



System i
Networking
Trivial File Transfer Protocol

Version 5 Release 4





System i
Networking
Trivial File Transfer Protocol

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 9.

Fifth Edition (February 2006)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 2000, 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Trivial File Transfer Protocol	1
Printable PDF	1
Configuring TFTP for clients	1
Changing TFTP attributes	2
Server ports and client ports	3
TFTP Transfer Size option	3
TFTP Subnet Broadcast option	4
Client-to-server TFTP Read Request options	5
Server-to-client TFTP option acknowledgment	6

Server-to-client broadcast data packets.	7
Exit points for controlling TFTP server.	7

Appendix. Notices	9
Programming Interface Information	10
Trademarks	11
Terms and conditions	11

Trivial File Transfer Protocol

Trivial File Transfer Protocol (TFTP) is a simple protocol that provides basic file transfer function with no user authentication.

TFTP is intended for applications that do not need the sophisticated interactions that File Transfer Protocol (FTP) provides. TFTP, together with Bootstrap Protocol (BOOTP), provides support for clients of a System i™ product. They also provide support for other clients that use the TFTP and BOOTP protocols.

You can work with TFTP server properties through iSeries™ Navigator, the graphical user interface (GUI) for the i5/OS® operating system.

Related concepts

Getting to know iSeries Navigator

Printable PDF

Use this to view and print a PDF of this information.

To view or download the PDF version of this document, select TFTP (about 182 KB).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html) .

Configuring TFTP for clients

To allow clients to use the Trivial File Transfer Protocol (TFTP) server, you must ensure that the QTFTP profile has authority to access the directories and files that the clients access through the TFTP server. You also need to set the TFTP server attributes to allow the required client requests.

When configuring TFTP for use by clients, first determine the directories and files that the clients are using. For this example, the clients use the TFTP server to read files from the directory `/netpc/bin/system`.

1. Use the Create Directory (MKDIR) command with an argument of `/netpc` to create the directory `/netpc`.
`MKDIR (netpc)`
2. Specify the Work with Object Links (WRKLNK) command with an argument of `/netpc`.
`WRKLNK (netpc)`
3. Specify option 9 (Work with Authority) to display the current authorities.

4. For the *PUBLIC user, specify option 2 (Change user authority), and specify *NONE for New data authorities.

This ensures that the file is not open to the public.

5. To add a user on the Work with Authority menu, specify the following on the first line: 1 for Opt, QTFTP for User, and *RX for Data Authority.

Press Enter.

6. Press F5 (Refresh) to refresh the menu. You see the user ID *PUBLIC with a data authority of *EXCLUDE, the user ID QTFTP with a data authority of *RX, and your own user ID with a data authority of *RWX.

Use the MKDIR command to create the following directories:

```
/netpc/bin  
/netpc/bin/system
```

Each directory inherits the authority of the parent directory and has the owner added implicitly as a user with *RWX authority. Copy any files that the client requests to the netpc/bin/system subdirectory. You can copy the files in various ways, such as using the COPY command, File Transfer Protocol (FTP), or iSeries Access. You must ensure that the QTFTP profile has *R authority to each file that the client requests. To set the authorities for the files, use the WRKLNK command and option 9 (Work with Authority).

7. Specify the Change TFTP Attributes (CHGTFTPA) command or press F4 (Change TFTP Attributes).
8. Change the Alternate source directory to /netpc/bin/system and press Enter.
This allows the TFTP server to request any file with the appropriate authority settings, including the directory /netpc/bin/system in its path.
9. To have the changes take effect, stop the TFTP server with ENDTCPSPVR *TFTP and restart it by using STRTCPSVR *TFTP.

Changing TFTP attributes

To change the Trivial File Transfer Protocol (TFTP) server attributes, use the Change TCP/IP TFTP Attributes (CHGTFTPA) command.

The following are two different ways to get to this command prompt:

- Specify the CHGTFTPA command.
- Select option 3 on the Configure TCP/IP Applications (CFGTCPAPP) display.

Note: You must have *IOSYSCFG special authority to make changes to the TFTP attributes with the CHGTFTPA command.

