representation architecture (CDRA). CDRA is an IBM architecture that defines a set of identifiers, services, supporting resources, and conventions to achieve a consistent representation, processing, and interchange of character data in SAA environments.

To convert character data, it has to be tagged with a coded character set identifier (CCSID) that is defined by the CDRA. A CCSID represents a specific encoding scheme, one or more character sets, and one or more code pages.

NetView FTP AIX can convert character data when the CCSIDs of the sending file and the receiving file are different. You can tell NetView FTP AIX to convert or not to convert character data by specifying the appropriate value for the Character Data Conversion parameter in the file-transfer request. It can be necessary to avoid character data conversion if, for example, the data can be processed as it is or if the data must remain in its original form (for example, backup of a file).

If NetView FTP AIX has to convert character data, it has to “know” how the character data in the sending file is encoded as well as how the character data in the receiving file is to be encoded.
You can supply NetView FTP AIX with this information by specifying a value for the Coded Character Set Identifier parameter in the file-transfer request. If you do not specify a CCSID in the file-transfer request, NetView FTP AIX uses a default CCSID.

The Character Data Conversion parameter and the Coded Character Set Identifier parameter are described in the NetView FTP Parameter Reference.

Character data conversion is supported for the following country groups:

- Latin-1
- Japan
- Korea
- Republic of China
- Greek
- Turkey
- Latin-2
- Cyrillic
- Hebrew.

Within a country group, conversion between all encoding schemes is possible, unless otherwise specified. Between country groups, conversion is done via code page 500. However, the integrity of the data is limited to the set of characters that is common between the CCSID of the sending system, the CCSID of the receiving system, and CCSID 500. In an RDF, you cannot use single byte Katakana of Japanese or DBCS for an AIX file specification.

**Latin-1**

Country group *Latin-1* includes:

- Australia
- Austria
- Belgium
- Brazil
- Canada
- Denmark
- Finland
- France
- Germany
- International Latin-1
- Italy
- Latin America (Spanish)
- Netherlands
- New Zealand
- Norway
- Portugal
- Spain
- Sweden
- Switzerland
- United Kingdom
- USA.
The CCSIDs for this group are shown in Figure 21.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>EBCDIC</td>
<td>USA, Canada, Netherlands, Portugal, Brazil, Australia, New Zealand</td>
</tr>
<tr>
<td>273</td>
<td>EBCDIC</td>
<td>Austria, Germany</td>
</tr>
<tr>
<td>277</td>
<td>EBCDIC</td>
<td>Denmark, Norway</td>
</tr>
<tr>
<td>278</td>
<td>EBCDIC</td>
<td>Finland, Sweden</td>
</tr>
<tr>
<td>280</td>
<td>EBCDIC</td>
<td>Italy</td>
</tr>
<tr>
<td>284</td>
<td>EBCDIC</td>
<td>Spain, Latin America (Spanish)</td>
</tr>
<tr>
<td>285</td>
<td>EBCDIC</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>297</td>
<td>EBCDIC</td>
<td>France</td>
</tr>
<tr>
<td>500</td>
<td>EBCDIC</td>
<td>Belgium, Canada (AS/400), Switzerland, International Latin-1</td>
</tr>
<tr>
<td>850</td>
<td>PC Data</td>
<td>All Latin-1 countries</td>
</tr>
<tr>
<td>819</td>
<td>ISO 8859-1</td>
<td>All Latin-1 countries</td>
</tr>
</tbody>
</table>

**Japan**

The CCSIDs for this group are shown in Figure 22.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>930</td>
<td>EBCDIC</td>
<td>Japan</td>
</tr>
<tr>
<td>939</td>
<td>EBCDIC</td>
<td>Japan</td>
</tr>
<tr>
<td>932</td>
<td>PC Data</td>
<td>Japan</td>
</tr>
<tr>
<td>5050</td>
<td>ISO (IBM-eucJP)</td>
<td>Japan</td>
</tr>
</tbody>
</table>

When you enter an AIX file specification at a host system, code some characters as specified in the following table, so that the characters are represented correctly.

<table>
<thead>
<tr>
<th>AIX character</th>
<th>Host code 930 (Katakana)</th>
<th>Host code 939 (Latin)</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclamation point</td>
<td>vertical bar</td>
<td>vertical bar</td>
</tr>
<tr>
<td>dollar sign</td>
<td>yen sign</td>
<td>dollar sign</td>
</tr>
<tr>
<td>yen sign</td>
<td>backslash</td>
<td>yen sign</td>
</tr>
<tr>
<td>caret</td>
<td>negation sign</td>
<td>negation sign</td>
</tr>
<tr>
<td>overline</td>
<td>Wa (Katakana)</td>
<td>Nn (Katakana)</td>
</tr>
</tbody>
</table>
Korea

The CCSIDs for this group are shown in Figure 23.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>933</td>
<td>EBCDIC</td>
<td>Korea</td>
</tr>
<tr>
<td>934</td>
<td>PC Data</td>
<td>Korea</td>
</tr>
<tr>
<td>970</td>
<td>ISO (IBM-eucKR)</td>
<td>Korea</td>
</tr>
</tbody>
</table>

When you enter an AIX file specification at a host system, code some characters as specified in the following table, so that the characters are represented correctly.

<table>
<thead>
<tr>
<th>AIX character</th>
<th>Host code 933</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclamation point</td>
<td>vertical bar</td>
</tr>
<tr>
<td>caret</td>
<td>negation sign</td>
</tr>
</tbody>
</table>

Republic of China

Country group Republic of China includes Traditional Chinese. The CCSIDs for this group are shown in Figure 24.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>937</td>
<td>EBCDIC</td>
<td>Traditional Chinese</td>
</tr>
<tr>
<td>938</td>
<td>PC Data</td>
<td>Traditional Chinese</td>
</tr>
<tr>
<td>950</td>
<td></td>
<td>Traditional Chinese</td>
</tr>
<tr>
<td>964</td>
<td>ISO (IBM-eucTW)</td>
<td>Traditional Chinese</td>
</tr>
</tbody>
</table>

When you enter an AIX file specification at a host system, code some characters as specified in the following table, so that the characters are represented correctly.

<table>
<thead>
<tr>
<th>AIX character</th>
<th>Host code 937</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclamation point</td>
<td>vertical bar</td>
</tr>
<tr>
<td>caret</td>
<td>negation sign</td>
</tr>
</tbody>
</table>

Greek

The CCSIDs for this group are shown in Figure 25.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>875</td>
<td>EBCDIC</td>
<td>Greek</td>
</tr>
<tr>
<td>869</td>
<td>PC Data</td>
<td>Greek</td>
</tr>
<tr>
<td>813</td>
<td>ISO 8859-7</td>
<td>Greek</td>
</tr>
</tbody>
</table>
Turkey

The CCSIDs for this group are shown in Figure 26.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>1026</td>
<td>EBCDIC</td>
<td>Turkey</td>
</tr>
<tr>
<td>857</td>
<td>PC Data</td>
<td>Turkey</td>
</tr>
<tr>
<td>920</td>
<td>ISO 8859-9</td>
<td>Turkey</td>
</tr>
</tbody>
</table>

Latin-2

Country group Latin-2 includes:
- Czechoslovakia (Czech and Slovak)
- Hungary
- Poland
- Yugoslavia.

The CCSIDs for this group are shown in Figure 27.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>870</td>
<td>EBCDIC</td>
<td>Latin-2 Multilingual</td>
</tr>
<tr>
<td>852</td>
<td>PC Data</td>
<td>Latin-2 Multilingual</td>
</tr>
<tr>
<td>912</td>
<td>ISO 8859-2</td>
<td>Latin-2 Multilingual</td>
</tr>
</tbody>
</table>

Cyrillic

Country group Cyrillic includes:
- Bulgaria
- Yugoslavia
- USSR Trade Development.

The CCSIDs for this group are shown in Figure 28.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>1025</td>
<td>EBCDIC</td>
<td>Cyrillic Multilingual</td>
</tr>
<tr>
<td>855</td>
<td>PC Data</td>
<td>Cyrillic Multilingual</td>
</tr>
<tr>
<td>866</td>
<td>PC Data</td>
<td>Cyrillic Multilingual</td>
</tr>
<tr>
<td>915</td>
<td>ISO 8859-5</td>
<td>Cyrillic Multilingual</td>
</tr>
</tbody>
</table>
Hebrew

The CCSIDs for this group are shown in Figure 29.

<table>
<thead>
<tr>
<th>CCSID</th>
<th>Encoding Scheme</th>
<th>Country/Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>424</td>
<td>EBCDIC</td>
<td>Hebrew</td>
</tr>
<tr>
<td>856</td>
<td>PC Data</td>
<td>Hebrew</td>
</tr>
<tr>
<td>916</td>
<td>ISO 8859-8</td>
<td>Hebrew</td>
</tr>
</tbody>
</table>

Error Recovery

NetView FTP AIX provides several ways of error recovery.

Automatic Allocation Retry

Sometimes, NetView FTP AIX cannot allocate a conversation with a transfer program at a remote location. This can happen if, for example, the responding transfer program has not been started or if it is already at its maximum limit of parallel transfers. When this happens, NetView FTP AIX periodically retries to allocate a conversation until either the allocation is successful or the number of allowed restart attempts is reached.

You can specify the maximum number of restart attempts (see “Retry Attempts” on page 40) and the wait time between the attempts (see “Retry Delay” on page 41) as initialization parameters.

Automatic Transfer Restart

NetView FTP AIX can use automatic transfer restart to recover from temporary errors. This facility enables NetView FTP AIX to recover from the following errors:

- There is a conversation interruption. This can happen when the server at either system terminates abnormally.
- The operator shuts down one or both of the two servers involved in the transfer.
- The pre-transfer user-exit routine on the NetView FTP host system has temporarily rejected the file-transfer request.

The value of the Automatic Transfer Restart parameter determines whether NetView FTP performs an automatic transfer restart in case of a temporary error. See the NetView FTP Parameter Reference for more information about this parameter.

If an error occurs, both the requester and the responder notify the users specified in the file-transfer request about the interruption.

If the request specifies automatic transfer restart, the requesting NetView FTP AIX waits for the time specified by the Retry Delay parameter (see “Retry Delay” on page 41) in the initialization file. When this time has elapsed, NetView FTP AIX retries to process the file-transfer request. The maximum number of retries is determined by the Restart Attempts parameter (see “Retry Attempts” on page 40) in the initialization file.
When the file-transfer request is restarted, a checkpoint record from the checkpoint file is used. The transfer begins at either the recorded checkpoint or the beginning of the sending file depending on the value you specified for the Restart Point parameter. The sending and the receiving transfer programs position their files to match with the checkpoint and resume the file transfer. NetView FTP AIX issues a special message that indicates the restart point.

**Checkpointing**

NetView FTP AIX on the receiving system stores information about the status of a file transfer when it is interrupted due to a temporary error. This is called *exceptional checkpointing*. The status information is called a *checkpoint*.

NetView FTP AIX can restart the file transfer using the previously written checkpoint. In this way, data that has already been stored at the receiving node does not have to be sent again. You can tell NetView FTP AIX to either resume the transfer where it has been interrupted or start again from the beginning of the sending file. You can do this with the Restart Point parameter. The Restart Point parameter is described in the *NetView FTP Parameter Reference*.
Security

When you initiate a file-transfer request, all files that you can access can be transferred.

A responding NetView FTP AIX accesses the files on behalf of the requesting user. The authorization of the responder component is defined by the file access mode that is assigned to the file. However, a responding NetView FTP AIX performs the following security checks before it allocates the file:

1. Verify and authenticate the requesting user
2. Check the file-access authorization.

Verify and Authenticate the Requesting User
The security scope for a responding NetView FTP AIX is defined by the Security Scope initialization parameter. This parameter is described in “Security Scope” on page 41.

If this initialization parameter is set to YES, a complete security check is made. The Access Security parameters in the request must specify an existing user ID and password. If the user ID does not exist on the workstation, the connection is rejected. If the user ID exists, NetView FTP AIX authenticates it by verifying the password that is specified in the Access Security parameter. If a group ID is specified, NetView FTP AIX validates it too.

If the value of the Security Scope parameter is NO, NetView FTP AIX additionally accepts the user ID anonymous and any password entry instead of a real user ID and password.

Check the File-Access Authorization
The file-access authorization depends on the file access mode that is assigned to the file and on the authorization (file creation mask) of the process that accesses the file.

A new file has the file creation mask of the process that created it. However, you can change the file creation mask by setting the File Access Mode parameter in the request.

For a file-transfer with the user ID anonymous, the following applies:

- Files that are to be read by the remote anonymous user must reside in a directory that allows public read access. This directory can be defined in the OUTBASKET initialization parameter. If this variable is not set, NetView FTP AIX searches for the file in the ./public subdirectory of the responder’s system directory.

- Files that are to be written by the remote anonymous user are put into the ./basket subdirectory of the responder’s system directory, unless a different directory was specified with the INBASKET initialization parameter.
Password Handling

Passwords in an RDF are kept on disk in clear-text form. You can omit this by including in the RDF a question mark as a placeholder for a password. In this case, you are prompted for the corresponding password when the file transfer starts.

In main storage, passwords are always kept in encrypted form.

Security for Systems Other than NetView FTP for OS/2, DOS, and Windows Workstations

For the security parameters defined for NetView FTP programs other than NetView FTP AIX, such as the Access Security or the VSAM Cluster Password parameters, you must specify at least a user ID and a password. For the passwords in these parameters, you can also specify a question mark in the RDF, so you will be prompted for the password when the file transfer starts.

Transferring Files on Networks

This section describes the environments where NetView FTP AIX can transfer files.

For file transfers in an SNA network, NetView FTP AIX needs a session using an SNA LU6.2 protocol with its NetView FTP communication partner. This is provided by the NetView FTP Server product. NetView FTP Server AIX uses the services of AIX SNA Services/6000 or AIX SNA Server/6000.

NetView FTP Server AIX and NetView FTP Client AIX communicate via TCP/IP. When the NetView FTP Server and the NetView FTP Client are on the same workstation, AIX STREAM I/O is used for communication.

Integration into NetView/6000

NetView FTP Server AIX provides users with an integrated environment to invoke the graphical user interface of NetView FTP Server AIX from the graphical user interface of NetView/6000. The graphical user interface of NetView FTP can be invoked from the NetView/6000 tools palette or from the NetView/6000 menu bar.

In addition, when sending or receiving files to or from a node shown on a NetView/6000, users can select that node and then select NetView FTP Server AIX from the NetView/6000 tools palette or from the NetView/6000 menu bar. In this case, the Send or Receive window of the NetView FTP graphical user interface is invoked and the selected node is used as workstation ID.
Appendix A. Command Reference

This appendix describes the NetView FTP commands in alphabetical order.

**NFTP PURGE**

```
رانف تيرميانا ـ/نول ـ/نولوگا
```

Use this command to purge all NetView FTP processes when an error occurred from which NetView FTP AIX cannot recover properly. You can use the option /nol or /nologo to suppress the logo display.

**NFTP RECEIVE**

```
رانف تيرميانا ـ/ر:DEFAULT ـ/ر:RDF_name ـ/س:س_FILEID ـ/ت:ر_FILEID ـ
/د:destination_ID ـ/م:workstation_ID ـ
/ع:APPC_user_ID ـ/ر:APPC_password ـ
/س:SAF_user_ID ـ/س:SAF_group_ID ـ/ن:SAF_password ـ/نول ـ/نولوگا
```

Use this command to receive a file.

Together with the nftp receive command, you can specify:

**RDF_name**

The name or the complete file specification of the RDF to be used. If you do not specify an RDF, the default RDF named default is used which is stored in the rdf directory of the system environment.

**s_fileid**

The name of the sending file at the remote system. Enclose the file name in quotes if it contains backslashes (\).

When you assign a value to this parameter via the RDF, specify the name in the RDF keyword SFILEID.

**r_fileid**

The name of the receiving file at your local system. Enclose the file name in quotes if it contains backslashes (\).

When you assign a value to this parameter via the RDF, specify the name in the RDF keyword RFILEID.
**destination ID**

The name of the connection-profile for a specific connection to a remote server. This connection profile must be defined in the SNA setup of the NetView FTP Server AIX to which your client is attached.

When you assign a value to this parameter via the RDF, specify the connection-profile name in the RDF keyword **RMTLU**.

**workstation ID**

The identification of the remote workstation to or from which the file is transferred using TCP/IP protocols. It can be the:

- **workstation address**
  
The decimal representation of the Internet address of the communication partner. It includes both a network ID and a host ID.

- **workstation nickname**
  
The nickname for the communication partner.

When you assign a value to this parameter via the RDF, specify the workstation ID in the RDF keyword **RMTWSTID**.

**APPC_user ID**

APPC conversation security parameter.

When you assign a value to this parameter via the RDF, specify the user ID with the RDF keyword **SECAPPC**.

**Note:** In the RDF, the APPC user ID and password are assigned to one keyword.

**APPC_password | ?**

APPC conversation security parameter.

When you assign a value to this parameter via the RDF, specify the password in the RDF keyword **SECAPPC**.

**Note:** In the RDF, the APPC user ID and password are assigned to one keyword.

**SAF_user ID**

An access-security parameter that might be required by the remote sending transfer partner. If you specify a user ID, you must also specify a password, in capital letters.

When you assign a value to this parameter via the RDF, specify the user ID in the RDF keyword **SSECURP**.

**Note:** In the RDF, the SAF user ID, group ID, and password are assigned to one keyword.

**SAF_group ID**

An access-security parameter that might be required by the remote sending transfer partner.

When you assign a value to this parameter via the RDF, specify the group ID in the RDF keyword **SSECURP**.

**Note:** In the RDF, the SAF user ID, group ID, and password are assigned to one keyword.
**SAF_password** | ?

An access-security parameter that might be required by the remote sending transfer partner. If you specify a user ID, you must also specify a password.

When you assign a value to this parameter via the RDF, specify the password in the RDF keyword SSECURP.

**Note:** In the RDF, the SAF user ID, group ID, and password are assigned to one keyword.

/nol | /nologo

The option to suppress the logo display.

---

**NFTP SEND**

Use this command to send a file.

Together with the `nftp send` command, you can specify:

**RDF_name**

The name or the complete file specification of the RDF to be used. If you do not specify an RDF, the default RDF named `default` is used which is stored in the `rdf` directory of the system environment.

**s_fileid**

The name of the sending file at your local workstation. Enclose the file name in quotes if it contains backslashes (`\`).

When you assign a value to this parameter via the RDF, specify the name in the RDF keyword `SFILEID`.

**r_fileid**

The name of the receiving file at the remote system. Enclose the file name in quotes if it contains backslashes (`\`).

When you assign a value to this parameter via the RDF, specify the name in the RDF keyword `RFILEID`.

**destination_ID**

The name of the connection profile for a specific connection to a remote server. This connection profile must be defined in the SNA setup of the NetView FTP Server AIX to which your client is attached.

When you assign a value to this parameter via the RDF, specify the connection-profile name in the RDF keyword `RMTLU`. 
**workstation_ID**

The identification of the remote workstation to or from which the file is transferred using TCP/IP protocols. It can be the:

**workstation address**

The decimal representation of the Internet address of the communication partner. It includes both a network ID and a host ID.

**workstation nickname**

The nickname for the communication partner.

When you assign a value to this parameter via the RDF, specify the workstation ID in the RDF keyword `RMTWSTID`.

**APPC_user_ID**

APPC conversation security parameter.

When you assign a value to this parameter via the RDF, specify the user ID in the RDF keyword `SECAPPC`.

**Note:** In the RDF, the APPC user ID and password are assigned to one keyword.

**APPC_password | ?**

APPC conversation security parameter.

When you assign a value to this parameter via the RDF, specify the password in the RDF keyword `SECAPPC`.

**Note:** In the RDF, the APPC user ID and password are assigned to one keyword.

**SAF_user_ID**

An access-security parameter that might be required by the remote receiving transfer partner. If you specify a user ID, you must also specify a password, in capital letters.

When you assign a value to this parameter via the RDF, specify the user ID in the RDF keyword `RSECURP`.

**Note:** In the RDF, the SAF user ID, group ID, and password are assigned to one keyword.

**SAF_group_ID**

An access-security parameter that might be required by the remote receiving transfer partner.

When you assign a value to this parameter via the RDF, specify the group ID in the RDF keyword `RSECURP`.

**Note:** In the RDF, the SAF user ID, group ID, and password are assigned to one keyword.
SAF_password /?

An access-security parameter that might be required by the remote receiving transfer partner. If you specify a user ID, you must also specify a password.

When you assign a value to this parameter via the RDF, specify the password in the RDF keyword RSECURP.

Note: In the RDF, the SAF user ID, group ID, and password are assigned to one keyword.

/nol | /nologo

The option to suppress the logo display.

---

NFTP START

Use this command to start the requester services of NetView FTP AIX

Together with the nftp start command, you can specify:

ini_file

The name or the complete file specification of the file containing the initialization parameters to be used. The default initialization file is ibmnftp.ini which is stored in the ini directory of the respective environment.

/nol | /nologo

The option to suppress the logo display.

---

NFTP STOP

Use this command to stop the requester services of NetView FTP AIX where /nol or /nologo is the option to suppress the logo display.
NFTPD PURGE

Use this command to purge all NetView FTP AIX system processes when an error occurred from which NetView FTP AIX cannot recover properly. You can use the option /nol or /nologo to suppress the logo display.

Note: You can use this command only with superuser authorization.

NFTPD START

Use this command to start the NetView FTP AIX system daemon on your workstation. This is necessary to enable the system for NetView FTP.

You can use the option /nol or /nologo to suppress the logo display.

Note: You can use this command only with superuser authorization.

NFTPD STARTRSP

Use this command to start a responder component at an AIX workstation.

Together with the nftpd startrsp command, you can specify:

*ini_file*

The name or the complete file specification of the file containing the initialization parameters to be used. The default initialization file is ibmftp.ini which is stored in the *ini* directory of the NetView FTP system.

/nol | /nologo

The option to suppress the logo display.

Note: You can use this command only with superuser authorization.
NFTPD STARTSRV

Use this command to start the SNA gateway services of a NetView FTP Server AIX.

Together with the **nftpd startsrv** command, you can specify:

- **ini_file**
  The name or the complete file specification of the file containing the initialization parameters to be used. The default initialization file is `ibmnftp.ini` which is stored in the **ini** directory of the server component environment.

- **/nol | /nologo**
  The option to suppress the logo display.

**Notes:**
1. The NetView FTP AIX system daemon must be active before you issue this command.
2. You can use this command only with superuser authorization.

NFTPD STOP

Use this command to stop the NetView FTP AIX system daemon using the command-line interface.

Together with the **nftpd stop** command, you can specify:

- **/f | /force**
  The option to force a stop of the system daemon even if file transfers are active.

- **/nol | /nologo**
  The option to suppress the logo display.

**Notes:**
1. Before issuing this command you must stop any responder component and the server component.
2. You can use this command only with superuser authorization.
NFTPD STOPRSP

Use this command to stop a responder component at an AIX workstation, where /nol or /nologo is the option to suppress the logo display.

Note: You can use this command only with superuser authorization.

NFTPD STOPSRV

Use this command to stop the SNA gateway services of a NetView FTP Server AIX, where /nol or /nologo is the option to suppress the logo display.

Note: You can use this command only with superuser authorization.

NFTPGUIC

Use this command to invoke:

- The NetView FTP Root Services, if you have superuser authorization
- The NetView FTP Status Panel, if you do not have superuser authorization.

NFTPGUID

Use this command to invoke the NetView FTP requester services.
Use this command to receive a file using the graphical user interface, where:

**workstation ID**

The identification of the remote workstation to or from which the file is transferred using TCP/IP protocols. It can be the:

- **workstation address**
  The decimal representation of the Internet address of the communication partner. It includes both a network ID and a host ID.

- **workstation nickname**
  The nickname for the communication partner.

When you assign a value to this parameter via the RDF, specify the workstation ID in the RDF keyword `RMTWSTID`.

Use this command to send a file using the graphical user interface, where:

**workstation ID**

The identification of the remote workstation to or from which the file is transferred using TCP/IP protocols. It can be the:

- **workstation address**
  The decimal representation of the Internet address of the communication partner. It includes both a network ID and a host ID.

- **workstation nickname**
  The nickname for the communication partner.

When you assign a value to this parameter via the RDF, specify the workstation ID in the RDF keyword `RMTWSTID`.
Appendix B. Diagnosing

This appendix lists the return codes of NetView FTP AIX and gives some information on trouble shooting. It also contains forms for problem reporting.

NetView FTP for OS/2, DOS, and Windows Workstations Interface
Return Codes

When any of the NetView FTP commands is invoked from a shell script, the following return codes can be used for further processing:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Function successfully completed.</td>
</tr>
<tr>
<td>100</td>
<td>File transfer scheduled.</td>
</tr>
<tr>
<td>110</td>
<td>An internal logic error occurred.</td>
</tr>
<tr>
<td>120</td>
<td>Incorrect invocation of NetView FTP.</td>
</tr>
<tr>
<td>200</td>
<td>The NetView FTP system is already started.</td>
</tr>
<tr>
<td>210</td>
<td>Errors were found in the request definition file.</td>
</tr>
<tr>
<td>220</td>
<td>Errors were found in the initialization parameter file.</td>
</tr>
<tr>
<td>230</td>
<td>The NetView FTP system is not active.</td>
</tr>
<tr>
<td>240</td>
<td>The NetView FTP Server cannot accept your request.</td>
</tr>
<tr>
<td>250</td>
<td>A STOP command is already in progress.</td>
</tr>
<tr>
<td>260</td>
<td>The NetView FTP system is terminating.</td>
</tr>
<tr>
<td>270</td>
<td>A responder is already active in this NetView FTP environment.</td>
</tr>
<tr>
<td>280</td>
<td>No responder is active in this NetView FTP environment.</td>
</tr>
<tr>
<td>290</td>
<td>The NetView FTP level of this workstation and that of the server do not match.</td>
</tr>
<tr>
<td>300</td>
<td>The NetView FTP AIX system is not active.</td>
</tr>
<tr>
<td>310</td>
<td>The NetView FTP AIX system is already active.</td>
</tr>
<tr>
<td>320</td>
<td>The NetView FTP AIX responder is not active.</td>
</tr>
<tr>
<td>330</td>
<td>The NetView FTP AIX responder is already active.</td>
</tr>
<tr>
<td>340</td>
<td>The NetView FTP AIX responder is active.</td>
</tr>
<tr>
<td>400</td>
<td>An internal processing error occurred.</td>
</tr>
<tr>
<td>410</td>
<td>An internal memory shortage occurred.</td>
</tr>
<tr>
<td>420</td>
<td>A communication error occurred.</td>
</tr>
<tr>
<td>430</td>
<td>An internal NetView FTP subprocess could not be started.</td>
</tr>
<tr>
<td>440</td>
<td>Transfer could not be accepted because session limit was exceeded.</td>
</tr>
<tr>
<td>450</td>
<td>Checkpoint file could not be initialized.</td>
</tr>
<tr>
<td>460</td>
<td>Processing was interrupted by a cancel command.</td>
</tr>
</tbody>
</table>
## NetView FTP for OS/2, DOS, and Windows Workstations File-Transfer Return Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>File transfer successful.</td>
</tr>
<tr>
<td>4</td>
<td>File transfer successful - noncritical error occurred (for example, Warning: Checkpointing not available).</td>
</tr>
<tr>
<td>8</td>
<td>File transfer completed successful - error occurred during termination processing (for example, post-transfer job in MVS not found).</td>
</tr>
<tr>
<td>10</td>
<td>File transfer failed, but will be retried (temporary error).</td>
</tr>
<tr>
<td>12</td>
<td>File transfer failed during data handling.</td>
</tr>
<tr>
<td>16</td>
<td>File transfer failed during initialization of the file transfer (for example, sending file not found).</td>
</tr>
</tbody>
</table>
### Trouble Shooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>The file transfer ends with return code 16 and these messages are issued:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVG0201E: APPC error: ALLOCATE primary RC: 0x0003(ALLOCATION_ERROR),</td>
<td></td>
</tr>
<tr>
<td>secondary RC: 0x00000004(ALLOCATION_FAILURE_NO_RETRY)</td>
<td></td>
</tr>
<tr>
<td>DVG0202E: APPC allocation failure sense data: 0x80040000</td>
<td></td>
</tr>
<tr>
<td>DVG0207E: APPC allocation to partner &lt; SDFPCHFF &gt; with mode name &lt; FTPBIND1 &gt; failed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probable cause</th>
<th>The remote LU is not active.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What you can do</th>
<th>Either have the remote LU activated or select an LU that is active.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>The requesting NetView FTP Client is unable to connect to the adjacent NetView FTP Server and the following messages are issued to the user's log file:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVG0030E: TCP/IP function connect returned 79; reason: Connection refused</td>
<td></td>
</tr>
<tr>
<td>DVG0024E: NetView FTP Server is not active</td>
<td></td>
</tr>
<tr>
<td>DVG0025E: An error occurred during START command processing</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probable cause</th>
<th>The port number specified in the initialization file does not match the port number specification in the initialization file of the adjacent NetView FTP Server or one of the two initialization files does not contain a port number specification.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What you can do</th>
<th>Ask the system administrator for the workstation running NetView FTP Server AIX whether a port number is specified in the initialization file for the server component. If yes, verify that you also have specified this parameter and that the statement contains the same port number. Otherwise, remove this statement from your initialization file. Then, both the NetView FTP Server and the NetView FTP Client use the same default for the port number.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Problem</th>
<th>The requesting NetView FTP Client receives the following messages:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVG0324I: File transfer error occurred at the NetView FTP Server node:</td>
<td></td>
</tr>
<tr>
<td>DVG0203E: An APPC error occurred; for more information see NetView FTP Server log file</td>
<td></td>
</tr>
</tbody>
</table>