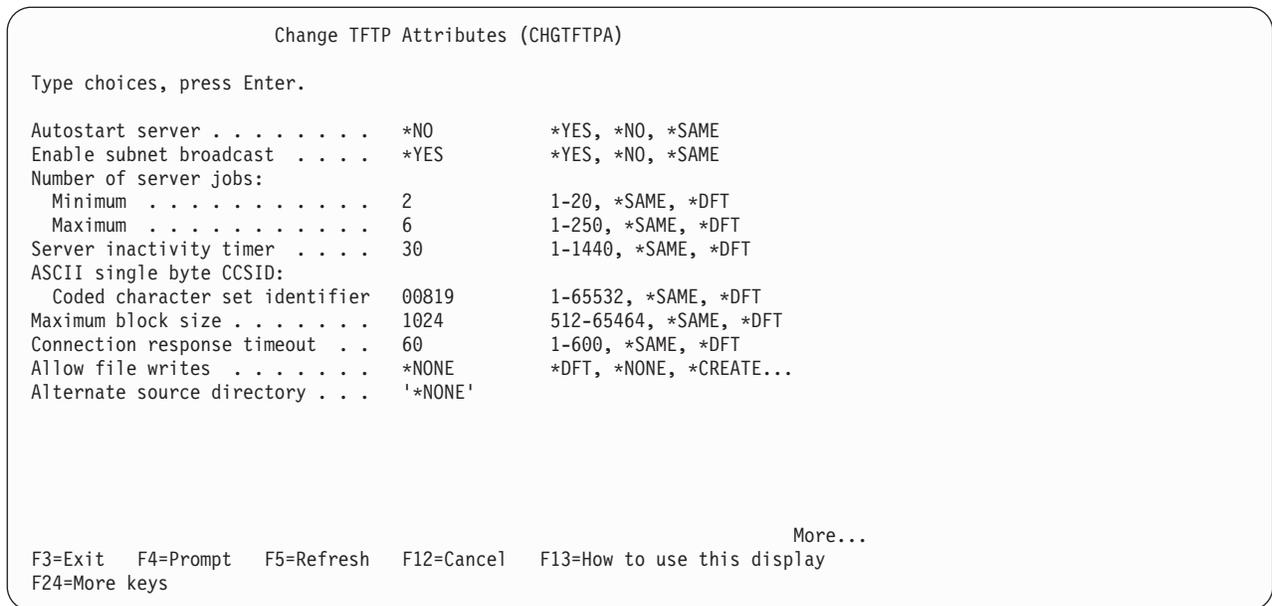


Figure 1. Change TFTP Attributes (CHGTFTP) – Display 1

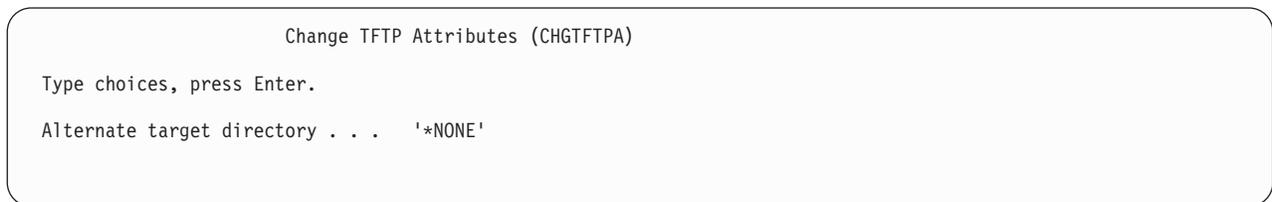


Figure 2. Change TFTP Attributes (CHGTFTP) – Display 2

Server ports and client ports

The Trivial File Transfer Protocol (TFTP) server uses a subnet-directed broadcast address as the destination address.

It also uses a well-known port as the port of datagrams sent to clients that have requested the subnet broadcast option. The clients listen for and receive datagrams on the well-known port. The keyword for the well-known port is `subntbcst_tftp`, and its decimal value is 247.

The TFTP server sends subnet-directed broadcast datagrams to clients that request the subnet broadcast option. The source ports from which the TFTP server sends these datagrams do not have to be unique. They can be arbitrarily allocated.

Some routers filter or block subnet-directed broadcast datagrams. In support of router filters, you can define restricted ports for the QTFTP profile. If you define restricted ports for the QTFTP profile, the TFTP server uses only the defined restricted ports as the source ports for the subnet-directed broadcast datagrams. Network administrators define router filtering rules to allow subnet-directed broadcast datagrams to pass through router filters based on the source port of subnet-directed datagrams being one of the restricted ports defined for the QTFTP profile.

TFTP Transfer Size option

By using the Transfer Size option, the client can determine how much data is transferred on a read request (RRQ).