The log file of your adjacent NetView FTP Server contains the following messages:

| DVG0201E: APPC error: snaread error RC: 0x007F (TPN not recognized) |

<table>
<thead>
<tr>
<th>Probable cause</th>
<th>The NetView FTP Server as addressed in the RMTNODE statement is not available or the connection-profile name does not reflect the desired connection or the connection is not active. If the connection is not active, the connection-profile name may not be specified in the server group table of your adjacent NetView FTP Server. If the remote system is controlled by a NetView FTP Server AIX, the same can be true for this location.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>What you can do</th>
<th>If the connection profile specified in the RMTNODE statement is correct, contact your system administrator.</th>
</tr>
</thead>
</table>
Problem

The requesting MVS user receives file-transfer return code 16 with reason code 16: APPC Error.

The log file of the NetView FTP V2.2 MVS server that obtained the file-transfer request contains the following message:

DVG065I ACF/VTAM APPCCMD MACRO ERROR; OPERAND CODE = SENDCONF; RETURN CODE IN RPL = 00; FEEDBACK FIELD in RPL = 0B; SENSE CODE IN RPL6 = 10086021; APPC PRIMARY RETURN CODE = 004 APPC SECONDARY RETURN CODE = 0008

Probable cause

The responding NetView FTP Server is not active or the NetView FTP V2.2 MVS server was active before the connection of the NetView FTP Server AIX was active. Note that for connections to MVS SNA Services/6000 needs to have a connection profile of type caller. If the NetView FTP V2.2 MVS server was not active at the time the connection profile was started, SNA Services/6000 was unable to establish the connection and responds to any connection attempt with a CNOS or SENDCONF error.

What you can do

For connections other than between two AIX workstations, the connection profiles must be of type caller. For a connection between two AIX workstations, one must be defined as listener and the other as caller. There must be an agreement between all potential communication partners which system is to be started first to allow others to call it.

Problem

The requesting NetView FTP Client receives file-transfer return code 16 and the following messages are issued:

DVG0150E: Error message received from remote file transfer program: DVG153I ERROR DURING VALIDATION OF USER uid ; RACROUTE RETURN CODE = 08; RACROUTE RETURN CODE = 08; RACROUTE REASON CODE = 00

Probable cause

Depending on the transfer direction you may have specified the sending or receiving access-security parameters for the remote system incorrectly. Note that these parameters have to be specified exactly as defined on the system; /370 systems use uppercase per default.

What you can do

Specify the access-security parameters in uppercase characters and rerun the file transfer request.

Problem

The requesting NetView FTP Client receives file-transfer return code 16 and the following messages are issued:

DVG0150E: Error message received from remote file transfer program: DVG182I DYNAMIC ALLOCATION ERROR; ERROR TYPE = P; DATA SET NAME = abc.def; RETURN CODE = 12; INFORMATION REASON CODE = 0002; ERROR REASON CODE = 035C

Probable cause

Depending on the transfer direction you may have specified the sending or receiving file ID for the remote system incorrectly. For transfers to or from /370 systems note that file IDs are usually defined in uppercase.

What you can do

Specify the file ID for the remote system in uppercase characters and rerun the file transfer request.
Problem

The requesting NetView FTP Client issues the following messages:

DVG0150E: Error message received from remote file transfer program:

DVG153I ERROR DURING VALIDATION OF USER xyz; RACROUTE RETURN CODE = 08;
RACROUTE RETURN CODE = 08;
RACROUTE REASON CODE = 00

Probable cause

You did not know which operating system runs on the remote workstation and specified the APPC security parameters though they were not required. If the responding NetView FTP Client runs under OS/2, the APPC security parameters are required for security reasons while they must not be specified if the operating system is AIX.

What you can do

Ask the user at the remote workstation for the operating system. Correct the RDF specification and rerun the file-transfer request.

Problem

The requesting NetView FTP Client receives the following messages:

DVG0324I: File Transfer error occurred at the NetView FTP Server node:

DVG0203E: An APPC error occurred; for more information see NetView FTP Server log file

The log file of your adjacent NetView FTP Server contains the following message:

DVG0201E: APPC error: snalloc error RC: 0x0070
(resource failure no_retry)

Probable cause

One of the following:

- The NetView FTP Server as addressed by the RMTNODE statement has been stopped while the appropriate attachment and connection on both locations were still active.
- If the partner transaction program is NetView FTP V2.2 MVS, the LU represented by the NetView FTP MVS server is not started.

What you can do

Contact the system administrator at the remote location.

Problem

The requesting NetView FTP Client receives the following messages:

DVG0324I: File Transfer error occurred at the NetView FTP Server node:

DVG0214E: Remote NetView FTP transaction program is temporarily not available; maybe no remote request handler is started at the remote MVS node

Probable cause

The NetView FTP Server as addressed by the RMTNODE statement may have been stopped while the appropriate attachment and connection on both locations were still active. If the connection addresses an MVS node, the following can be true: The LU represented by the NetView FTP MVS server is active but can currently not accept another session. The reason for this can be one of the following:

- The maximum number of sessions permitted for remotely initiated sessions is already in use.
- No remote request handler is started on that server.

What you can do

Contact the system administrator at the remote location.
Reporting a Problem

When an error occurred that you could not resolve using the information from “Trouble Shooting” on page 101, fill in the problem report form and contact the IBM service organization for your country.

Information You Need to Report a Problem

When reporting a problem, have the following information ready:

- A complete description of the scenario in which the problem occurred.
- Both the report files of the requesting and the responding system. If the responding system was NetView FTP AIX, a report file is available either from the user to which a report file was sent or it has to be extracted from the common report file of the responder component.
- Switch on the trace in the initialization files at the requesting and the responding system and provide:
  - At the requesting system:
    - The private user log and the log of the server component
    - The private initialization file and the initialization file of the server component.
  - At the responding system:
    - The logs of the server component and the responder component
    - The initialization files of the server component and the responder component.
- If the error relates to a connectivity problem:
  - The appropriate SNA Services/6000 specifications exported to a file.
  - The contents of the server group table on both the requesting and the responding system.
- A complete description of all attempts you made to fix the problem.
- An indication of how often the problem occurs and any other processing patterns related to the problem. For example, does it occur for all objects or only for objects with certain data?

Note: Save the report and log files as soon as the problem has occurred.

If you cannot identify the source of the problem, your service representative might ask you to provide additional information, which could include:

- A record of the contents of your database at the time of the error
- Any customized source code related to the problem
- Diagnostic data from prerequisite or other products installed on your system.

The more information you provide, the faster a problem can be solved. Gather any related information you think might help to identify and solve the problem.
Reporting Problems and Submitting Requirements

Report defects found in the NetView FTP Server AIX and the NetView FTP Client AIX licensed programs to IBM via an Authorized Program Analysis Report (APAR), form number G150-180, or via APAR/SYS, an electronic direct problem reporting system.

Several items should be submitted with each problem:

- The APAR form
- The problem determination form
- Any supporting data as discussed in “Information You Need to Report a Problem” on page 104.

Your IBM representative can assist you in the appropriate procedure.

**Note:** Write the APAR, PASR, or PMR number on all forms, media, or supporting materials sent to development.
Problem Report Form

To help determine the cause of a problem, provide the following information along with your APAR.

1. How much RAM was in your workstation?
2. Which product are you using on your workstation? (NetView FTP Server AIX or NetView FTP Client AIX)
3. What release of the product were you using?
4. Are you using RLM or node-lock licensing?
5. What release and PTF level of AIX/6000 were you using?
6. What release and PTF level of SNA Services/6000 or SNA Server/6000 were you using?
7. What is the operating system to or from which you want to transfer files?
8. What is the NetView FTP product release and PTF level of the system to or from which you want to transfer files?
9. Did an abnormal ending (core dump) occur?
10. What is the IBM RISC System/6000 model number of your workstation?
11. How much file space was left in the file system being written to?
12. Describe the exact sequence of commands that caused the problem.

13. Describe any messages that accompanied the problem.

14. Expected Results:

15. Actual Results:

16. If a message was inaccurate, give the message and reason:
   Message:
   Reason:

17. If a function did not work as the document described:
   Function:
   Document:
   Document Number:
   Page:
   Problem:
Appendix C. Sample Request Definition Files

An RDF is an ASCII file that contains values for file-transfer parameters. You enter the control statements in the format keyword=value.

The samples in this appendix are the RDFs used in the file-transfer examples in Chapter 5, “Getting Started” on page 45. The ASCII files of these and other RDFs are provided on the product diskettes. You can modify them according to your needs by changing the corresponding control statements. You can also use the sample RDFs as a basis for developing your own RDFs.

For a complete description of the parameters and their values, refer to the NetView FTP Parameter Reference.
Sample RDF : Send a binary file to another AIX workstation

NetView FTP for Workstations assumes default values for parameters to which you did not assign a value.

Change the following to fit your environment:

/usr/lpp/nftp/samples - to the NetView FTP/AIX product directory
cpname - to the connection profile name as defined in your SNA
wstid - to the remote workstation's IP address or name
ruserid - to the user ID at the remote workstation to which the file is sent.
( You will be prompted to enter the responder's password. )

User command values

RMTNODE = cpname The connection profile name which describes the connection between the NFTP Server/AIX which serves your requesting NFTP Client/AIX and the NFTP Server/AIX which serves the responding NFTP Client/AIX.
RMTWSTID = wstid The ID of the remote workstation where the user resides. It is the absolute ID as registered in the IP network or the host name as known to the AIX name server.
RSECURP = ( ruserid , ? ) User ID and password at the remote workstation. You are prompted for the password.
SFHMODE = STREAM Sending file is byte-oriented
RFHMODE = STREAM Receiving file is byte-oriented
RSTATOPT = MAYEXIST Receiving file may or may not exist
RPROCOPT = REPLACE Replace contents of the receiving file if it already exists
RCHMOD = 755 Make it executable
Bin2BinX

/* Sample RDF : Receive a binary file from another AIX workstation */
/* NetView FTP for Workstations assumes default values for parameters */
/* to which you did not assign a value. */
/* Change the following to fit your environment: */
/* cpname - to the connection profile name as defined in your SNA */
/* wstid - to the remote workstation's IP address or name */
/* suserid - to the user ID at the remote workstation from which the */
/* file is received. */
/* ( You will be prompted to enter the responder's password. ) */
/* /spath - to the directory path where the file is to be sent from */
/* /rpath - to the directory path where the file is to be received to */

>User command values

RMTNODE = cpname /* The connection profile name which */
/* describes the connection between */
/* the NFTP Server/AIX which serves */
/* your requesting NFTP Client/AIX and */
/* the NFTP Server/AIX which serves */
/* the responding NFTP Client/AIX. */

RMTWSTID = wstid /* The ID of the remote workstation */
/* where the user resides. It is the */
/* absolute ID as registered in the */
/* IP network or the host name as */
/* known to the AIX name server. */

SSECURP = ( suserid, ? ) /* User ID and password at the remote */
/* workstation. */
/* You are prompted for the password */

SFILEID = /spath/NFTPTEST.EXE /* test file */
RFILEID = /rpath/BIN2BINX.NFTPTEST.EXE

>Transfer Parameters

COMPMODE = NONE /* Do not compress data */
RETRY = YES /* Automatic retry if file transfer is */
/* interrupted */
WAIT = YES /* Wait for file transfer to complete */

>File Handling Characteristics

SFHMODE = STREAM /* Sending file is byte-oriented */
RFHMODE = STREAM /* Receiving file is byte-oriented */
RSTATOPT = MAYEXIST /* Receiving file may or may not exist */
RPROCOPT = REPLACE /* Replace contents of the receiving */
/* file if it already exists */
RCHMOD = 755 /* Allow execution */
Sample RDF: Send a text file from AIX to a VSAM ESDS file on MVS

NetView FTP for Workstations assumes default values for parameters to which you did not assign a value.