This is useful for requesting a subnet broadcast of a file. The client finds the size of the buffer it needs in order to store the file in memory. Drawing from this block size, the client determines the number of blocks for the transfer. The number of blocks is helpful information for tracking the blocks that have been received. You can also use it for the last block acknowledgment (ACK), which must be sent to end a transfer normally. Without the Transfer Size option, determining the size and the last block of the transfer requires the client to wait for a block to be received that is smaller than the block size of the transfer.

Note: For files transferred in `netascii` mode, this option might not be as useful if you are converting the data during the transfer in a way that changes its size. Also, the system might require additional processing time to determine the transfer size due to conversion of the file to the appropriate coded character set identifier (CCSID).

TFTP Subnet Broadcast option

Broadcast storms are a performance problem that might occur when large numbers of systems start from the network. Trivial File Transfer Protocol (TFTP) Subnet Broadcast option helps solve this problem.

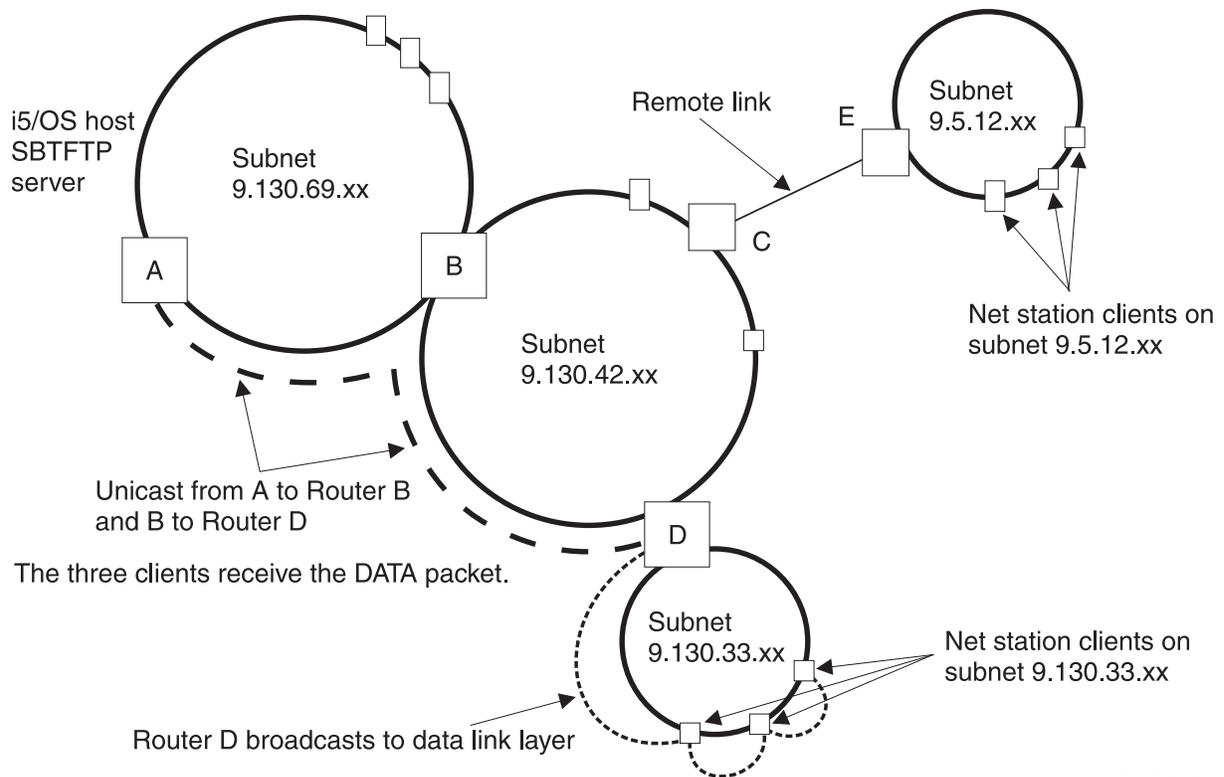
These broadcast storms occur when large numbers of clients request their boot code at the same time. When hundreds of systems are started, the same data must be routed through each hop in the network between each system and the TFTP server.

The TFTP Subnet Broadcast option allows the server to broadcast the boot code to systems on a subnet basis. Using subnet-directed broadcast, Subnet Broadcast data packets are transmitted between routers until they reach the subnet on which the systems reside. The packets transmission is unicast. At this point, the router at the destination subnet broadcasts the data packets to the systems on the subnet. Disinterested hosts on the subnet throw the data packets away. The packets are typically thrown away by the host's IP layer after it determines that no applications are interested in receiving data on the port to which the broadcast was directed. See Figure 3 on page 5 for an illustration of a subnet-directed broadcast. This solution can drastically reduce the network traffic as well as the time that it takes many systems to start (when starting simultaneously).