Change the following to fit your environment:

- /usr/lpp/nftp/samples - to the NetView FTP/AIX product directory
- cpname - to the connection profile name as defined in your SNA Services/6000 environment for the remote NetView FTP server
- qualifier - to the first level qualifier to use on the MVS system
- mvsuser - to the user ID of the user on MVS
- mvsgroup - to the group ID of the user on MVS
- mvssys - to the JES node ID of the MVS system
- volser - volume serial number

User command values

RMTNODE = cpname

SFFILEID = /usr/lpp/nftp/samples/rdf/TXT2ESDS
RFILEID = qualifier.EXAMPLE.XFERAIX.TXT2ESDS

Transfer Parameters

CONVERT = YES
COMPMODE = ADAPT
RETRY = YES
WAIT = YES
RSECURP = (mvsuser,?,mvsgroup)
RNOTIFY = (mvsuser, mvssys)

File Handling Characteristics

SFHMODE = RECORD
REOPOK = KEEP
REOPNO = KEEP
RSTATOPT = MUSTEXIST
RVOLSER = volser
RFILEORG = VSAM
RRECORPB = NONINDEXED
Appendix D. Sample Profiles for APPC Configuration

This appendix contains sample profiles for the APPC configuration required for NetView FTP Server AIX.

SNA Server/6000

SNA Node Profile

prof_name = "sna"
max_sessions = 200
max_conversations = 200
restart_action = once
rrm_enabled = no
dynamic_inbound_partner_lu_definitions_allowed = yes
standard_output_device = "/dev/console"
standard_error_device = "/var/sna/sna.stderr"
nmvt_action_when_no_nmvt_process = reject
comments = "Standard SNA NodeProfile"

SNA Control Point Profile

prof_name = "node_cp"
xid_node_id = 0x071ffcc4
network_name = "DEABCYZ"
control_pt_name_alias = "AURIGA"
control_pt_name = "YZF8040A"
control_pt_node_type = appn_network_node
max_cached_trees = 500
max_nodes_in_topology_database = 500
route_addition_resistance = 128
comments = "AURIGA"
SNA Data Link Control Profile

```
prof_name = "trdlc"
datalink_device_name = "tok0"
force_timeout = 120
user_defined_max_i_field = yes
max_i_field_length = 30729
max_active_link_stations = 100
num_reserved_inbound_activation = 0
num_reserved_outbound_activation = 0
transmit_window_count = 16
dynamic_window_increment = 1
retransmit_count = 8
receive_window_count = 8
priority = 0
inact_timeout = 48
response_timeout = 4
acknowledgement_timeout = 1
link_name = 
local_sap = 0x04
retry_interval = 60
retry_limit = 20
dynamic_link_station_supported = no
trace_base_listen_link_station = no
trace_base_listen_link_station_format = long
dynamic_link_solicit_sscp_sessions = yes
dynamic_link_cp_cp_sessions_supported = yes
dynamic_link_cp_cp_session_support_required = no
dynamic_link_TG_effective_capacity = 4300800
dynamic_link_TG_connect_cost_per_time = 0
dynamic_link_TG_cost_per_byte = 0
dynamic_link_TG_security = nonsecure
dynamic_link_TG_propagation_delay = lan
dynamic_link_TG_user_defined_1 = 128
dynamic_link_TG_user_defined_2 = 128
dynamic_link_TG_user_defined_3 = 128
comments = "Std. TR SNA DLC Profile"
```
SNA LU6.2 TPN Profile

prof_name = "dvgftpb1"

tp_name = "DVGDUMMY"

tp_name_in_hex = no

pip_data_present = yes

pip_data_subfields_number = 1

conversation_type = basic

sync_level = confirm

resource_security_level = none

resource_access_list_profile_name = ""

full_path_tp_exe = "/usr/bin/dvgcsac.exe"

multiple_instances = yes

user_id = "/zerodot"

server_synonym_name = ""

restart_action = once

communication_type = signals

ipc_queue_key = 0

standard_input_device = "/dev/null"

standard_output_device = "/dev/null"

standard_error_device = "/dev/null"

comments = "Std. NFTP TPN Profile"

SNA LU6.2 Mode Profile

prof_name = "FTPBIND"

mode_name = "FTPBIND"

max_sessions = 128

min_conwinner_sessions = 8

min_conloser_sessions = 8

auto_activate_limit = "/zerodot"

max_adaptive_receive_pacing_window = 63

receive_pacing_window = 63

max_ru_size = 256

min_ru_size = 256

class_of_service_name = "#CONNECT"

comments = "NFTP Default Mode name"

SNA Side Information Profile

prof_name = "dvgftpsi"

local_lu_or_control_pt_alias = ""

partner_lu_alias = ""

fq_partner_lu_name = ""

mode_name = ""

remote_tp_name_in_hex = no

remote_tp_name = ""

comments = "NFTP Side Information"
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>prof_name</td>
<td>&quot;LAURL&quot;</td>
</tr>
<tr>
<td>use_control_pt_xid</td>
<td>yes</td>
</tr>
<tr>
<td>xid_node_id</td>
<td>&quot;c&quot;</td>
</tr>
<tr>
<td>sna_dlc_profile_name</td>
<td>&quot;trdlc&quot;</td>
</tr>
<tr>
<td>stop_on_inactivity</td>
<td>no</td>
</tr>
<tr>
<td>time_out_value</td>
<td>0</td>
</tr>
<tr>
<td>LU_registration_supported</td>
<td>no</td>
</tr>
<tr>
<td>LU_registration_profile_name</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>link_tracing</td>
<td>no</td>
</tr>
<tr>
<td>trace_format</td>
<td>long</td>
</tr>
<tr>
<td>access_routing_type</td>
<td>link_address</td>
</tr>
<tr>
<td>remote_link_name</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>remote_link_address</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>remote_sap</td>
<td>0x04</td>
</tr>
<tr>
<td>verify_adjacent_node</td>
<td>no</td>
</tr>
<tr>
<td>net_id_of_adjacent_node</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>cp_name_of_adjacent_node</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>xid_node_id_of_adjacent_node</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td>node_type_of_adjacent_node</td>
<td>learn</td>
</tr>
<tr>
<td>solicit_sscp_sessions</td>
<td>yes</td>
</tr>
<tr>
<td>call_out_on_activation</td>
<td>no</td>
</tr>
<tr>
<td>activate_link_during_system_init</td>
<td>no</td>
</tr>
<tr>
<td>activate_link_on_demand</td>
<td>no</td>
</tr>
<tr>
<td>cp_cp_sessions_supported</td>
<td>yes</td>
</tr>
<tr>
<td>cp_cp_session_support_required</td>
<td>no</td>
</tr>
<tr>
<td>adjacent_node_is_preferred_server</td>
<td>no</td>
</tr>
<tr>
<td>initial_Tg_number</td>
<td>0</td>
</tr>
<tr>
<td>restart_on_normal_deactivation</td>
<td>no</td>
</tr>
<tr>
<td>restart_on_abnormal_deactivation</td>
<td>no</td>
</tr>
<tr>
<td>restart_on_activation</td>
<td>yes</td>
</tr>
<tr>
<td>TG_effective_capacity</td>
<td>4300800</td>
</tr>
<tr>
<td>TG_connect_cost_per_time</td>
<td>0</td>
</tr>
<tr>
<td>TG_cost_per_byte</td>
<td>0</td>
</tr>
<tr>
<td>TG_security</td>
<td>nonsecure</td>
</tr>
<tr>
<td>TG_propagation_delay</td>
<td>lan</td>
</tr>
<tr>
<td>TG_user_defined_1</td>
<td>128</td>
</tr>
<tr>
<td>TG_user_defined_2</td>
<td>128</td>
</tr>
<tr>
<td>TG_user_defined_3</td>
<td>128</td>
</tr>
<tr>
<td>comments</td>
<td>&quot;General Listening Link&quot;</td>
</tr>
</tbody>
</table>
SNA Token Ring Link Station Profile — Caller

prof_name = "LAURC370"
use_control_pt_xid = yes
xid_node_id = "/c5197"
sna_dlc_profile_name = "trdlc"
stop_on_inactivity = no
time_out_value = 0
LU_registration_supported = no
LU_registration_profile_name = 
link_tracing = no
trace_format = long
access_routing_type = link_address
remote_link_name = 
remote_link_address = 0x400010000008
remote_sap = 0x04
verify_adjacent_node = yes
net_id_of_adjacent_node = "DEABCYZ"
cp_name_of_adjacent_node = "YZZ"
xid_node_id_of_adjacent_node = 
node_type_of_adjacent_node = appn_end_node
solicit_sscp_sessions = no
call_out_on_activation = yes
activate_link_during_system_init = yes
activate_link_on_demand = no
cp_cp_sessions_supported = yes
cp_cp_sessions_supported = yes
adjacent_node_is_preferred_server = no
initial_Tg_number = 1
restart_on_normal_deactivation = no
restart_on_abnormal_deactivation = no
restart_on_activation = no
TG_effective_capacity = 4300800
TG_connect_cost_per_time = 0
TG_cost_per_byte = 0
TG_security = nonsecure
TG_propagation_delay = lan
TG_user_defined_1 = 128
TG_user_defined_2 = 128
TG_user_defined_3 = 128
comments = "Calling link to MVS IF4 Server"

SNA LU6.2 Partner LU Profiles

prof_name = "CAURCIF4"
fq_partner_lu_name = "DEABCXY.XYCA6IF4"
partner_lu_alias = "CAURCIF4"
session_security_supp = no
parallel_session_supp = yes
conversation_security_level = none
comments = "AURIGA calls IF4 MVS Server"

prof_name = "CAURCMAG"
fq_partner_lu_name = "DEABCYZ.YZD8900A"
partner_lu_alias = "CAURCMAG"
session_security_supp = no
parallel_session_supp = yes
conversation_security_level = none
comments = "AURIGA calls MAGELLAN"
SNA LU6.2 Partner LU Location Profile

```
prof_name = "CAURPMAG"
fq_partner_lu_name = "DEABCYZ.YZD89D/zerodotA"
fq_partner_owning_cp_name = "DEABCYZ.YZD89D/zerodotA"
local_node_is_network_server_for_len_node = yes
fq_node_server_name = ""  
comments = "Partner LU is MAGELLAN"
```

```
prof_name = "CAURPIF4"
fq_partner_lu_name = "DEABCXY.XYCA6IF4"
fq_partner_owning_cp_name = "DEABCYZ.YZZ"
local_node_is_network_server_for_len_node = yes
fq_node_server_name = ""  
comments = "Partner LU is IF4 MVS Server"
```

SNA Services/6000

SNA Node Profile

```
PROFILE name sna
Total active open CONNECTIONS (1-5000) [200]
Total SESSIONS (1-5000) [200]
Total CONVERSATIONS (1-5000) [200]
SERVER synonym name [sna]
RESTART action once
Perform ERROR LOGGING? no
Standard INPUT file/device [/dev/null]
Standard OUTPUT file/device [/dev/console]
Standard ERROR file/device [/dev/console]
```

SNA Control Point Profile

```
PROFILE name MAGELLAN
XID node ID [071YZD90]
NETWORK name [DEIBMYZ]
CONTROL POINT name [YZD89D]
```

SNA Token Ring Logical Link Profile

```
PROFILE name TDEFAULT
TRANSMIT window count (1-127) [10]
DYNAMIC window increment (1-127) [1]
RETRANSMIT count (1-30) [8]
RECEIVE window count (1-127) [127]
RING ACCESS priority 0
RETRY limit [20]
DROP LINK on inactivity? yes
INACTIVITY timeout (1-120 seconds) [120]
RESPONSE timeout (1-40, 500 msec intervals) [2]
ACKNOWLEDGE timeout (1-40, 500 msec intervals) [1]
FORCE DISCONNECT timeout (1-600 seconds) [120]
DEFINITION of maximum I-FIELD size system_defined
```

```
If user_defined, max. I-FIELD SIZE (265-3/zerodot729) [3/zerodot729]
TRACE link? no
If yes, TRACE SIZE long
```

SNA Token Ring Physical Link Profile

PROFILE name: TDEFAULT
DATALINK device name: tok/zerodot
LOCAL LINK name: []
Maximum number of LOGICAL LINKS (1-255): 32
Local SAP address (hex 04-ec): [04]

SNA Token Ring Attachment Profile — Listener

PROFILE name: AMAGLWEG
CONTROL POINT profile name: MAGELLAN
LOGICAL LINK profile name: TDEFAULT
PHYSICAL LINK profile name: TDEFAULT
STOP ATTACHMENT on inactivity? no
If yes, inactivity TIMEOUT (0-10 minutes): [0]
RESTART on deactivation? no
LU address REGISTRATION? no
If yes, LU address REGISTRATION PROFILE name: [LDEFAULT]
CALL type: listen
If listen,
  AUTO-LISTEN? yes
  MINIMUM SAP address (hex 04-ec): [04]
  MAXIMUM SAP address (hex 04-ec): [EC]
If call, ACCESS ROUTING link_name
  If link_name, REMOTE LINK name: []
  If link_address,
    Remote LINK address: [08005A81C3FE]
    Remote SAP address (hex 04-ec): [04]

SNA Token Ring Attachment Profile — Caller

PROFILE name: AWEGLMAG
CONTROL POINT profile name: WEGA
LOGICAL LINK profile name: TDEFAULT
PHYSICAL LINK profile name: TDEFAULT
STOP ATTACHMENT on inactivity? no
If yes, inactivity TIMEOUT (0-10 minutes): [0]
RESTART on deactivation? no
LU address REGISTRATION? no
If yes, LU address REGISTRATION PROFILE name: [LDEFAULT]
CALL type: call
If listen,
  AUTO-LISTEN? no
  MINIMUM SAP address (hex 04-ec): [04]
  MAXIMUM SAP address (hex 04-ec): [EC]
If call, ACCESS ROUTING link_address
  If link_name, REMOTE LINK name: []
  If link_address,
    Remote LINK address: [10005A4F9C85]
    Remote SAP address (hex 04-ec): [04]
### SNA LU6.2 Local LU Profile — Listener

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE name</td>
<td>YZD89D0A</td>
</tr>
<tr>
<td>TPN LIST profile name</td>
<td>[NFTP_TPN]</td>
</tr>
<tr>
<td>NETWORK name</td>
<td>[DEIBMYZ]</td>
</tr>
<tr>
<td>Local LU NAME</td>
<td>[YZD89D0A]</td>
</tr>
<tr>
<td>INDEPENDENT LU?</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>If no, Local LU ADDRESS (1-255)</td>
</tr>
<tr>
<td></td>
<td>SSCP ID</td>
</tr>
</tbody>
</table>

### SNA LU6.2 Local LU Profile — Caller

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE name</td>
<td>YZD89D0B</td>
</tr>
<tr>
<td>TPN LIST profile name</td>
<td>[NFTP_TPN]</td>
</tr>
<tr>
<td>NETWORK name</td>
<td>[DEIBMYZ]</td>
</tr>
<tr>
<td>Local LU NAME</td>
<td>[YZD89D0B]</td>
</tr>
<tr>
<td>INDEPENDENT LU?</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>If no, Local LU ADDRESS (1-255)</td>
</tr>
<tr>
<td></td>
<td>SSCP ID</td>
</tr>
</tbody>
</table>

### SNA LU6.2 Logical Connection Profile — Listener

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE name</td>
<td>CMAGLWEG</td>
</tr>
<tr>
<td>ATTACHMENT profile name</td>
<td>[AMAGLWEG]</td>
</tr>
<tr>
<td>LOCAL LU profile name</td>
<td>[YZD89D0A]</td>
</tr>
<tr>
<td>NETWORK name</td>
<td>[DEIBMYZ]</td>
</tr>
<tr>
<td>STOP CONNECTION on inactivity?</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>If yes, TIMEOUT (0-10 minutes)</td>
</tr>
<tr>
<td>REMOTE LU name</td>
<td>[YZD89D0B]</td>
</tr>
<tr>
<td>SECURITY Accepted</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>If conversation or already_verified, CONVERSATION SECURITY ACCESS LIST profile</td>
</tr>
<tr>
<td></td>
<td>(If no name entered, /etc/passwd used)</td>
</tr>
<tr>
<td>REMOTE TPN LIST profile name</td>
<td>[RDEFAULT]</td>
</tr>
<tr>
<td>MODE LIST profile name</td>
<td>[FTPBINDS]</td>
</tr>
<tr>
<td>INTERFACE type</td>
<td>extended</td>
</tr>
<tr>
<td></td>
<td>If extended, SESSION CONCURRENCY</td>
</tr>
<tr>
<td>Node VERIFICATION?</td>
<td>no</td>
</tr>
</tbody>
</table>

### SNA LU6.2 Logical Connection Profile — Caller

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE name</td>
<td>CWEGLMAG</td>
</tr>
<tr>
<td>ATTACHMENT profile name</td>
<td>[AWEGCMAG]</td>
</tr>
<tr>
<td>LOCAL LU profile name</td>
<td>[YZD89D0B]</td>
</tr>
<tr>
<td>NETWORK name</td>
<td>[DEIBMYZ]</td>
</tr>
<tr>
<td>STOP CONNECTION on inactivity?</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>If yes, TIMEOUT (0-10 minutes)</td>
</tr>
<tr>
<td>REMOTE LU name</td>
<td>[YZD89D0A]</td>
</tr>
<tr>
<td>SECURITY Accepted</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>If conversation or already_verified, CONVERSATION SECURITY ACCESS LIST profile</td>
</tr>
<tr>
<td></td>
<td>(If no name entered, /etc/passwd used)</td>
</tr>
<tr>
<td>REMOTE TPN LIST profile name</td>
<td>[RDEFAULT]</td>
</tr>
<tr>
<td>MODE LIST profile name</td>
<td>[FTPBINDS]</td>
</tr>
<tr>
<td>INTERFACE type</td>
<td>extended</td>
</tr>
<tr>
<td></td>
<td>If extended, SESSION CONCURRENCY</td>
</tr>
<tr>
<td>Node VERIFICATION?</td>
<td>no</td>
</tr>
</tbody>
</table>
SNA LU6.2 Mode Profile — FTPBIND

PROFILE name FTPBIND
MODE name FTPBIND
Maximum number of SESSIONS (1-999) 128
Minimum contention WINNERS (0-499) 8
Minimum contention LOSERS (0-500) 8
Auto ACTIVATIONS limit (0-500) 0
RECEIVE pacing (0-63) 63
SEND pacing (0-63) 63
Maximum RU SIZE (256,288,...,3840) 256
RECOVERY level no_reconnect

SNA LU6.2 Mode List Profile

* PROFILE name [FTPBINDS]
Add profile names to list:
   Name 1 [FTPBIND]
   Name 2
   Name 3
   Name 4
   Name 5
   Name 6
   Name 7
   Name 8
   Name 9
   Name 10
   Name 11
   Name 12
   [MORE...52]

SNA LU6.2 TPN Profile

PROFILE name dvgftpb1
Transaction program name is in HEXADECIMAL? no
TRANSACTION program name [DUMMY]
PIP data? yes
   If yes, SUBFIELDS (0-99) 1
CONVERSATION type basic
RECOVERY level no_reconnect
SYNC level confirm
Full PATH to TPN executable [/usr/bin/dvgcsac.exe]
MULTIPLE INSTANCES supported? yes
User ID 0
SERVER synonym name
RESTART action once
COMMUNICATION type signals
   If IPC, communication IPC queue key 0
Standard INPUT file/device [/dev/null]
Standard OUTPUT file/device [/dev/console]
Standard ERROR file/device [/dev/console]
SECURITY Required none
   If access,
      RESOURCE SECURITY ACCESS LIST profile [RSRCDEFAULT]
      (If no name entered, /etc/passwd used)
SNA LU6.2 TPN List Profile

* PROFILE name

Add profile names to list:

Name 1: [dvgftpb1]
Name 2:
Name 3:
Name 4:
Name 5:
Name 6:
Name 7:
Name 8:
Name 9:
Name 10:
Name 11:
Name 12:

[NFTP_TPN]

SNA LU6.2 RTPN Profile

PROFILE name: RDEFAULT
RTPN name is in HEXADECIMAL? no
RTPN name: [rtpn]
PIP data? yes
CONVERSATION type: basic
RECOVERY level: no_reconnect
SYNC level: confirm

Server Group Table (srvgrp.tab) Entries

CMAGLWEG
CMAGLFRS
CMAGLIF4

Monitoring Your SNA Activities

Sometimes it is useful to monitor the SNA activities to know which attachments and which connection are active at a workstation. The following is a sample script for that purpose. You can use it, but you must modify the workstation host names stated in uppercase in the sample. Place the script into a directory that contains executable parts.

```
while true
do
    echo local SNA Status MAGELLAN:
    lssrc -l -s'sna'
    echo remote SNA Status WEGA:
    rexec wega lssrc -l -s'sna'
    sleep 10
tput clear
done
```

In your $HOME directory, set up a .netrc file to permit access to the remote TCP/IP node. The file must have entries such as:

```
machine wega login fred password xyz
```
Appendix E. Summary of Installed Files

The following table summarizes the files and directories that are stored on your workstation during the installation of NetView FTP AIX. Additionally, a short description of the files is given.
<table>
<thead>
<tr>
<th>File:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/lib/libdvg.a</td>
<td>NetView FTP shared library.</td>
</tr>
<tr>
<td>/usr/lib/libdvgsv.a</td>
<td>Shared library of the NetView FTP server component.</td>
</tr>
<tr>
<td>/usr/lib/libxvtxmhelp_shr.a</td>
<td>Shared library of the NetView FTP graphical user interface help.</td>
</tr>
<tr>
<td>/usr/lib/libxvtmtk_shr.a</td>
<td>Shared library of the NetView FTP graphical user interface.</td>
</tr>
<tr>
<td>/usr/bin/nftp</td>
<td>Command handler executable for all users.</td>
</tr>
<tr>
<td>/usr/bin/nftpd</td>
<td>Command handler executable for root.</td>
</tr>
<tr>
<td>/usr/bin/dvgdem.exe</td>
<td>NetView FTP system daemon executable. This component is responsible for controlling the NetView FTP system resources.</td>
</tr>
<tr>
<td>/usr/bin/dvgrsp.exe</td>
<td>NetView FTP responder component executable. This component is responsible for controlling the remote access to a workstation.</td>
</tr>
<tr>
<td>/usr/bin/dvgtrm.exe</td>
<td>NetView FTP transfer manager. This component is started by the command handler or by the responder component to perform the file transfer.</td>
</tr>
<tr>
<td>/usr/bin/dvgcs.exe</td>
<td>Main module of the NetView FTP server component. This component controls the started child’s dvgcslc.exe and dvgcsac.exe.</td>
</tr>
<tr>
<td>/usr/bin/dvgcslc.exe</td>
<td>NetView FTP server component module that controls the handling of the client and the responder component within the local network.</td>
</tr>
<tr>
<td>/usr/bin/dvgcsac.exe</td>
<td>NetView FTP server component module that controls the conversation with the SNA network.</td>
</tr>
<tr>
<td>/usr/bin/dvgpdc.exe</td>
<td>NetView FTP protocol data converter. This component is responsible for the protocol parsing between different nodes.</td>
</tr>
<tr>
<td>/usr/bin/dvgprot.inc</td>
<td>Include file that the protocol-data converter reads in case of any protocol violation.</td>
</tr>
<tr>
<td>/usr/bin/nftp_smit</td>
<td>NetView FTP SMIT converter executable.</td>
</tr>
<tr>
<td>/usr/bin/nftpguic</td>
<td>Control panel for the NetView FTP graphical user interface: root services for root, status panel for all other users.</td>
</tr>
<tr>
<td>/usr/bin/nftpguid</td>
<td>NetView FTP user interface for user services.</td>
</tr>
<tr>
<td>/usr/bin/nftpguis</td>
<td>NetView FTP user interface, send panel.</td>
</tr>
<tr>
<td>/usr/bin/nftpguir</td>
<td>NetView FTP user interface, receive panel.</td>
</tr>
<tr>
<td>/usr/lpp/nftp/samples/*</td>
<td>NetView FTP samples: ini, rdf, Xdefaults.</td>
</tr>
<tr>
<td>/usr/lpp/nftp/etc/*</td>
<td>NetView FTP files for customization, online documentation.</td>
</tr>
</tbody>
</table>
Glossary

This glossary defines many of the terms and abbreviations used with NetView FTP. If you do not find the term you are looking for, refer to the Dictionary of Computing, New York: McGraw-Hill, 1994.

**Access Method Services.** A utility program that defines VSAM data sets and allocates space for them, converts indexed sequential data sets to key-sequenced data sets with indexes, modifies data set attributes in the catalog, facilitates data set portability between operating systems, creates backup copies of data sets and indexes, helps make inaccessible data sets accessible, and lists data set records and catalog entries.

**ACF/VTAM.** Advanced Communications Function for the Virtual Telecommunications Access Method.

**active request.** A request that is presently being scheduled or for which the corresponding file transfer is in progress.

**adaptive compression.** A method by which the amount of storage required for data can be reduced by replacing character strings that are repeated with references to a directory of such character strings.

**added request.** A request that has been added to the request queue.

**administrator query command.** A type of command that causes NetView FTP to retrieve information about the request queue or the requests in it; the information retrieved is intended for the NetView FTP administrator. Contrast with user query command.

**administrator query record.** A record containing the information NetView FTP retrieves when an administrator issues an administrator query command. Contrast with user query record.

**adopted authority.** When a program is created, it can specify that the program always runs under the program owner’s user profile. A user does not need authority specifically given to him for the objects used by the program, but uses (adopts) the program owner’s authority. The user has authority for the objects used by the program only when he is running the program and other programs called by the program.

**Advanced Communications Function for the Virtual Telecommunications Access Method.** An IBM licensed program that controls communication and the flow of data in an SNA network. It provides single-domain, multiple-domain, and interconnected network capability. VTAM runs under MVS, VSE, and VM/SP, and supports direct control application programs and subsystems such as NetView FTP and VSE/POWER.

**Advanced Function Feature.** A set of extra functions that extend the capabilities of the NetView FTP V1 MVS base product.

**advanced peer-to-peer networking.** Data communications support that routes data in a network between two or more APPC systems that are not directly attached.

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

**AET.** Application Entity Title.

**AFF.** Advanced Function Feature.

**alias.** An alternative name for a member of a partitioned data set.

**AMS.** Access Method Services.

**APAR.** Authorized program analysis report.

**APF.** Authorized Program Facility.

**APL.** Application program parameter list.

**APPC.** Advanced program-to-program communication.

**Application Entity Title.** The name by which an OSI application (and filestore) can be addressed by remote users. By contrast, the local name of the filestore is the filestore nickname.

**application program parameter list.** A control block used by application programs to pass parameter values to NetView FTP.

**application program parameter list extension.** A control block used by application programs to pass parameter values to NetView FTP; a supplement to the application program parameter list.

**APPN.** Advanced peer-to-peer networking.

**APX.** Application program parameter list extension.

**attended mode.** An operating mode of NetView FTP for Workstations that assumes that a user at a workstation expects to be informed about the success of transfers and is available to load devices such as diskettes or tapes. Contrast with unattended mode.
automatic logon retry. NetView FTP’s method for eventually establishing a conversation with a remote system. It is used when a server cannot initiate a conversation with a server at a remote system because:

- All the servers at the remote system are busy with other transfers
- None of the servers at the remote system has been started
- ACF/VTAM is temporarily unable to find a path between the two servers.

The server at the local system automatically changes the status of the request from active back to waiting, and goes on to process the next request in the request queue (MVS, VSE, or VM) or request database (OS/400). Later, NetView FTP tries again to process the request. It keeps trying until it succeeds in initiating a conversation.

automatic transfer restart. NetView FTP’s method for automatically restarting a file transfer that was interrupted. In the following situations, NetView FTP is not able to recover a conversation:

- The queue handler or server at either system is terminated
- The server at either system cannot allocate the file being transferred
- A pre-transfer user-exit routine at either system rejected the file transfer
- There is a severe or prolonged conversation outage.

However, when you create a request you can specify that if one of these situations arises, NetView FTP is to change the status of the request back to waiting. The servers at your system then periodically reprocess the request until one of them succeeds in restarting the transfer.

basic partitioned access method. An access method that can be used to create program libraries in direct-access storage for convenient storage and retrieval of programs.

basic sequential access method. An access method for storing or retrieving data blocks in a continuous sequence, using either a sequential access or a direct access storage device.

BIND. Bind Session.

Bind Session. In SNA, a request to activate a session between two logical units.

blocked request. A waiting request that is trapped in the queue. The request was passed to the queue handler at a time when there was enough CSA storage available to NetView FTP to do so. However, in the meantime, the limit of the amount of CSA storage available to NetView FTP was reduced and is not enough to allow the queue handler to pass the request to a server for processing. The request cannot be processed until the limit of the amount of CSA storage available to NetView FTP is raised.

BPAM. Basic partitioned access method.

BSAM. Basic sequential access method.

callback. In the AIX operating system, a procedure that is called if and when certain specified conditions are met. This is accomplished by specifying the procedure in a callback list.

callback list. (1) A list of procedures that are called if and when certain specified conditions are met. (2) In the program IBM AIXwindows Environment/6000, individual widgets can define callback lists.

CCB. Command control block.

CCI. Common control block insertion.

CCSID. Coded character set identifier.

CCW. Channel command word.

CDC. Character data conversion.

CDRA. Character Data Representation Architecture.

CDRM. Cross-domain resource manager.

CDE. Cross-domain resource.

character data. Data in the form of letters, numbers, and special characters, such as punctuation marks, that can be read by the human eye.

Character Data Representation Architecture. An IBM architecture that defines a set of identifiers, services, supporting resources, and conventions to achieve a consistent representation, processing, and interchange of graphic character data in SAA environments.

character literal. A symbol, quantity, or constant in a source program that is itself data, rather than a reference to data.

checkpoint. A point at which information about the status of a file transfer is recorded. If the file transfer is interrupted, NetView FTP can use this information to resume the file transfer from a point near where the interruption occurred instead of from the beginning of the file.

checkpoint data set. A data set that contains information about the current status of an active file
transfer. If the file transfer is interrupted, NetView FTP can use this information to resume the file transfer from a point near where the interruption occurred instead of from the beginning of the file.

**checkpoint file.** A synonym for checkpoint data set.

**checkpoint record.** A record of a checkpoint data set or file. One checkpoint record contains the information needed to restart one file transfer from a checkpoint.

**checkpoint/restart data set.** A deprecated term for checkpoint data set.

**checkpoint/restart record.** A deprecated term for checkpoint record.

**class.** See server class.

**client.** On a local area network, a workstation that requests service from a server workstation.

**CLIST.** Command list.

**Coded character set identifier.** In NetView FTP, an identifier that represents a set of graphic characters and their code point assignment. The coded character set identifier defines how characters are mapped to decimal values.

**command control block.** A control block that contains details of the queue handler command to be carried out.

**command list.** A list of commands and control statements that is assigned a name. When the name is invoked (as a command) the commands in the list are executed.

**common service area.** In MVS, a part of the common area that contains data areas that are addressable by all address spaces. During use, these areas are protected by the key of the requester.

**completion user exit.** Deprecated term for post-transfer user exit.

**compression.** A technique for converting data into a form that requires less storage space and less transmission time than its original form. Contrast with decompression. See also SNA compaction and SNA compression.

**condition code.** A 4-digit decimal value derived from the value a server places in register 15 before returning control to the operating system. The digits of the condition code consist of the server return code and, for a server running in single mode, the file-transfer return code.

**continuous mode.** A server running mode in which a server continues running after it has transferred a file.

**control language.** The set of all commands with which a user requests system functions.

**control point.** A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network.

**control statement.** A statement that controls or affects the running of a program. For example, NOTAFTER=('21:34', '94/12/25') is a control statement that assigns the value ('21:34', '94/12/25') to the parameter represented by the keyword NOTAFTER.

**conversation.** In SNA, a connection between two transaction programs over an LU-LU session that lets them communicate with each other while processing a transaction.

**CP.** Control point.

**CP-CP sessions.** The parallel sessions between two control points, using LU 6.2 protocols.

**Cross-domain resource.** In VTAM programs, synonym for other-domain resource.

**Cross-domain resource manager.** The functions of the system services control point (SSCP) that control initiation and termination of cross-domain resources.

**cryptographic key.** A value used to encrypt and decrypt data transmitted in an LU-LU session that uses cryptography.

**cryptography.** The transformation of data to conceal its meaning.

**CSA.** Common service area.

**current request.** The request currently being created or changed by the user of the NetView FTP panels.

**daemon.** In the AIX operating system, a program that runs unattended to perform a standard service.

**daemon process.** In the AIX operating system, a process begun by the root user or the root shell that can be stopped only by the root user. Daemon processes generally provide services that must be available at all times.

**DASD.** Direct-access storage device.

**data control block parameters.** The following parameters: Record Format, Logical Record Length, and Physical Block Size.
**data set control block.** A control block containing specifications for data sets that are to be created.

**data transfer message unit.** The message unit used to send the data object.

**DCB parameters.** Data control block parameters.

**decompression.** A technique for converting compressed data back into its original form. Contrast with compression.

**default first qualifier.** Server initialization parameter. Sometimes referred to as the GID initialization parameter. The server uses this parameter as the first qualifier when it creates a name for the data set.

**default value.** The value that is assigned to a parameter by a program if no value is specified by a user.

**deferred request.** A waiting request that is temporarily trapped in the queue. CSA storage was obtained for NetView FTP, but not enough for the queue handler to pass the request to a server for processing. The request is processed later, when more CSA storage is available to NetView FTP.

**delay time.** The amount of time a finished request stays in the request queue before rebuilding the request queue causes it to be deleted automatically.

**direct transfer.** Transfer of data from one file to another file without first storing the data in an intermediate file.

**direct-access storage device.** A storage device for which access time is effectively independent of the location of the data being accessed.

**directory file.** In the AIX operating system, a file that contains information the system needs to access all types of files.

**distribution-service component.** A component of NetView FTP VM that handles communication with the queue handler (such as retrieving requests to be processed), and with the network (such as establishing conversations and transferring files). In NetView FTP VM, each server consists of one distribution-service component and up to 32 file-service components.

**distribution-service machine.** With NetView FTP VM, a virtual machine in which a distribution-service component runs.

**DSCB.** Data set control block.

**DTMU.** Data transfer message unit.

**dynamic allocation.** The allocation of a file when it is needed, not in advance. Contrast with job allocation.

**encrypt.** To scramble data or convert data to a secret code that masks the meaning of the data to any unauthorized recipient.

**entry sequence.** The order in which records are physically arranged in auxiliary storage.

**entry-sequenced data set.** A data set whose records are loaded without respect to their contents, and whose relative byte addresses cannot change.

**ESDS.** Entry-sequenced data set.

**ESTAE.** Extended specify task abnormal exit.

**exceptional checkpointing.** To take a checkpoint when certain types of errors occur.

**exchange identification.** The ID that is exchanged with the remote physical unit when an attachment is first established.

**exclude members.** To choose those members of a PDS that are not to be transferred. Contrast with select members.

**exit.** A point in a program at which control is passed to another program.

**exit routine.** A routine that receives control when a specified event occurs.

**Exit(n) Message Unit.** The message unit used to convey information provided by the Post-Transfer User Exit routine n (where n is 1 or 2) of the sender to the receiver.

**extended specify task abnormal exit.** A macroinstruction that allows a user to intercept a scheduled abnormal termination.

**FAT.** File allocation table.

**FBA.** Feedback area.

**feedback area.** An area of storage containing information related to a queue handler command. For example, an FBA can contain a request control block, a query data area, or a server data area.

**file allocation table.** A table used by DOS and OS/2 to allocate space on a disk for a file and to locate and chain together parts of the file that may be scattered on different sectors so that the file can be used in a random or sequential manner.

**file group.** One or more files that reside on one system. For example, all files that are stored in the
same directory or whose file names consist of partly matching character strings are considered a file group.

**file pool.** A collection of minidisks managed by SFS. It contains user files and directories and associated control information. Many user's files and directories can be contained in a single file pool.

**file transfer.** The sending and receiving of the contents of a file.

**File Transfer Access and Management.** A set of programs, such as OSI/File Services, which conforms to FTAM standards to manage and transfer files over an OSI network.

**file-service component.** A component of NetView FTP VM that handles file access and the taking of checkpoints. In NetView FTP VM, each server consists of one distribution-service component and up to 32 file-service components.

**file-transfer completion message.** A message, sent by a server to a user after a file transfer, which describes the outcome of a file transfer.

**file-transfer report.** A file, sent by a server to a user after a file transfer which describes the outcome of a file transfer.

**file-transfer request.** A list of parameters and their values that tell NetView FTP (1) that it is to transfer a file from one system to another, and (2) about the file transfer and the sending and receiving data sets.

**filestore.** See local filestore and remote filestore.

**filestore nickname.** The name of the filestore at the local level. It is defined by the filestore owner when registering the filestore in the LRD, and is used by authorized local users to access that filestore.

**filestore owner.** The single user, local or remote, who has created the filestore and who controls the passwords for accessing it and the filestore accessibility. Each OSI/File Services user owns one filestore.

**filestore subset.** A subdivision of the local filestore. It is the first qualifier of the MVS data-set name. Each local file is registered in the LRD under a related filestore subset, which in turn belongs to a local filestore.

**filter.** In the AIX operating system, a command that reads standard input data, modifies the data, and sends it to the display screen.

**finished request.** A request for which the corresponding file transfer has finished, whether successfully or unsuccessfully.

**FIU.** File Interchange Unit.

**FTAM.** File Transfer Access and Management.

**FTP level.** A character that represents the level of sophistication of an FTP or NetView FTP program.

**FTP V2.** File Transfer Program Version 2 Release 2.

**FSB.** NetView FTP shared block.

**FSBX.** NetView FTP shared block extension.

**GDG.** Generation data group.

**generation data group.** A collection of data sets kept in chronological order; each data set is a generation data set.

**generation data set.** One generation of a generation data group.

**GETVIS area.** Storage space within a partition or the shared virtual area, available for dynamic allocation to programs.

**GID initialization parameter.** See default first qualifier.

**GUI.** The graphical user interface of NetView FTP for Workstations.

**handle.** (1) In the Advanced DOS and OS/2 operating systems, a binary value created by the system that identifies a drive, directory, and a file so that the file can be found and opened. (2) In the AIX operating system, a data structure that is a temporary local identifier for an object.

**HDAM.** Hierarchic direct access method.

**hex.** Abbreviation of hexadecimal.

**hierarchic direct access method.** A database access method that uses algorithmic addressability of records in a hierarchic direct organization.

**hierarchic indexed sequential access method.** A database access method that uses indexed access to records in a hierarchic sequential organization.

**High Performance File System.** A file organization available under OS/2.

**HISAM.** Hierarchic Indexed Sequential Access Method.

**HPFS.** High Performance File System.

**ICCF.** Interactive computing and control facility.

**ICF.** Intersystem communications function.
IMS/VS. Information Management System/Virtual Storage.

independent LU. A logical unit (LU) that does not receive an ACTLU over a link. Such LUs can act as primary logical units (PLUs) or secondary logical units (SLUs) and can have one or more LU-LU sessions at a time.

INI file. See initialization file.


input field. An area on a panel in which data is entered.

instance. In the AIX operating system, the concrete realization of an abstract object class. An instance of a widget or gadget is a specific data structure that contains detailed appearance and behavioral information that is used to generate a specific graphical object on-screen at run time.

Internet. A wide area network connecting thousands of disparate networks in industry, education, government, and research. The Internet network uses /IP as the standard for transmitting information.

Internet Protocol. A protocol used to route data from its source to its destination in an Internet environment.

Intersystem communications function. Communications between application programs on an AS/400 system and an application program on a remote system are accomplished using the AS/400 system intersystem communications function (ICF) and the underlying support.

IP. Internet Protocol.

ISPF. Interactive System Productivity Facility.

JCL. Job control language.

JES. Job entry subsystem.

job allocation. The allocation of a file by a server startup job. The allocation takes place when a server is started, which is before (sometimes long before) the file transfer takes place. Contrast with dynamic allocation.

job control language. A control language used to identify a job to an operating system and to describe the job's requirements.

key sequence. In VSAM, the collating sequence of data records as determined by the value of the key field in each record.

key-sequenced data set. A VSAM data set whose records are loaded in key sequence and controlled by an index.

keyword. A part of a control statement that consists of a specific character string.

KSDS. Key-sequenced data set.

LAN. Local area network.

LAN gateway. A functional unit that connects a local area network with another network using different protocols.

LDS. Linear data set.

LEN node. Low-entry networking node. That is a node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

linear data set. A VSAM data set that contains data but no control information. A linear data set can be accessed as a byte-string in virtual storage. A linear data set has no records and a fixed control interval size of 4096 bytes.

local. Refers to one's own system.

local area network. A data network located on the user's premises in which serial transmission is used for direct data communication among workstations.

local filestore. A collection of local files. Each local filestore is registered in the LRD with a filestore nickname for local access, and a filestore AET for remote access.

Local Resource Directory. The file containing information on local users, local filestores, filestore subsets, and local files necessary for OSI/File Services to run initiator and responder functions.

local-request handler. A server subtask that can process a request submitted at the local system and can initiate a conversation.

log file. A file to which a NetView FTP component writes messages.

logical unit. In SNA, a port through which an end user accesses an SNA network. Each NetView FTP server is a logical unit.

logical unit name. A name used to represent the address of a logical unit.

LRD. Local Resource Directory.
LU. Logical unit.

LU name. Logical unit name.

LU 0 conversation. The type of conversation NetView FTP uses for file transfers between a node where NetView FTP V2.1 MVS, NetView FTP V1 VM, or NetView FTP V1 VSE is installed and a node where NetView FTP V1 MVS or FTP V2 is installed.

LU-LU session. In SNA, a session between two logical units (LUs) in an SNA network.

manual transfer restart. NetView FTP’s method for allowing a user to restart a file transfer that was interrupted by submitting a restart request for that file transfer.

master password. A password, set by the NetView FTP system programmer that lets those who specify it query, modify, or delete any request in the request queue, regardless of whether or not it is password-protected, and regardless of who added it to the queue.

message area. The area of storage to which NetView FTP writes the messages it issues to an application program.

mode. The session limits and common characteristics of the session associated with advanced program-to-program (APPC) devices managed as a unit with a remote location.

mode description. A system object created for advanced program-to-program (APPC) devices that describes the session limits and the characteristics of the session, such as the maximum number of sessions allowed, maximum number of conversations allowed, and other controlling information for the session.

MVS node. A node with MVS as its operating system.

MVS system. A system with MVS as its operating system.

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

NetView FTP application program. An application program that adds, queries, modifies, or deletes a request, or that retrieves information about NetView FTP.

NetView FTP batch job. A batch job that adds, queries, modifies, or deletes a request, or that retrieves information about NetView FTP.


NetView FTP MVS. NetView File Transfer Program for MVS.


NetView FTP partition. A VSE partition that contains the main components of NetView FTP VSE.

NetView FTP shared block. An area of CSA storage that is used to pass data between the components of NetView FTP. Any data that does not fit in the FSB is put in the NetView FTP shared block extension.

NetView FTP shared block extension. An area of ECSA storage that is used to pass data between the components of NetView FTP. It contains any data that does not fit in the NetView FTP shared block.

NetView FTP VM. NetView File Transfer Program for VM.

NetView FTP VSE. NetView File Transfer Program for VSE.

network. An interconnected group of nodes.

network drive. With NetView FTP, it is a shared resource that can be accessed from each workstation in the LAN.

network job entry facility. A facility that uses the network job-interface (NJI) protocols to allow a computer system to communicate with other computer systems in a network.

NFTP directory. The directory that contains the NetView FTP/2 product files.

NFTWORK directory. The directory that contains all NetView FTP/2 work files, for example, the NetView FTP message and log files.

NJE. Network job entry.

NJI. Network job-interface.
node. An endpoint in a link, or a junction common to two or more links in a network. A deprecated term for server group.

node ID. Deprecated term for server group.

node ID table. Deprecated term for server group table.

not-after time. The time after which NetView FTP is not to process a request.

not-before time. The time before which NetView FTP is not to process a request.

numeric literal. A numeric character or string of numeric characters whose value is implicit in the characters themselves; for example, 777 is the literal as well as the value of the number 777.

octal. Pertaining to a selection, choice, or condition that has eight possible different values or states.

OEM. Original equipment manufacturer.

Open Systems Interconnection. The seven-layer communications architecture used for the definition of protocol standards for networks.

operation mode. See attended mode and unattended mode.

operational key. Deprecated term for cryptographic key.

Original equipment manufacturer. A manufacturer of equipment that may be marketed by another manufacturer.

originator ID. A string of characters that identifies the job, started task, or user that added a request to the request queue.

OSI. See Open Systems Interconnection.

other-domain resource. A recommendation for a logical unit that is owned by another domain and is referenced by a symbolic name, which can be qualified by a network identifier.

panel. A predefined image displayed on a terminal screen.

panel flow. The way in which panels are chained together so that a user can move from one to another.

panel layout. The way in which the text and the input fields on a panel are arranged.

partitioned data set. A data set in direct access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data.

PCF. Programmed Cryptographic Facility.

PDS. Partitioned data set.

path information unit. In SNA, a message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

phase. The smallest unit of executable code that can be loaded into virtual storage.

ping. The use of the ping command to send an echo request to a network host or gateway.

port. With NetView FTP, the communication end point in TCP/IP. A port is identified by a port number.

port number. In TCP/IP, a 16-bit number used to communicate between TCP/IP and a higher-level protocol or application.

post-conversation user exit. A user exit that passes control to a routine at the system at which the file-transfer request originated. This routine is to run just after the servers terminate their conversation.

post-transfer user exit. A user exit that passes control to a routine that is to run just after a server closes a file that has been transferred.

pre-queuing user exit. A user exit that passes control to a routine that is to run just after a request is submitted to NetView FTP and just before NetView FTP adds the request to the queue.

pre-transfer user exit. A user exit that passes control to a routine that is to run just before a server opens a file that is to be transferred.

preparation user exit. Deprecated term for pre-transfer user exit.

process (a request). To obtain and try to carry out (a request).

program temporary fix. A temporary solution to bypass of a problem diagnosed by IBM as resulting from a defect in a current unaltered release of a program.

PTF. Program temporary fix.

PUBX. Physical Unit Control Block Extension.

QDA. Query data area.

QRA. Query response area.
QSAM. Queued sequential access method.

QSR. Query Status Record.

query (a request). To ask for information about (a request).

query data area. The area of ECSA storage into which NetView FTP places either user query records or administrator query records.

query response area. The area of storage into which NetView FTP places information it retrieves for an application program.

queue handler. A NetView FTP component that controls access to the request queue. In NetView FTP MVS, the queue handler also controls all other NetView FTP components and all communication with the operator.

queue handler command. A command that a component of NetView FTP issues to the queue handler when it wants the queue handler to do something.

queued sequential access method. An extended version of the basic sequential access method (BPAM). When this method is used, a queue is formed of (1) input data blocks that are awaiting processing or (2) output data blocks that have been processed and are awaiting transfer to auxiliary storage or to an output device.

raw device. In the AIX operating system, a device that treats data I/O as a continuous stream, without consideration for the data's logical structure. For example, I/O for fixed disks and streaming tapes occurs in units of bytes that have no relationship to characters.

RCB. Request control block.

RCE. Request control element.

RDF. Request definition file.

reason code. A value issued by a program that gives additional information about a situation described by a return code.

receiving data set. A data set in which a copy of a file that has been sent using NetView FTP has been placed. Contrast with sending data set.

receiving file. A data set in which a copy of a file is placed that has been sent using NetView FTP. Contrast with sending file.

receiving system. The NetView FTP system that receives the file being transferred.

regular checkpointing. To take a checkpoint at specified regular intervals.

regular file. In the AIX operating system, a file that contains data. A regular file can be a text file or a binary file. Text files contain information readable by the user. This information is stored in ASCII. Binary files contain information readable by the computer.

relative record data set. In VSAM, a data set whose records are loaded into fixed-length slots and are represented by the relative-record numbers of the slots they occupy.

remote. Pertaining to a system other than one's own.

remote filestore. A collection of remote files. OSI/File Services users can access a file residing in a remote system only if they specify the filestore AET of the remote filestore, and the OSI file name of the related file.

remote-request handler. A server subtask that can accept a conversation initiated by a local-request handler at a remote system.

report. Synonym for file-transfer report.

report recipient. A user to whom a server sends a file-transfer report.

request. Synonym for file-transfer request.

request class. A deprecated term for server class.

request control block. A control block that contains some or all of a file-transfer request. Data that does not fit in the RCB is put in the request control block extension.

request control block extension. A control block that contains data that does not fit in the request control block.

request control element. An element of the request queue directory.

request database. In NetView FTP/400, the database in which NetView FTP stores all requests.

request definition file. A file containing NetView FTP control statements, that is, all NetView FTP parameters with their appropriate values that are necessary for a file transfer.

request handler. A server subtask. See also remote-request handler.

request number. A number that the queue handler assigns to a request when it adds the request to the request queue and that is used to identify the request.
**request password.** A character string, assigned by a user to a request, that prevents users sharing that user's originator ID from deleting or modifying that user's waiting and active requests. If a user specifies a request password for a request, another user with the same originator ID must specify either the request password or the master password to be able to delete or modify the request while it is waiting, or to delete the request while it is active.

**request priority.** A number, assigned by a user to each request, that determines the order in which a server is to process it. When a server is ready to process a request and several requests are eligible, the server processes the request with the highest priority first.

**request queue.** In NetView FTP for MVS, VSE, or VM, the file in which NetView FTP stores requests that have been submitted for processing.

**request queue directory.** A directory of the contents of the request queue.

**request unit.** A message unit that contains control information, end-user data, or both.

**request-queue user exit.** Deprecated term for pre-queuing user exit.

**requesting system.** The system where the file-transfer request has been initiated.

**resident session partner.** An FTP V2 MVS or FTP V2 VSE server that runs continuously and can perform an indefinite number of file transfers, however, these file transfers must all be initiated by servers at remote systems.

**responding system.** The system responding to a file-transfer request.

**return code.** A value issued by a program that describes the outcome of an operation performed by that program.

**root.** In the AIX operating system, the user name for the system user with the most authority.

**RRDS.** Relative record data set.

**RTM.** Recovery Termination Manager.

**RU.** Request unit.

**RXB.** Request control block extension.

**SAF.** System authorization facility.

**SAM.** Sequential access method.

**SAS.** Spool Access Services.

**saved request.** A request that has been created with the NetView FTP panels and that has then been saved in an ISPF table data set.

**scheduling a request.** Determining which request is to be obtained, obtaining it, and passing it to a server.

**scroll amount.** The amount that the list on a panel is scrolled up or down when you enter the **UP** or **DOWN** command.

**SDA.** Server data area.

**SDMU.** Source description message unit.

**SDWA.** System Diagnostic Work Area.

**select members.** To choose those members of a PDS that are to be transferred. Contrast with exclude members.

**sending data set.** A data set, a copy of which is to be transferred using NetView FTP. Contrast with receiving data set.

**sending file.** A file of which a copy is to be transferred using NetView FTP. Contrast with receiving file.

**sending system.** The NetView FTP system stores the file that will be transferred to the receiving system.

**sequential access method.** See basic sequential access method.

**server.** (1) A NetView FTP component that establishes or accepts conversations and that transfers files. (2) With NetView FTP for Workstations, a NetView FTP Server program that serves as a gateway for one or more NetView FTP Client programs.

**server class.** A number or letter, assigned by a user to a request, that specifies which servers can process that request.

**server data area.** The area of ECSA into which NetView FTP places information about a server or servers.

**server group.** A group of servers (logical units).

**server group table.** A data set that specifies which servers make up each server group, and that contains information about each server.

**server modification area.** An area of storage that contains the modifications to a server's session parameters.
**session.** In SNA, a logical connection between two network-addressable units.

**SFS.** Shared file system.

**SFS directory.** A group of files. SFS directories can be arranged to form a hierarchy in which one directory can contain one or more subdirectories as well as files.

**shared file pool.** See file pool.

**shared file system.** A part of CMS that lets users organize their files into groups known as directories, and selectively share those files and directories with other users.

**single mode.** A server running mode in which a server stops running after it has transferred a file (or attempted to transfer a file and failed).

**slot.** A space in the request queue directory that is able to hold a request control element (RCE).

**SMA.** Server modification area.

**SMF.** System management facilities.

**SMS.** Storage Management Subsystem.

**SNA.** Systems Network Architecture.

**SNA compaction.** The transformation of data by packing two characters in a byte that normally would only hold one character.

**SNA compression.** The replacement of a string of up to 64 repeated characters by an encoded control byte to reduce the length of the string.

**SNA network.** In SNA, the part of a user-application network that conforms to the formats and protocols of Systems Network Architecture. It enables reliable transfer of data among end users and provides protocols for controlling the resources of various network configurations. The SNA network consists of network addressable units, boundary function components, and the path control network.

**SNA node.** A node that supports SNA protocols.

**socket.** In the AIX operating system: (1) A unique host identifier created by the concatenation of a port identifier with a TCP/IP address. (2) A port identifier. (3) A 16-bit port number. (4) A port on a specific host; a communications end point that is accessible through a protocol family’s addressing mechanism. A socket is identified by a socket address. See also socket address.

**socket address.** In the AIX operating system, a data structure that uniquely identifies a specific communications end point. A socket address consists of a port number and a network address. It also specifies the protocol family.

**SRMU.** Statistics report message unit.

**special file.** In the AIX operating system, a file that defines a FIFO (first-in, first-out) file or a physical device.

**SSCP.** System Services Control Point.

**statistics report message unit.** A message unit sent by the target (receiver of the file), at the end of the file transfer.

**status.** The state of a request in the request queue (MVS, VSE, or VM) or request database (OS/400). In NetView FTP for MVS, VSE, or VM, the possible statuses are waiting, active, and finished. In NetView FTP/400, the possible statuses are held, waiting, active, finished, and failed.

**status data area.** The area of ECSA into which NetView FTP places details of the status of a server or servers.

**Storage Management Subsystem.** An MVS subsystem that helps automate and centralize the management of DASD storage. SMS provides the storage administrator with control over data class, storage class, management class, storage group, and ACS routine definitions.

**submit (a request).** To give (a request) to NetView FTP so that NetView FTP can add it to the request queue.

**superuser.** In the AIX operating system, the user who has unrestricted authority to access and modify any part of the operating system, usually the user who manages the system.

**supervisor call instruction.** An instruction that interrupts a running program and passes control to the supervisor so that the supervisor can perform the service indicated by the instruction.

**SVA.** Shared Virtual Area.

**SVC.** Supervisor call instruction.

**symbolic constant.** A data item that has an unchanging, predefined value.

**system authorization facility.** At an MVS or VM location, a generic interface to security products that is provided by the operating system. In this way, an installation has the possibility to run a security program, such as IBM RACF.
System management facilities. An optional control program for MVS that provides the means for gathering and recording information that can be used to evaluate system usage.

system services control point. In SNA, a focal point within an SNA network for managing the configuration, coordinating network operator and problem determination requests, and providing directory support and other session services for end users of the network. Several SSSCPs, cooperating as peers, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units within its domain.

Systems Network Architecture. The description of the logical structure, formats, protocols, and operating sequences for transmitting information units through, and for controlling the configuration and operation of, networks. The layered structure of SNA allows the origin and ultimate destination of information to be independent of and unaffected by the SNA network services and facilities used to transfer that information.

table display panel. A panel that contains a scrollable list.

Target Information Message Unit. A message unit sent by the receiving node after it receives an SDMU. A TIMU updates the original request, to inform the sender where to start or restart sending, and, to convey statistical information.

TCP. Transmission Control Protocol.

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

TIMU. Target Information Message Unit.

token-ring network. A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

Transfer Request Message Unit. A message unit used to send or receive a file, or to restart a previously interrupted file transfer.

Transmission Control Protocol. A communications protocol used in Internet and in any network that follows the U.S. Department of Defense standards for inter-network protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

TRMU. Transfer Request Message Unit.

unattended mode. An operating mode of NetView FTP for Workstations that assumes that a user is not available at the workstation, for example, to load devices such as diskettes or tapes. Contrast with attended mode.

unused slot. A slot that does not contain a request control element (RCE).

user exit. A point in an IBM-supplied program at which a user-exit routine is given control.

user interface. Hardware, software, or both that allows a user to interact with and perform operations on a system or program.

user query command. A type of command that causes NetView FTP to retrieve information about the requests in the request queue; the information retrieved is intended for users of NetView FTP. Contrast with administrator query command.

user query record. A record containing the information NetView FTP retrieves when a user issues a user query command. Contrast with administrator query record.

user-exit routine. An exit routine written by a user.

user-written file handler. An exit routine, written by a user, that gains access to a file and passes its records to NetView FTP, or that retrieves the records from NetView FTP and writes them to a file.

virtual storage access method. An access method for indexed or sequential processing of fixed- and variable-length records on direct-access storage devices. The records in a VSAM data set can be organized (1) in logical sequence by means of a key field (key sequence), in the physical sequence in which they are written in the data set (entry sequence), or (2) by means of a relative-record number.


VM node. A node with VM as its operating system.

VM system. A system with VM as its operating system.

VSAM. Virtual storage access method.

VSE node. A node with VSE as its operating system.

VSE system. A system with VSE as its operating system.

waiting request. A request that is waiting to be processed.

WAN. Wide area network.

Wide area network. A network that provides communication services to a geographic area larger than that served by a local area network and that may use or provide public communication facilities.

wildcard character. Either a question mark (?) or an asterisk (*) used as a variable in a file name or file name extension when referring to a particular file or group of files.

WTO. Write-to-operator.

XID. Exchange identification.

XnMU. Exit(n) message unit.
Bibliography

The NetView FTP Library

This manual is part of a library of publications that describe NetView FTP and explain how to use it. The publications in this library are:

**NetView File Transfer Program for VSE:**
- NetView FTP Licensed Program Specifications, GH12-5485
- NetView FTP VSE Installation, Operation, and Administration, SH12-5674
- NetView FTP Customization, SH12-5482
- NetView FTP Messages and Codes, SH12-5483
- NetView FTP Parameter Reference, SH12-6052

**NetView File Transfer Program for VM:**
- NetView FTP General Information, GH12-5480
- NetView FTP Licensed Program Specifications, GH12-5485
- NetView FTP VM Installation, Operation, and Administration, SH12-5676
- NetView FTP Customization, SH12-5482
- NetView FTP Messages and Codes, SH12-5483

**NetView File Transfer Program for OS/400:**
- NetView FTP General Information, GH12-54802
- NetView FTP V1 for OS/400 Licensed Program Specifications, GH12-5777
- NetView FTP V3 for OS/400 Licensed Program Specifications, GH12-6176
- NetView FTP V1 for OS/400 Installation and User's Guide, SH12-5776

**NetView File Transfer Program Version 2 for MVS:**
- NetView FTP Licensed Program Specifications, GH12-5485
- NetView FTP V2 MVS Installation, Operation, and Administration, SH12-5657
- NetView FTP Customization, SH12-5482
- NetView FTP Messages and Codes, SH12-5483
- NetView FTP Parameter Reference, SH12-6052

**NetView File Transfer Program Server for AIX,**
**NetView File Transfer Program Client for AIX:**
- NetView FTP Parameter Reference, SH12-6052

**NetView File Transfer Program Server/2,**
**NetView File Transfer Program Client/2**
**NetView File Transfer Program Client for DOS**
**and Windows:**
- NetView FTP Parameter Reference, SH12-6052

The unlicensed manuals with prefix SH are also available as softcopy on the following collection kits:

- IBM Networking Softcopy Collection Kit, SK2T-6012
- IBM Online Library Omnibus Edition: MVS Collection, SK2T-0710
- IBM Online Library Omnibus Edition: VM Collection, SK2T-2067
- IBM Online Library Omnibus Edition: VSE Collection, SK2T-0060
- IBM Online Library Omnibus Edition: AIX Collection, SK2T-2066

---

2 NetView FTP/400 V1 only.
Index

Special Characters
/etc/rc.tcpip  61

A
about NetView FTP AIX  71
access mode, file  75
access of root user  41
access of superuser  41
access-security parameter  90, 92
address, workstation  90, 92, 97
addressing a responder component  4
allocation, dynamic  74
allocation, space  74
APPC configuration, sample profiles  111
APPC conversation security parameter  90, 92
attributes, file access mode  75
authenticate the requesting user  85
authorization
  file access  85
automatic allocation retry  83
automatic transfer restart  83

B
basket directory  85
BIN2BINX  50, 109
built-in client  1
byte-oriented file handling  72

C
CCSID  78
CDRA  78
character data conversion  78
character data representation architecture  78
checking the NetView FTP status  65
checkpointing  84
clients, maximum number of  39
coded character set identifier  78
coding control statements, rules  69
combinations of file handling modes  72
command reference  89
communication device configuration  17
communication path  26
communication protocol  37
compression  78
configuration
  AIX communication device  17
  sample profiles for APPC  111
connection to server failed  101
customizing NetView FTP AIX  11
data compression  78
default directory
  for incoming files  37
  for outgoing files  38
destination ID  90, 91
diagnosis  99
dynamic allocation  74
dynamic creation  74
end-of-file character  72
end-of-processing option
  NOT_SUCCESSFUL  75
  NOT_YET_SUCCESSFUL  75
  SUCCESSFUL  75
error description  101
error recovery
  automatic allocation retry  83
  automatic transfer restart  83
  checkpointing  84
file access  74
file access mode  75
file access mode attributes  75
file allocation, dynamic  74
file creation, dynamic  74
file handling
  byte-oriented  72
  mode  72
  record-oriented  72
file names  74
file processing option
  APPEND  75
  REPLACE  75
file status option
  MAY_EXIST  75
  MUST_EXIST  75
  MUST_NOT_EXIST  75
file transfer
  in an IP network  86
  in an SNA network  86
  to and from NetView FTP AIX  45
file types
  host  71
file types (continued)
  on workstations 71
  supported 71
file-access authorization, check the 85
file-transfer request 2

G
getting started 45
glossary 123
group table, server 26
  guimsg.dat
  See user-interface log file

I
ibmnftp.ini 35
identification
  network 40
inbasket 37
initialization parameters
  overview 36
  tailoring the 35
installation verification 27
installing NetView FTP AIX 9
interface log file 75
introducing NetView FTP AIX 1
invoking
  the NetView FTP requester services 96
  the services window 96
IP server workstation ID 38
ipserverwstid 38

L
log file 76
log.dat
  See log file
logging 75
logical unit name 39
luname 39

M
maxclients 39
maximum number of
  clients 39
  transfers 39
maxtransfers 39
menu, SMIT 69
message format 78
modename 42

N
NetView FTP AIX customization 11
NetView FTP AIX installation 9
NetView FTP AIX requester component 62
NetView FTP AIX system log file 76
NetView FTP root services
  starting the responder component 63
  starting the server component 63
  starting the system daemon 63
  stopping the responder component 63
  stopping the server component 63
  stopping the system daemon 63
NetView FTP server component 61
NetView FTP system processes, purge 94
NetView FTP user services
  starting the requester services 66
NetView/6000, integration 86
network ID 40
nftp purge 89
nftp receive 62, 89
nftp send 62, 91
nftp start 93
nftp stop 63, 93
nftpdp purge 94
nftpdp start 61, 94
nftpdp startrsp 61, 94
nftpdp startsvn 61, 95
nftpdp stop 63, 95
nftpdp stoprsp 63, 96
nftpdp stopsrv 63, 96
nftpguic 96
nftpguir 68, 97
nftpguis 67, 97
nickname, workstation 90, 92, 97
notification 78

O
online documentation
  installing 10
  using 10
operation mode 40
opmode 40
outbasket 38

P
password handling 86
planning for NetView FTP AIX 8
port, server 42
post-transfer processing 74
prerequisites
  hardware, AIX 7
  software, AIX 7
protocol 37
public read access 85
purge NetView FTP 89
purge NetView FTP AIX system processes 94
purge NetView FTP daemon 94

R
RDF 2, 89, 91
RDF sample 108, 109, 110
read access 74
read access, public 85
receiving a file
via the command-line interface 89
via the graphical user interface 97
receiving file 2
receiving file name 74
receiving files from a remote node 62, 68
record delimiter 72
record-oriented file handling 72
recovery 83
remote communication 16
report file 76
report.dat
See report file
reporting 75
reporting a problem 104
request definition file 107
See also RDF
requester services 62, 66, 67, 68
requesting transfer node 2
responder component 61
responder component report file 75
responder service 61
responder-component log file 75
responding transfer node 2
restart point 84
restart, transfer 83
retry, allocation 83
retryattempts 40
retrydelay 41
return codes
file transfer 100
interface 99
RFILEID 89, 91
RMTNODE 90, 91
RMTWSTID 90, 92, 97
root access 41
root services 63
RSECURP 92
rules for coding control statements 69

S
scope of security 41
SECAPPC 90, 92
secpar 41
security
for NetView FTP AIX 85
security (continued)
for systems other than NetView FTP AIX 86
security scope 41
sending a file
via the command-line interface 91
via the graphical user interface 97
sending file 2
sending file name 74
sending files to a remote node 62, 67
server group table 26
server log file 75
server port 42
server report file 75
server workstation ID 38
serverport 42
SFILEID 89, 91
SMIT menu entries 69
SNA gateway services 61
SNA mode name 42
SNA Services/6000 17
space allocation 74
SSECURP 90
starting
NetView FTP AIX 61
NetView FTP AIX requester component 62
NetView FTP AIX system daemon 61
NetView FTP server component 61
system daemon 61
starting the system from the command line 61
starting, from the command line
NetView FTP AIX 93
NetView FTP AIX responder component 94
NetView FTP AIX system daemon 94
NetView FTP Server AIX gateway services 95
starting, via the graphical user interface
the NetView FTP requester services 96
the NetView FTP responder component 96
the NetView FTP server component 96
the NetView FTP system daemon 96
the NetView FTP user services 96
status of the NetView FTP system 65
stopping
NetView FTP AIX 63
NetView FTP AIX system daemon 63
responder component 63
server component 63
stopping the system from the command line 63
stopping, from the command line
NetView FTP AIX 93
NetView FTP AIX responder component 96
NetView FTP AIX system daemon 95
NetView FTP Server AIX gateway services 96
system log file 76
system status 65
T

table, server group 26
trace 42
transfers, maximum number of 39
TXT2ESDS 54, 110

U

umask 43
user ID
  root 41
user interface reporting 77
user log file 75
user notification 78
user report file 75
user services 66
user-interface log file 75
using NetView FTP AIX 61
using the command-line interface 61
using the graphical user interface 63

V

verification
  starting a NetView FTP client environment 33
  starting the NetView FTP responder component 30
  starting the NetView FTP server component 28
  starting the NetView FTP system daemon 27
verify the requesting user 85
verifying the installation 27

W

wait time 83
working with request definition files 69
workstation address 90, 92, 97
workstation ID 90, 92, 97
workstation ID, server 38
workstation nickname 90, 92, 97
write access 74
writing to tape 74

X

XBIN2BIN 46, 108
Your comments, please ...

NetView
File Transfer Program
for Workstations: AIX
Installation and User’s Guide
Publication No. SH12-6187-00

Use this form to tell us what you think about this manual. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

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. This form is provided for comments about the information in this manual and the way it is presented.

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 mail this form to us, be sure to print your name and address below if you would like a reply.

You can also send us your comments using:

- A FAX machine. The number is: +49–7031–166609.
- Internet. The address is: gadlid@sdfvm1.vnet.ibm.com.
- IBMLink. The address is: SDFVM1(GADLID).
- IBM Mail Exchange. The address is: DEIBM3P3 at IBMMAIL.
  Please include the title and publication number (as shown above) in your reply.

Name

Address

Company or Organization

Phone No.
Program Numbers: 5765-435 (Server for AIX)
               5622-242 (Client for AIX)

Printed in Denmark by IBM Danmark A/S