The TFTP Subnet Broadcast option enables clients to join a broadcasting file group. It also allows clients to receive all subsequent blocks for a file until the client becomes the master client. A client becomes the master client when it receives an Option Acknowledge (OACK) packet from the TFTP server that indicates that it is the master client. A client must keep track of blocks that it receives. After a client becomes the master client, it can request the blocks that it has not received. The master client requests blocks by sending ACK packets that include the block number of the block before the block that the master client requires. For example, if the client wants block 5, it sends an ACK with a block number of 4.

When a client receives an OACK packet that indicates that it is the master client, the client must send an ACK that requests the first block it requires. From then on, the client must request blocks in ascending, but not necessarily consecutive order. A master client continues to send ACK packets to the server to indicate the next block that it requires. When the master client receives all of the blocks it requires, it sends an ACK with the number of the last block on the file being transferred. After the server receives an ACK with the last block number of the file being transferred, the transfer to the client sending the ACK is considered complete. A client can stop its transfer at any time by sending an ACK for the last block or by sending an Error (ERR) packet. A client can end this transfer regardless of whether it is the master client.

Note: This TFTP Subnet Broadcast option is designed to improve simultaneous transfer of large files to multiple clients on a common subnet. This option does not help with files that require only a few blocks to transfer or single client transfers.



RV4E002-3

Figure 3. Example of broadcasting over subnets

Client-to-server TFTP Read Request options

This information includes the client-to-server Trivial File Transfer Protocol (TFTP) Read Request options and a description of their use.

To view the standard TFTP request parameters and their meanings, refer to Internet Request for Comments (RFC) 1350. For more information about the TFTP options, see RFCs 1782, 1783, and 1784. Internet RFC 2090 describes the TFTP multicast option, which has some similarities to the Subnet Broadcast option. However, the TFTP Multicast option is not supported at this time. The TFTP Multicast option RFC is mentioned here as a reference to help understand the Subnet Broadcast option.

Here is a list of supported options and their descriptions:

blksize

Null (0h) terminated keyword `blksize` that is followed by the requested block size and represented as a null-terminated ASCII string. This option requests a block size for the requested file transfer instead of using the default of 512.

sbroadcast

Null-terminated keyword `sbroadcast` that is followed by the subnet mask of the subnet to which the client is connected. This option indicates that the client wants to participate in a subnet-directed broadcast group. The subnet mask that is included with this option is used with the client's IP address to determine the client's subnet address.

tsize

Null-terminated keyword `tsize` that is followed by a null-terminated ASCII representation of 0 (30h). This option is a request for the server to return the file size in an Option Acknowledgment (OACK).

Related reference

“Server-to-client TFTP option acknowledgment”

The Trivial File Transfer Protocol (TFTP) server sends an option acknowledgment (OACK) to a client in response to either a read request or a write request that includes additional TFTP options as described in client-to-server TFTP Read Request (RRQ) options.

Server-to-client TFTP option acknowledgment

The Trivial File Transfer Protocol (TFTP) server sends an option acknowledgment (OACK) to a client in response to either a read request or a write request that includes additional TFTP options as described in client-to-server TFTP Read Request (RRQ) options.

An OACK that the servers sends in response to a transfer request includes only responses to requested options that the server supports. The server can also send an OACK to a client subsequently to the start of a subnet broadcast transfer. This is done to indicate to the client whether it is the master client in a subnet broadcast file group. An OACK packet that the server sends subsequently to the start of a subnet broadcast transfer includes the sbroadcast option.

Here is a list of supported options and their descriptions:

blksize

Null (0h) terminated blksize keyword that is followed by the block size that is used for this file transfer. It is represented as a null-terminated ASCII string. This is the response to a requested block size, and the value returned here can be less than the requested block size. The server determines the block size for the transfer based on the requested block size, the maximum configured block size, and possibly the subnet broadcast transfers that are already in progress.

sbroadcast

Null-terminated sbroadcast keyword that is followed by a null-terminated ASCII string that includes the following fields separated by commas:

port

The ASCII representation of the port to which the subnet-directed broadcast datagrams are broadcast. This is the well-known port that is registered with the Internet Assigned Number Authority (IANA) with the keyword of subntbcst_tftp and a decimal value of 247. This field might be empty in OACK packets that the server sends subsequently to the start of a subnet broadcast transfer.

sbid

The ASCII representation of a decimal number that is called the subnet broadcast identifier. Possible values are 0 through 4 294 967 295 (FFFFFFFFh). This is used along with the server source port to determine if a subnet-directed broadcast datagram is part of a requested transfer. This field can be empty in OACK packets that the server sends subsequently to the start of a subnet-based broadcast transfer.

mc

This is either an ASCII (31h) 1 or ASCII 0 (32h) to indicate to the client whether it is currently the master client. A value of 1 indicates that the client is the master client, and a value of 0 indicates that the client is not the master client.

In response to an OACK, the master client must send an ACK to the server. The master client sets the block number in this ACK to the number of the block before the first block that is required by the master client.

The master client acknowledges subnet broadcast data (BDATA) packets by sending an ACK to the server. The master client sets the block number in this ACK to the block before the current block that the master client requires.

Clients that are not indicated as being the master client respond to an OACK packet with an ACK that has the block number set to zero.

Note: The block number in ACK packets is the 2-byte binary representation of the number in network byte order.

tsize

The null-terminated `tsize` keyword that is followed by the null-terminated ASCII representation of the decimal number that represents the file size of the requested file. The client uses this information to ensure that it has enough space to store the file and to determine the last block number of the file.

Note: The client can also determine the file size and last block of a transfer when it receives a block that contains less data than the block size.

Related concepts

“Client-to-server TFTP Read Request options” on page 5

This information includes the client-to-server Trivial File Transfer Protocol (TFTP) Read Request options and a description of their use.

Server-to-client broadcast data packets

This information explains the fields in a broadcast data (BDATA) packet in detail.

block#

2-byte binary number in the network byte order that indicates the number of a particular block of data.

sbid

4-byte binary number in the network byte order that is called the *subnet broadcast identification*. This must be compared with the `sbid` that was returned in the OACK response to a read request (RRQ) with the Subnet Broadcast option. Along with the source port, this uniquely identifies a Subnet Broadcast File Transfer. The source port of the BDATA packet must be compared with the source port of the initial OACK packet that was received for this transfer. Only BDATA packets that match on both the SBID and source ports are considered part of the requested transfer. All other BDATA packets must be ignored.

data

This is the data for this block of the file transfer. With the exception of the last block of the file, the size of the data is equal to the block size for the transfer. The last block of the file must be less than the block size, even if it means that the length of the data in the last block is zero. However, the server might not be done broadcasting blocks after the last block of the file is broadcast. Control can be transferred to another client in the subnet broadcast file group that has not yet received all the blocks in the file.

Exit points for controlling TFTP server

An *exit point* is a specific point in the Trivial File Transfer Protocol (TFTP) program where control can pass to an exit program. An *exit program* is a program to which the exit point passes control. With the use of exit programs, the experienced programmer can create customized processing when an application is running.

If the TFTP server finds a program registered to one of the exit points for the system, it calls that program using parameters that are defined by the exit point.

For each exit point, there is an associated programming interface, called an *exit point interface*. The exit point uses this interface to pass information between the TFTP application and the exit program. Each exit point has a unique name. Each exit point interface has an exit point format name that defines how information is passed between the TFTP application and the customer-written exit program.

Different exit points can share the same exit point interface. When this is the case, multiple exit points can call a single exit program.

To allow the exit programs to work properly, you must install and register your exit point programs. If your programs are no longer needed, you must properly remove the exit point programs to prevent their future functioning.

Exit point performance

The following table lists exit points that give you additional control over the TFTP server.

Table 1. TFTP exit point and format

TCP/IP exit point	Application	Exit point format	Brief description
QIBM_QTOD_SERVER_REQ	TFTP	VLRQ0100	The TCP/IP request validation exit point provides additional control for restricting an operation.

Notes:

- The same interface format is used for request validation for the File Transfer Protocol (FTP) client, FTP server, REXEC server, and TFTP server. This allows the use of one exit program for request validation of any combination of these applications.
- The same interface format is used for server log-on processing for the FTP server and TFTP server applications. This allows the use of one exit program to process log-on requests for both of these applications.

Related concepts

Using server exit programs

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

- | The licensed program described in this information and all licensed material available for it are provided
- | by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement,
- | IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This TFTP publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- | i5/OS
- | IBM
- | IBM (logo)
- | iSeries
- | System i

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA