Tekelec EAGLE® 5
Integrated Signaling System

FTP-Based Table Retrieve Application (FTRA) User Guide

910-4919-001 Revision A
February 2007

TEKELEC

Copyright 2007 Tekelec.
All Rights Reserved
Printed in U.S.A.

Notice

Information in this documentation is subject to change without notice. Unauthorized use or copying of this documentation can result in civil or criminal penalties.

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks

The Tekelec logo, EAGLE, G-Flex, G-Port, IP^7, IP^{7}Edge, IP^7 Secure Gateway, and TALI are registered trademarks of Tekelec. TekServer is a trademark of Tekelec. All other trademarks are the property of their respective owners.

Patents

This product is covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:

5,008,929, 5,953,404, 6,167,129, 6,324,183, 6,327,350, 6,456,845, 6,606,379, 6,639,981, 6,647,113, 6,662,017, 6,735,441, 6,745,041, 6,765,990, 6,795,546, 6,819,932, 6,836,477, 6,839,423, 6,885,872, 6,901,262, 6,914,973, 6,940,866, 6,944,184, 6,954,526, 6,954,794, 6,959,076, 6,965,592, 6,967,956, 6,968,048, 6,970,542

Ordering Information

For additional copies of this document, contact your sales representative.

Table of Contents

User Guide Conventions 2

Overview 2

Hardware and Software Requirements 4

Using the FTRA Application 6

Software Installation 7

FTRA Initialization 20

Exit the FTRA 21

STP Connection Configuration Menu 23

Adding an STP Configuration Record 26

Displaying an Existing STP Configuration Record 31

To Use the STP Name Drop Down List 31

To Enter the STP Name 33

Testing an STP Configuration Record 35

Connectivity Test Log File Menu 36

Clearing the Connectivity Test Log Display 37

Printing the Connectivity Test Log 37

Saving the Connectivity Test Log to a File 39

Closing the Connectivity Test Log Window 40

Modifying an Existing STP Configuration Record 40

Deleting an STP Configuration Record 43

Selecting the Current STP 43

Secure EAGLE 5 ISS Host Key Provisioning 46

FTP Server Configuration 52

Retrieve Database Tables from an STP 57

Retrieve Tables Window 57

Retrieve Tables Log 72

Retrieve Tables Log File Menu 74

Clearing the Retrieve Tables Log Display 74

Printing the Retrieve Tables Log 75
Saving the Retrieve Tables Log to a File 76
Closing the Retrieve Tables Log Window 78

Command Line Interface 79

Updating Database Tables in the Selected STP 87

Validating a Command File 88
Update Validation Complete Window 93
Sending a Command File to the Selected STP 94
Stop Without Sending or Editing a Command File 95
Editing a Command File 95

Update Tables Log Window 98

File Menu in the Update Tables Log Window 102
Clearing the Update Tables Log Display 103
Printing the Update Tables Log 104
Saving the Update Tables Log to a File 105
Closing the Update Tables Log Window 106

The System Log 107

File Menu in the System Log Window 107
Clearing the System Log Display 108
Printing the System Log 109
Saving the System Log to a File 110
Closing the System Log Window 111

About FTRA Window 112

FTRA release 4.0 112
Change summary. 112
RTRV-STP Command. 113
Retrieve Tables 113
RTRV-STP Command Retrieval Session 113
Command line interface 115
Version Information 116

SSH/SFTP Error Codes 118

Troubleshooting Procedures 134
FTP Server Verification 134
SFTP /SSHD Server Verification 134
Connectivity Test – I 134

Connectivity Test - II 135
Network Outage Trouble Shooting 136
SSH/SFTP/SFTPD/SSHD Protocol Troubleshooting 137

Index

List of Figures

Figure 1. Explore the FTRA CD Using Windows Explorer 8
Figure 2. Add or Remove Programs Window 9
Figure 3. Select a Custom Installation 10
Figure 4. Java Runtime-Environment Install shield Wizard 10
Figure 5. Create a New Folder for FTRA Installation 11
Figure 6. Rename New Folder to ftra 12
Figure 7. Copy the ftra_install.exe File 13
Figure 8. Extract Program Files 13
Figure 9. Set the FTRA Environment Variables 14
Figure 10. Creating FTRA Shortcut - FTRA 4.0 16
Figure 11. FTP-Based Table Retrieve Application Window 20
Figure 12. File Menu in the FTP-Based Table Retrieve Application Window 21
Figure 13. Exit Confirmation Window 21
Figure 14. Exit Window 22
Figure 15. Edit Menu 23
Figure 16. STP Connection Configuration Menu Window (FTRA 4.0) 23
Figure 17. Invalid STP Name Error Message 26
Figure 18. Adding an STP Configuration Record (FTRA 4.0) 27
Figure 19. Invalid IP Address Error Message 28
Figure 20. Invalid STP User Name Error Message 28
Figure 21. Invalid STP Password Error Message 28
Figure 22. Invalid FTP User Name Error Message 29
Figure 23. Invalid FTP Password Error Message 29
Figure 24. STP Added Window 30
Figure 25. Selecting an STP Name from the STP Name Drop Down List (FTRA 4.0 31
Figure 26. STP Name Selected from the STP Name Drop Down List (FTRA 4.0) 32
Figure 27. Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 4.0) 33
Figure 28. STP Configuration Record (FTRA 4.0) 34

Figure 29. STP Name Does Not Exist Error Message 34
Figure 30. Connectivity Test Log Window with No Errors 35
Figure 31. Connectivity Test Log Window with Errors 36
Figure 32. Command Complete Connectivity Test Window 36
Figure 33. File Menu in the Connectivity Test Log Window 37
Figure 34. Print Window 38
Figure 35. Save Window 39
Figure 36. Saved File Confirmation Window 39
Figure 37. Modifying STP Configuration Record Parameters (FTRA 4.0) 41
Figure 38. STP Data Modified Window 42
Figure 39. Modify Warning Window 42
Figure 40. Delete STP Window 43
Figure 41. STP Selection Change Window 44
Figure 42. Current STP Selected (FTRA 4.0) 45
Figure 43. IP Address Warning Message 46
Figure 44. FTP Server Configuration Menu in the FTP-Based Table Retrieve Application Window 52
Figure 45. FTP Server Configuration Menu Window 53
Figure 46. Invalid IP Address Error Message 54
Figure 47. Select Starting Directory Window 54
Figure 48. Invalid Subpath Window 55
Figure 49. FTP Server Configuration Example 56
Figure 50. FTP Server Data Set Window 56
Figure 51. GTT Warning Window 57
Figure 52. Retrieve Tables Window 58
Figure 53. Retrieve Table Log - Release Not Compatible Error 60
Figure 54. Commands Menu in the FTP-Based Table Retrieve Application Window 61
Figure 55. Selecting a Command 61
Figure 56. Selecting a Range of Commands 62
Figure 57. Selecting Multiple Commands 63
Figure 58. Adding a Command to the Selected Commands Box 64
Figure 59. Adding a Range of Commands to the Selected Commands Box 65
Figure 60. Adding Multiple Commands to Selected Commands Box 66

Figure 61. Command Selected to be Removed in the Selected Commands Box 67
Figure 62. Command Removed from the Selected Commands Box 67
Figure 63. Command Data Stored Window 68
Figure 64. Retrieving Database Tables from the Local Database 69
Figure 65. Retrieve Tables Log Window - Processing Retrieve Request 70
Figure 66. Command Complete Window Without Errors 70
Figure 67. Command Complete Window With Errors 71
Figure 68. Retrieve Tables Log Window without Errors 72
Figure 69. Retrieve Table Log with Errors 73
Figure 70. Retrieve Table Log with the RTRV-STP Command 73
Figure 71. File Menu in the Retrieve Tables Log Window 74
Figure 72. View Menu 75
Figure 73. Print Window 76
Figure 74. Save Window 77
Figure 75. Saved File Confirmation Window 77
Figure 76. FTRA Windows Command Line Interface 80
Figure 77. FTRA Windows Command Line Interface to modify STP data. 80
Figure 78. FTRA UNIX Command Line Interface 81
Figure 79. FTRA UNIX Command Line Interface to modify STP data. 81
Figure 80. FTRA Windows Scheduled Task 82
Figure 81. FTRA Windows Scheduled Task to modify STP data 82
Figure 82. UNIX cron job scheduled via crontab (note: last line shows FTRA scheduled to run at 3am Monday through Friday 83
Figure 83. FTRA wrapper script example for Unix (might be necessary if running from cron) 83
Figure 84. FTRA wrapper script example on Unix for modifying STP configuration (might be necessary if running from cron) 84
Figure 85. Update Tables Window 87
Figure 86. Edit Menu 88
Figure 87. Select Window 90
Figure 88. Update Tables Window with a Command File Selected and Stop on Error Box Checked 91
Figure 89. Update Tables Log Window - Processing Retrieve Request 92
Figure 90. Must Enter Command Script File Name Message 92

Figure 91. Update Validation Complete Window without Errors 93
Figure 92. Update Validation Complete Window with Errors 94
Figure 93. Command Complete Window 94
Figure 94. Command File Editor Window 95
Figure 95. Command In progress, Cannot Close Window 96
Figure 96. Command File Editor with Invalid Command 96
Figure 97. File Menu in the Command File Editor Window 97
Figure 98. Command Complete Window 97
Figure 99. Update Tables Log Window after the Commit Command Completed 98
Figure 100. Update Tables Log 99
Figure 101. Update Tables Log with Stop on Error Box Checked in the Update Tables Window 100
Figure 102. Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window 101
Figure 103. File Menu in the Update Tables Log Window 103
Figure 104. View Menu 103
Figure 105. Print Window 104
Figure 106. Save Window 105
Figure 107. Saved Confirmation Window 106
Figure 108. System Log Window 107
Figure 109. File Menu in the System Log Window 108
Figure 110. View Menu 108
Figure 111. Print Window 109
Figure 112. Save Window 110
Figure 113. Saved Confirmation Window 111
Figure 114. Help Menu 112
Figure 115. Typical About FTRA Window 112
Figure 116. Retrieve Tables window with rtrv-stp command selected for retrieval. 113
Figure 117. Successful Retrieval Session for rtrv-stp command 114
Figure 118. Rtrv-stp Command unsupported on EAGLE release 114
Figure 119. STP data modified through CLI. 115
Figure 120. Invalid STP name 116
Figure 121. Invalid number of arguments. 116
Figure 122. About FTRA Display Window 117

List of Tables

Table 1. FTP-Based Table Retrieve Application Menu Description 20
Table 2. STP Connection Configuration Menu Description 24
Table 3. FTP Server Configuration Menu Window Descriptions 53
Table 4. Select Starting Directory Window Descriptions 55
Table 5. Retrieve Tables Window Description 59
Table 6. FTRA – Eagle Compatibility Matrix 86
Table 7. Update Tables Window Description 88
Table 8. Select Window Descriptions 90
Table 9. Update Validation Complete Window Description 93
Table 10. FTP/SFTP/SSH Error Codes 118
Table 11. Generic Network Error Codes 131
Table 12. TCP Fault Tolerance Table for FTP/SFTP 137

List of Acronyms

CSV	Comma Separated Value
FTP	File Transfer Protocol
FTRA	FTP-Based Table Retrieve Application
GPSM	General Purpose Service Module
IPSM	IP Services Module
PC	Personal Computer
STP	Signal Transfer Point
TDM	Terminal Disk Module
UIM	Unsolicited Information Message

User Guide Conventions

In order to clearly differentiate between references to objects, actions, literal entries, and user-supplied information, the following conventions are used in this user guide:

- Menu selections and buttons are shown in bold, and the steps in a menu path are represented with ">". For example:

  Select **Edit > STP Connection Configuration** from the menu.

  The **Add** button is not enabled when the **STP Connection Configuration** menu opens.

- Commands and entries that must be entered exactly as shown in this document are shown in the 10 point Courier bold font. For example:

  Using a text editor (such as Notepad) add the following lines to the AUTOEXEC.BAT file:
  SET FTRA_HOME="C:<*download_directory*>**"**
  SET JRE_HOME="C:\Program Files\Java\j2re1.4.0_01"

- User-specific information is shown in italics and enclosed in "<>". For example, the name of the folder you wish to use as the download directory in the previous example is shown as <*download_directory*>.

Overview

The FTP-Based Table Retrieve Application (FTRA) is designed in conjunction with the FTP Retrieve and Replace feature to transfer EAGLE 5 ISS database tables using an FTP session to a remote server for offline processing. The FTRA is a stand-alone application that interfaces with one or more STPs. Database tables can be retrieved from the EAGLE 5 ISS, using the EAGLE 5 ISS's retrieve commands. The output of these retrieve commands is converted to CSV (comma separated value) files. EAGLE 5 ISS commands in the form of a command file can be read into the FTRA where they are validated and sent to the selected STP. Logs are provided for event tracking and error message display.

The FTRA provides the following features through the use of a graphical user interface:

- STP Connection Configuration.
- STP Connectivity Test.
- FTP Server Configuration.
- Retrieving the EAGLE 5 ISS database tables with the results converted to CSV files.
- Automated or manual retrieval of database tables from multiple STPs with the command line interface. The results are converted to CSV files.
- Configuration provisioning for automated retrieval of database tables from multiple STPs.

- Validation of the command files before being sent to the STP
- Validation of STP database update command files using an offline database
- Command file editing
- Viewing the log files for event tracking and error message display.

Hardware and Software Requirements

To run the offline application, a workstation on the Windows or Unix platform is required.

The Windows workstation requires that the following hardware and software is installed:

- Operating system – Windows® 2000/XP or later[1]
- Processor speed – Pentium III, 750 MHz or faster
- RAM – Minimum 128 MB
- Disk Space – Minimum 500 MB + 500 MB per STP
- A CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java™ 2 Runtime Environment (JRE) 1.4.2 or later.[2]

The Unix workstation requires that the following hardware and software is installed:

- Operating system – Solaris 7 or later
- Processor speed – 500 MHz or faster
- RAM – Minimum 512 MB
- Disk Space – Minimum 500 MB + 500 MB per STP
- CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java™ 2 Runtime Environment (JRE) 1.4.2 or later

---

1 Windows is a registered trademark of Microsoft Corporation in the United States of America and/or other countries.

2 Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States of America and other countries. Tekelec is independent of Sun Microsystems, inc.

To configure the EAGLE 5 ISS for the FTP Retrieve and Replace feature, these requirements must be met:

- The IP User Interface feature is enabled and activated. The status of the IP User interface feature is shown in the EAGLE 5 ISS **`rtrv-ctrl-feat`** command output. If the IP User Interface feature is not enabled and activated, perform the "Activating Controlled Features" procedure in the *Database Administration Manual - System Management* and enable and activate the IP User Interface.
- Up to three IPSMs are installed and configured in the database. The IPSMs are shown with the entry IPSM in the **`TYPE`** column of the EAGLE 5 ISS **`rtrv-card`** output. If IPSMs are not shown in the **`rtrv-card`** output, perform the "Adding an IPSM" procedure in the *Database Administration Manual - System Management* and add the IPSMs.
- If the EAGLE 5 ISS is running release 30.2 or greater, and you wish to use a secure connection for the FTRA to EAGLE 5 ISS communication, make sure the Eagle OA&M IP Security Enhancements feature is enabled and activated. This can be verified by entering the **`rtrv-ctrl-feat`** command at the EAGLE 5 ISS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the "Activating the Eagle OA&M IP Security Enhancements Controlled Feature" procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature.
- GPSM-II cards must be installed in card locations 1113 and 1115. The GPSM-II cards in card locations 1113 and 1115 are shown with the entry GPSM in the TYPE column of the EAGLE 5 ISS **`rtrv-card`** output.
- TDMs, P/N 870-0774-10 or later, installed in card locations 1114 and 1116. Visually verify that these TDMs are installed in the EAGLE 5 ISS.

CAUTION: Never install or initialize MCAP cards in card locations 1113 and 1115 after GPSM-II cards have been installed and features that require GPSM-II cards have been provisioned. Attempting to initialize MCAP cards with features requiring GPSM-II cards will cause a system outage. Before replacing existing GPSM-II or MCAP cards (if the EAGLE 5 ISS currently has MCAP cards installed) in card locations 1113 or 1115, or replacing TDMs in card locations 1114 and 1116, contact the Customer Care Center at one of the following locations:

- Tekelec, UK

Phone: +44 1784 467 804
Fax: +44 1784 477 120
Email: **`ecsc@tekelec.com`**

- Tekelec, USA

Phone (within the continental US) 888-367-8552 (888-FOR-TKLC)
(outside the continental US) +1 919-460-2150.

Email: **support@tekelec.com**.

Using the FTRA Application

The following is an overview of the steps required to use the FTRA application.

1. Install the FTRA software on the PC (personal computer) – refer to the "Software Installation" section on page 7.

2. Start the FTRA application – refer to the “FTRA Initialization” section on page 20.

3. Select the current STP that the database tables will be retrieved from, or that the command files will be sent to – refer to the “Selecting the Current STP” procedure on page 43.

   If you wish to use another STP, and that STP is not shown in the STP Name field of the **STP Connection Configuration** window, refer to the “Adding an STP Configuration Record” procedure on page 26 and add the new STP.

4. Before database tables can be retrieved from the EAGLE 5 ISS, or command files can be sent to the EAGLE 5 ISS, the FTP server configuration information for that EAGLE 5 ISS must be configured – refer to the “FTP Server Configuration” section on page 52.

5. To retrieve database tables from the selected STP, select the commands for the database tables you wish to retrieve in the Retrieve Tables Window – refer to the “Retrieve Database Tables from an STP” section on page 57.

6. To send commands to the selected STP, go to the Update Tables Window and select the command file to be sent, or create a command file – refer to the “Updating Database Tables in the Selected STP” section on page 87.

7. Exit the FTRA application – refer to the “Exit the FTRA” section on page 21.

Software Installation

The FTRA software can be installed locally or remotely through a LAN. The software installation can be accomplished in 5 to 10 minutes if the Java™ 2 Runtime Environment has been previously installed.

The JRE version 1.4.2_03 is provided in the FTRA 4.0 installation package. Installation procedures are also described in terms of the JRE version 1.4.2_03. However, you can install JRE version 1.4.2 or higher if you are downloading JRE from Sun Microsystems' web site.

Java™ 2 Runtime Environment software can be installed from FTRA CD or download the Java™ 2 Runtime Environment software from Sun Microsystems' web site (for installation on the Unix platform). Should you decide to download the software from Sun Microsystems' web site, the software installation can take from 30 to 90 minutes, depending on the download speed of your Internet connection. The FTRA is not providing service during this time. If the FTRA is being upgraded, it will not be necessary to re-create directories or environment variables that already exist.

If the FTRA software is being installed for the first time, perform one of these procedures:

- "- FTRA Software Installation on Windows" on page 7
- "– FTRA Software Installation on Unix" on page 16

If the FTRA software is being upgraded to FTRA 4.0, perform one of these procedures:

- "– Upgrade to FTRA 4.0 on Windows" on page 18
- "– Upgrade to FTRA 4.0 on Unix" on page 19

Procedure - FTRA Software Installation on Windows

1. Place the FTRA CD in the CD-ROM drive.

a. To see the contents of the FTRA CD, double-click on the **My Computer** icon on the desktop of your computer. This will open Windows Explorer.

b. Click on the **Folders** tab at the top of the **Windows Explorer** menu. The drives in your computer are displayed.

c. Select the CD by clicking on the CD drive in the **Folders** pane of Windows Explorer. The contents of the CD are displayed as shown in Figure 1 on page 8.

Figure 1. Explore the FTRA CD Using Windows Explorer

2. Install the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 from the CD.

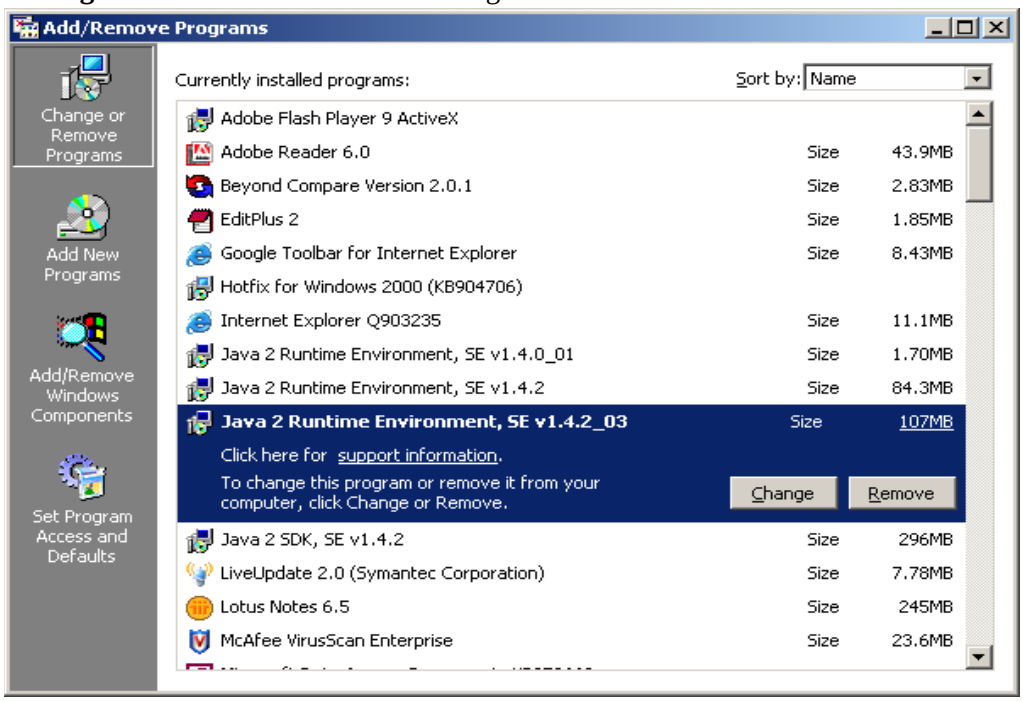
   You may not need to install the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 software if it is already installed on your computer. Perform the following steps to verify this:

   a. Go to Start Menu > Control Panel > Add or Remove Programs. All the programs installed on your computer are displayed.

   NOTE: If you use Windows XP in the classical mode. Perform the following steps: Go to Start Menu > Settings > Control Panel > Add or Remove Programs.

   b. If the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 software is installed on your computer as shown in Figure 2 on page 9, go to step 4. If the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 software is not installed on your computer, go to step 3

Figure 2. Add or Remove Programs Window



3. Install the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 software on your computer by performing these steps:

a. Select the CD drive on your computer.

b. Select the windows folder on the CD drive. The executable files for installing the FTRA software and the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 software are displayed.

c. Double-click on the j2re-1_4_2_03 windows-i586-l icon. The InstallShield Wizard opens. Follow the InstallShield Wizard instructions. When prompted, click the Yes or Next buttons, as appropriate, to proceed with the installation procedure.

d. The InstallShield Wizard asks you to choose the destination location for the Java™ 2 Runtime Environment Standard Edition Version 1.4.2_03 software only if you selected the Custom installation. You may change the destination location by clicking the Change button as shown in Figure 4 on page 10, or you may use the default destination location given in the wizard. Record the path information which will be required in step 7.

Figure 3. Select a Custom Installation

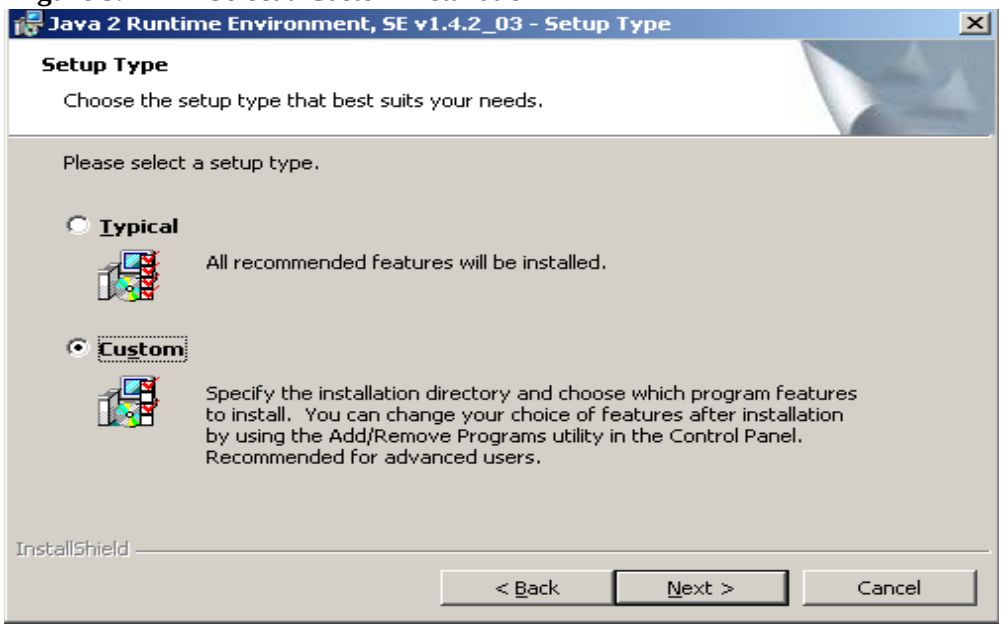
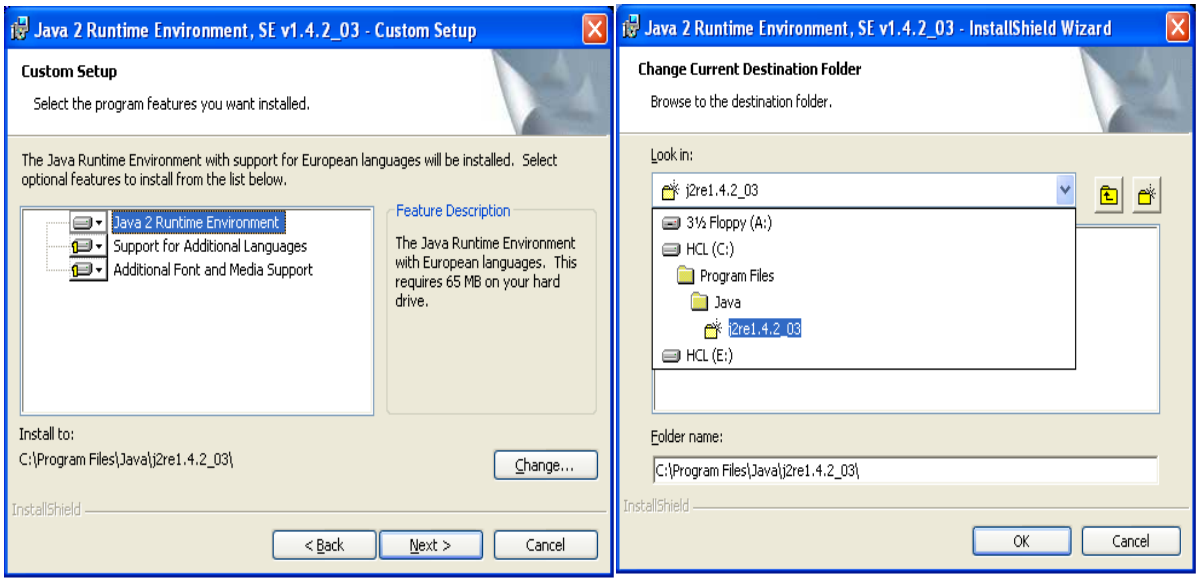


Figure 4. Java Runtime-Environment Install shield Wizard



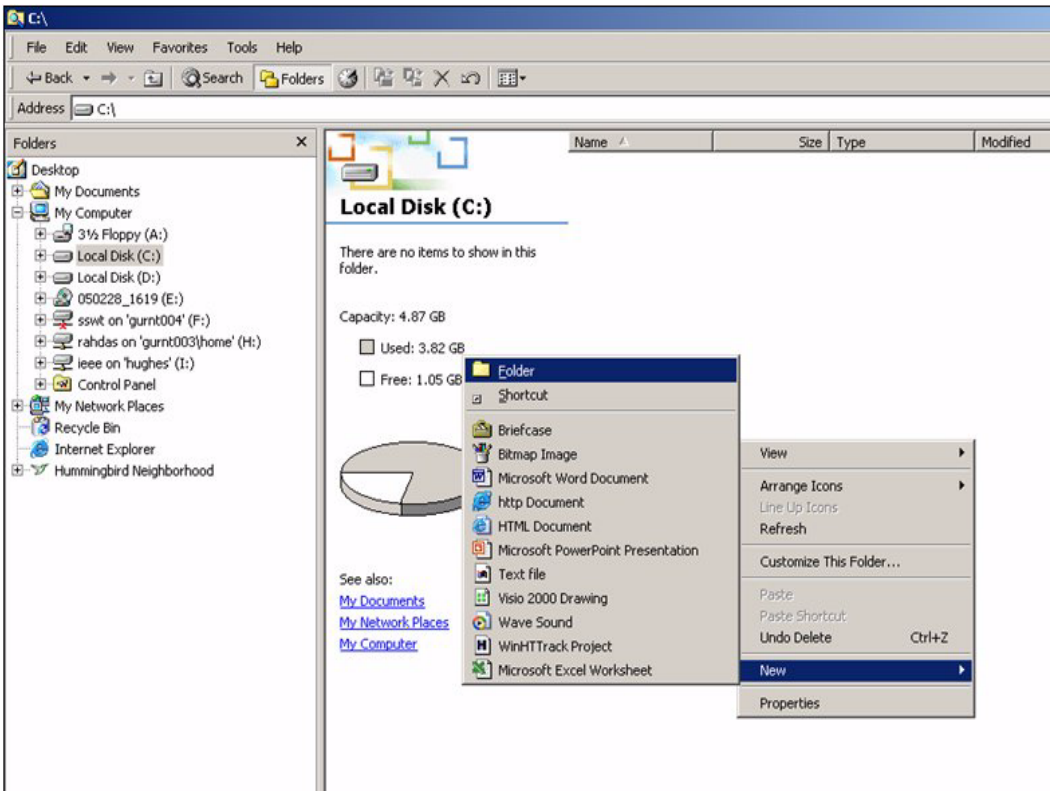
4. Create a folder that the FTRA software will be installed in (the <base_directory>), for example, C:\ftra.

   The new folder can be created on any drive on your computer. Perform the following steps to create the folder. For this example, a new folder named ftra is created on the C: drive.

   a. Select the C: drive from Windows Explorer.

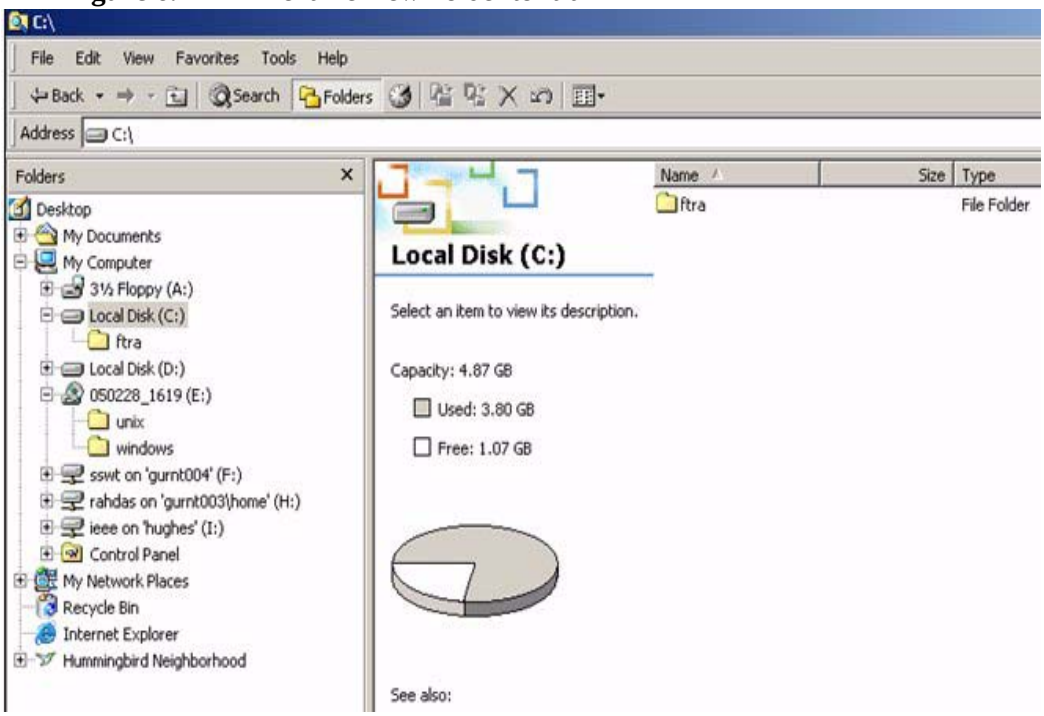
b. Right-click and select New > Folder as shown in Figure 5. A folder named New Folder is created.

Figure 5. Create a New Folder for FTRA Installation



c. Rename this folder to ftra as shown in Figure 6.

Figure 6. Rename New Folder to ftra



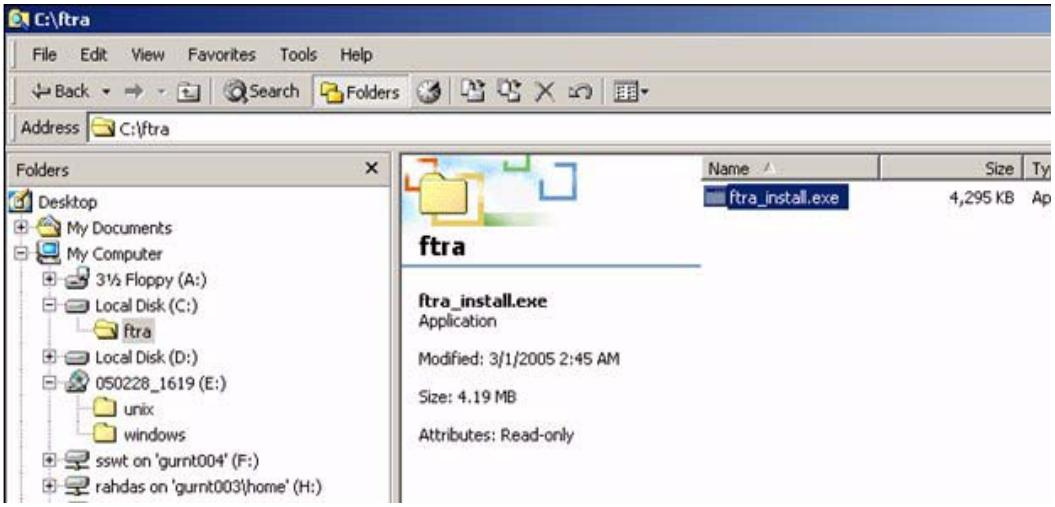
NOTE: Make sure that there is no previous installation of the FTRA software inside the ftra folder on your computer. If a previous installation of the FTRA software is inside the ftra folder, you may choose a different name for your <base_directory> or you may choose to remove or rename your previous FTRA installation.

5. Copy the ftra_install.exe file from the FTRA CD to the <base_directory> folder by performing these steps:

   a. In Windows Explorer, select the CD drive on your computer and select the windows folder.

   b. Copy the ftra_install.exe file from the windows folder to the <base_directory> folder as shown in Figure 7 on page 13.

Figure 7. Copy the ftra_install.exe File



6. Extract the FTRA program files using only the command prompt. Do not use the Windows Explorer window to extract the FTRA program files.

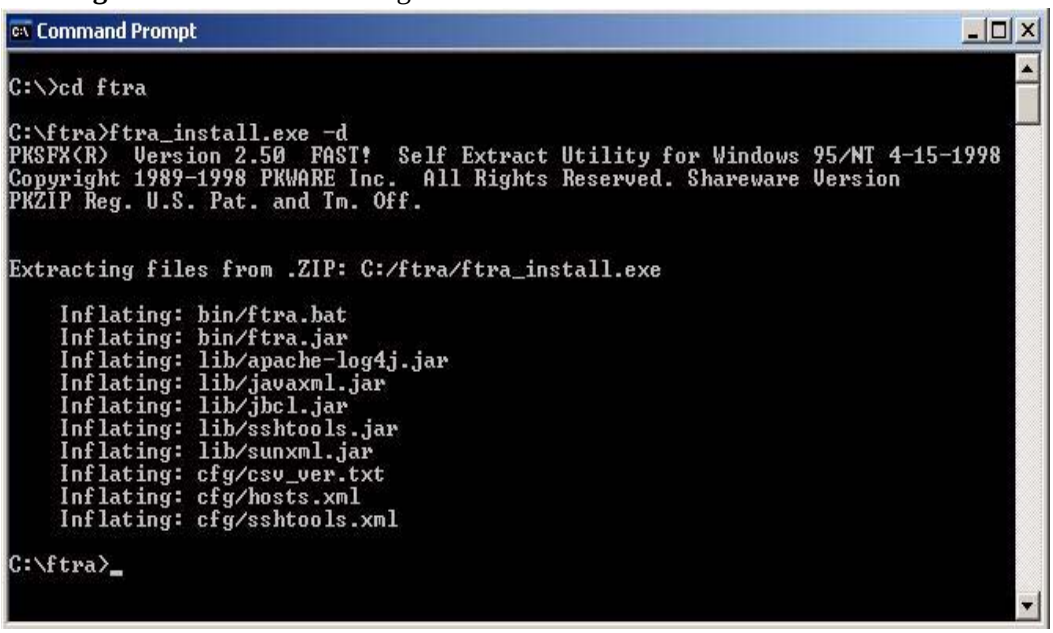
   a. Open the Windows command prompt.

   b. Change directory to the FTRA <base_directory>.

   c. Enter the command ftra_install -d as shown in Figure 8 on page 13.

   The FTRA program files are extracted to the FTRA <base_directory>.

Figure 8. Extract Program Files



7. Set the required system/user environment variables.The method for defining environment variables differs between Windows systems.

   Windows 2000 or Windows XP Operating System

   a. Right-click the My Computer icon on the desktop and select Properties.

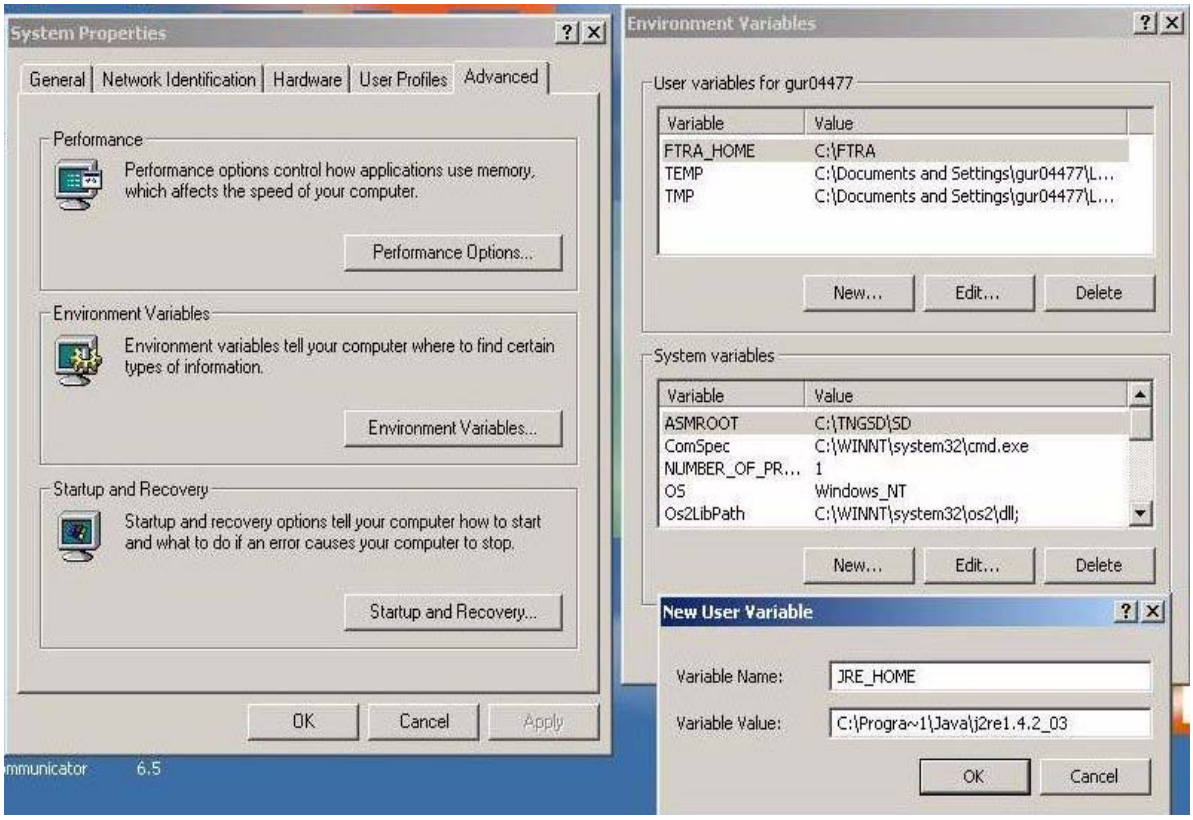
   b. In the Advanced tab, click Environment Variables and then click New as shown in Figure 9 on page 14.

   c. Under User variables, enter the following variable names and their values:

   FTRA_HOME = C:\<base_directory created for FTRA> (typically, C:\ftra)
   JRE_HOME = C:\Progra~1\Java\j2re1.4.2_03 (typically, the folder where Java is installed, and the Java path information recorded in step 2)

   NOTE: If the directory name has spaces, or is over eight characters in length, the DOS short name may be required to define the environment variable. For example, using the JRE_HOME environment variable above, the variable would be defined as "C:\Progra~1\Java\j2re1.4.0_01" (without the quotes) with the maximum eight characters for the directory name

Figure 9. Set the FTRA Environment Variables



Windows NT® Operating System[1]

NOTE: Installing the FTRA software on a computer using the Windows NT operating system is supported only on computers using Windows NT 4.0.

a. Right-click the My Computer icon on the desktop and select Properties.

b. In the Environment tab, select any user environment variable, enter the new variable names and values, and click Set.

c. Under User variables, enter the following variable names and their values:

FTRA_HOME = C:\<base_directory created for FTRA> (typically, C:\ftra)
JRE_HOME = C:\Progra~1\Java\j2re1.4.2_03 (typically, the folder where Java is installed, and the Java path information recorded in step 2.)

---

8. Create an FTRA shortcut on your desktop.

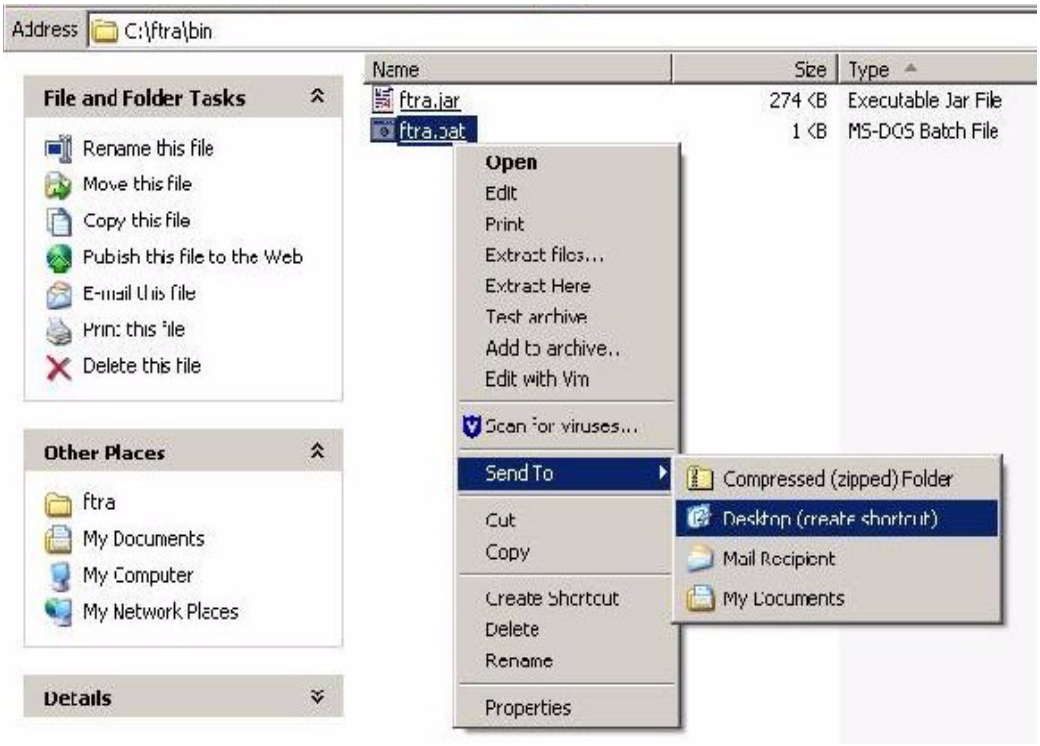
a. Using Windows Explorer, open the <base_directory>\bin folder.

b. Right-click on the ftra.bat file and then select Create Shortcut as shown in Figure 10. A shortcut to the ftra.bat file is created in the <base_directory>\bin folder.

c. Cut and paste this shortcut to the desktop.

1 Windows NT is a registered trademark of Microsoft Corporation in the United States of America and/or other countries.

Figure 10. Creating FTRA Shortcut - FTRA 4.0



NOTE: On multi-user systems, the shortcut should be placed in the Default User or All Users desktop folder in order to make it available to all users.

Procedure – FTRA Software Installation on Unix

1. Place the FTRA CD in the CD-ROM drive.

2. Install the Java™ 2 Runtime Environment SE V1.4.2_03 software either from the FTRA CD or download the Java™ 2 Runtime Environment SE V1.4.2_03 software from Sun Microsystems' web site.

a. To install the Java™ 2 Runtime Environment SE V1.4.2_03 software from the FTRA CD, open FileManager and go to the CDROM drive. From FileManager, double-click on the j2re-1_4_2_03-solaris-sparc.sh file and follow the installation instructions in "– Java™ 2 Runtime Environment Installation" on page 18.

b. To install the Java™ 2 Runtime Environment (JRE) 1.4.2_03 from Sun Microsystems' web site, enter the following address into your web browser and follow the product installation instructions:

http://java.sun.com/j2se/1.4/jre/install-solaris.html.

---

3. Create an <install_directory> into which the FTRA software will be installed. The preferred location is <HOME_DIRECTORY>/ftra, but you may place it wherever you would prefer. Open FileManager and go to the installation location. From FileManager, select File>New Folder and rename it ftra. Copy the file ftra_install.tar from the FTRA CD to the new <install_directory> (for example, <HOME_DIRECTORY>/ftra).

---

4. Extract the FTRA file(s) from the new <install_directory> (for example, <HOME_DIRECTORY>/ftra). From FileManager, right-click on the ftra_install.tar file and select Archive Unpack. This will extract the program files into a new /bin subdirectory.

   NOTE: The Archive Unpack function is only available when using the CDE (Common Desktop Environment) X-window File Manager. If you are not using the CDE, the Unix tar command should be used. Please refer to the man pages for more information about the tar command.

---

5. Set the required environment variables by adding the following lines to the user's cshrc file:

   a. setenv FTRA_HOME '<ftra_install_directory>' (for example, <HOME_DIRECTORY>/ftra).

   b. setenv JRE_HOME '<jre_install_directory>'.

---

6. Change to bin directory to run FTRA.

   Change to FTRA BIN <bin directory> (for example <cd/ftra/bin>)

   Run FTRA <./ftra>

Procedure – Java™ 2 Runtime Environment Installation

1. Log on as root.

2. Go to the Java installation directory: Shell> cd /usr

3. Copy the Java distribution from the FTRA CD: Shell> cp <path to the FTRA CD>/j2re1_4_2_03-solsparc.sh

4. Execute the Java installation program. Make sure the file is executable by entering the ls -l command. If the file is not executable, use the chmod command to change the permissions of the file to make the file executable. Shell> ./j2re1_4_2_3-solsparc.sh This will create a directory called j2re1_4_2_03.

5. Make a symbolic link to this directory called /usr/java by entering this command: Shell> ln -s j2re1_4_2_03 java. If a Java link already exists in the directory (use the ls -l command to verify that the link exists), remove the existing link first by entering the command **`rm java`**.

Procedure – Upgrade to FTRA 4.0 on Windows

1. Place the FTRA CD in the CD-ROM drive.

2. From Windows Explorer, copy the ftra_install.exe file from the FTRA CD to the existing folder containing the FTRA software. For details on the folder containing the FTRA software, see Procedure “- FTRA Software Installation on Windows” on page 7”.

3. Extract the FTRA program files from the FTRA CD. From the Windows command line, the MS-DOS prompt, enter the command ftra_install -d. The ftra_install -d command creates all the required directories and extracts the program files. During the execution of the ftra_install -d command, you will be asked if you wish to overwrite an existing file. Answer "no" if you wish to retain the entries in the hosts.xml file. This file contains previously provisioned host entries. Answer "yes" if you do not wish to retain the entries in the hosts.xml file. Choosing this option will cause the existing

hosts.xml file to be overwritten. When the ftra_install -d command has finished executing, the FTRA 4.0 software has been installed.

4. Start the FTRA software. See the "FTRA Initialization" section in the FTP-Based Table Retrieve Application (FTRA) User Guide (910-3489-001) for more information on starting the FTRA software. The existing FTRA STP Connection Configuration data will automatically be converted during the FTRA system initialization.

Procedure – Upgrade to FTRA 4.0 on Unix

---

1. Place the FTRA CD in the CD-ROM drive.

---

2. From FileManager, copy the ftra_install.tar file from the FTRA CD to the existing directory containing the FTRA software. For details on the directory containing the FTRA software, see Procedure "– FTRA Software Installation on Unix" on page 16.

---

3. From FileManager, right-click on the ftra_install.tar file that was copied from the FTRA CD, not the ftra_install.tar file on the FTRA CD, and select Archive Unpack. The program files will be extracted into the existing directory containing the FTRA software. If prompted, do not choose to overwrite the hosts.xml file in case some host entries were previously provisioned and need to be retained. Otherwise, choose to overwrite all other files.

   NOTE: The Archive Unpack function is only available when using the CDE (Common Desktop Environment) X-window File Manager. If the CDE is not being used, the Unix tar command should be used to extract the program files. Please refer to the man pages for the tar command for more information about using the tar command.

   When the extraction of the FTRA program files has completed, the FTRA 4.0 software has been installed.

---

4. Start the FTRA software. See the "FTRA Initialization" section in the FTP-Based Table Retrieve Application (FTRA) for more information on starting the FTRA software. The existing FTRA STP Connection Configuration data will automatically be converted during the FTRA system initialization.

FTRA Initialization

To start the FTRA, double-click the FTRA icon on the desktop. When the application starts, the **FTP-Based Table Retrieve Application** window is displayed. See Figure 11. The **Initializing** window opens and displays the message “Initializing, please wait……” until the initialization process has been completed.

Figure 11. FTP-Based Table Retrieve Application Window

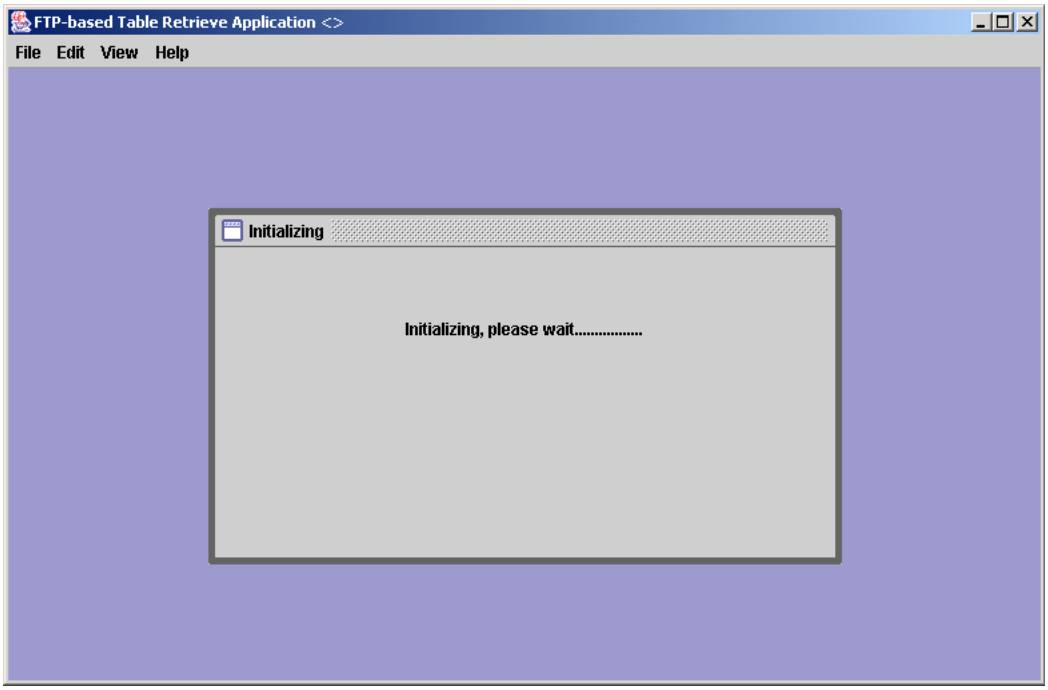


Table 1 shows the description of the menus in the **FTP-Based Table Retrieve Application** window.

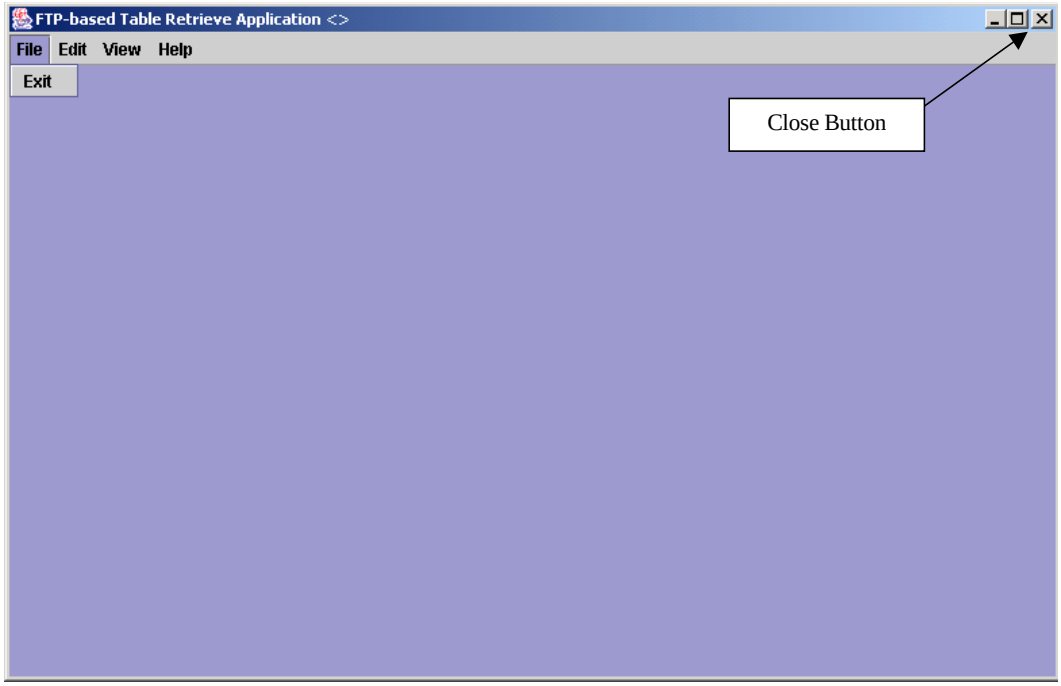
Table 1. FTP-Based Table Retrieve Application Menu Description

Item	Description
File	Selects the **Exit** menu.
Edit	Selects the **STP Connection Configuration** menu, the **FTP Server Configuration** menu, or the **Commands** menu
View	Selects these logs: • The Retrieve Tables Log • The Update Tables Log • The System Log.
Help	Selects the **About FTRA** window.

Exit the FTRA

To close the **FTP-Based Table Retrieve Application** window and exit the FTRA, either select **File > Exit** from the **File** menu, see Figure 12, or click the close window button in the upper right hand corner of the window.

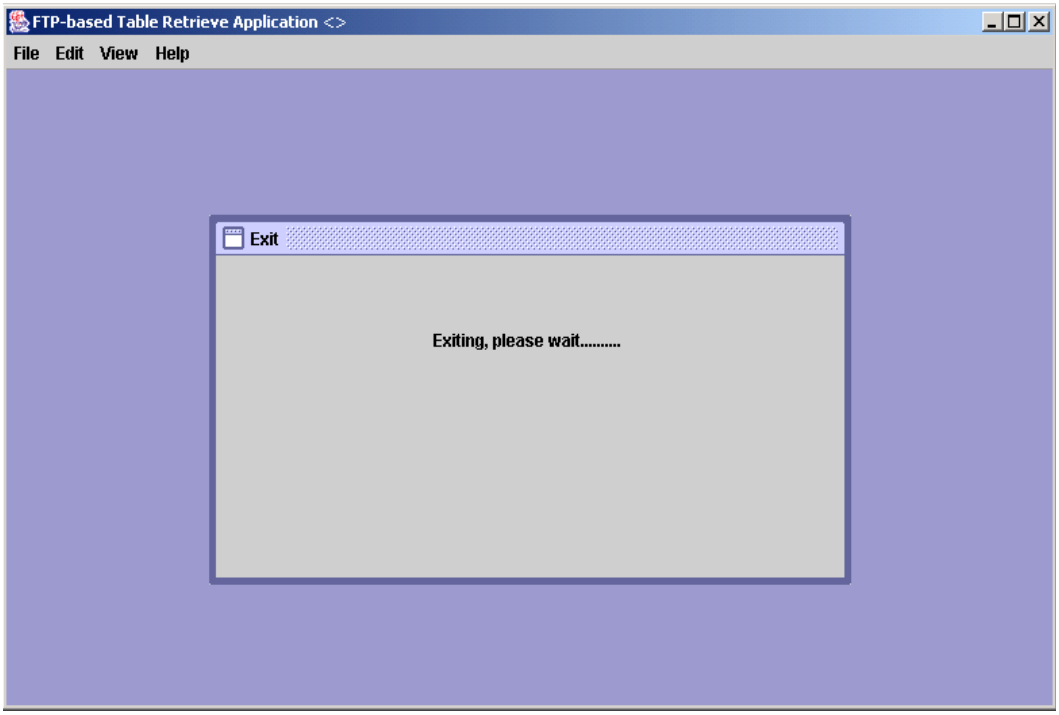
Figure 12. File Menu in the FTP-Based Table Retrieve Application Window



The **Exit?** confirmation window (see Figure 13) opens with “You are about to exit. Continue?” Click **OK** to exit and close the application. The **Exit** window (see Figure 14 on page 22) is displayed until the Exit process is completed. To cancel the exit and resume using the application, click **Cancel**.

Figure 13. Exit Confirmation Window

Figure 14. Exit Window



STP Connection Configuration Menu

Before database tables can be retrieved from an STP, or command files can be sent to an STP, the STP must be defined as an STP configuration record in the STP Connection Configuration database. The STP configuration record is configured and selected using the **STP Connection Configuration Menu** window.

The **STP Connection Configuration Menu** window is displayed by selecting **Edit > STP Connection Configuration**. See Figure 15.

Figure 15. Edit Menu

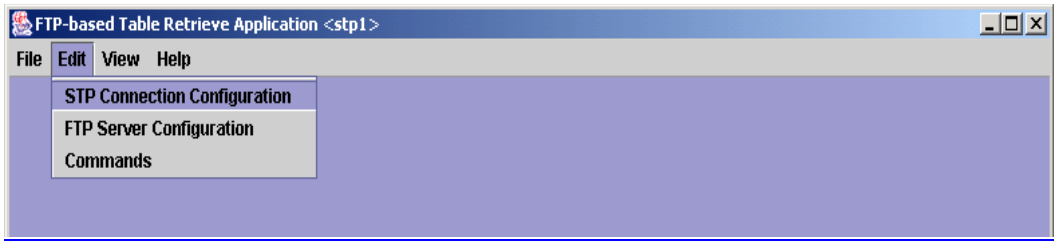


Figure 16. STP Connection Configuration Menu Window (FTRA 4.0)

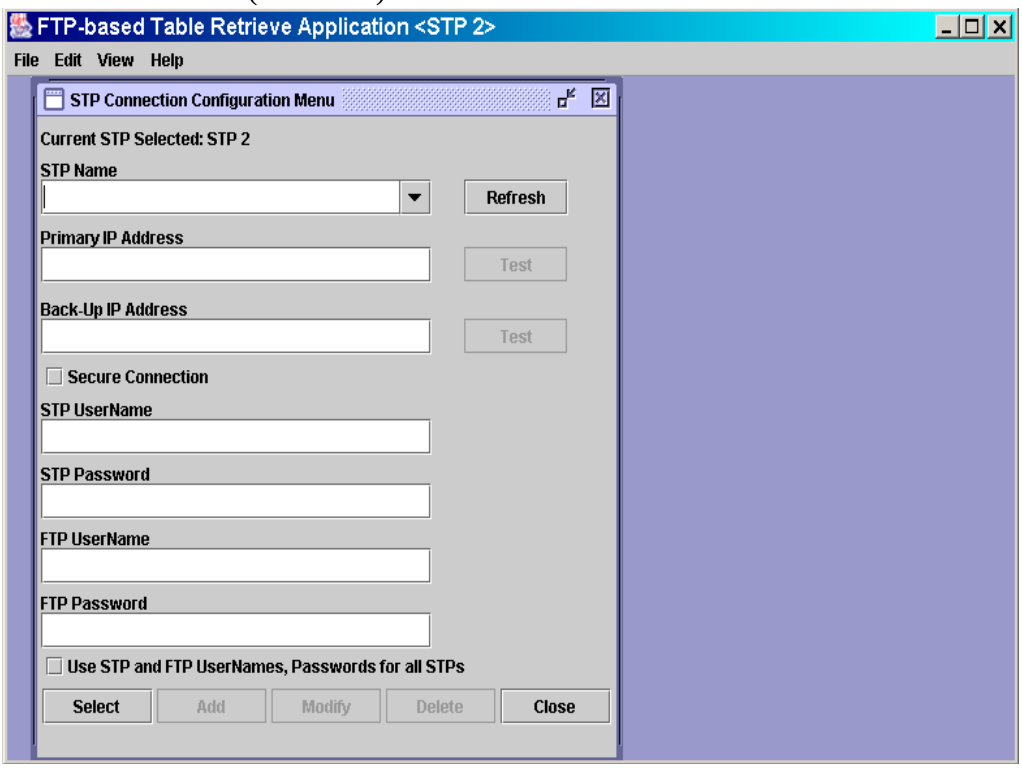


Table 2 shows the description of the fields, buttons, and boxes in the **STP Connection Configuration Menu** window.

Table 2. STP Connection Configuration Menu Description

Item	Description
Fields	
STP Name	Contains the STP Names. The STP name must contain at least one alphanumeric character and a maximum of 64 upper-case alphanumeric characters. The STP Name will always be entered in uppercase regardless of the Caps Lock key setting on your keyboard. This field also provides a drop down list for selecting stored STP configuration records.
Primary IP Address (FTRA 4.0)	The primary IP address of the associated STP (used for telnet sessions). The FTRA uses this IP address first when connecting to the STP. The primary IP address is the IP address of an IPSM in the associated EAGLE 5 ISS.
Backup IP Address (FTRA 4.0)	The backup IP address of the associated STP (used for telnet sessions). The FTRA uses this IP address when the connection using the primary IP address fails. The backup IP address should be the IP address of another IPSM in the same EAGLE 5 ISS.
STP UserName	The user name assigned to the user by the STP system administrator (used for telnet sessions).
STP Password	The password assigned to the user by the STP system administrator (used for telnet sessions).
FTP UserName	The FTP user name assigned to the user by the administrator (used for FTP). Any FTP user name with symbols must be enclosed within double quotation marks (for example, to specify the FTP user name **`mylogin#1`**, you would enter **`"mylogin#1"`**).
FTP Password	The FTP password assigned to the user by the administrator (used for FTP).
Buttons	
Refresh	Displays the data of the STP configuration record typed in the STP Name field. If an STP name is selected from the STP Name drop down list, the data fields are automatically displayed.
Test	Verifies that the FTRA can successfully connect and login to the EAGLE 5 ISS through an available telnet terminal at the specified IP address. For FTRA 4.0, the STP Connection Configuration Menu window has two **Test** buttons, one for the Primary IP address, and one for the Backup IP address.
Select	Selects the displayed STP name to be connected to the FTRA. The **STP Selection Change** window opens to verify if you want to proceed.
Add	Adds a newly entered STP configuration record and associated data to the STP Connection Configuration database.
Modify	Modifies the fields of the displayed STP configuration record.
Delete	Deletes the displayed STP configuration record and associated data from the STP Connection Configuration database.

Table 2. STP Connection Configuration Menu Description (Continued)

Item	Description
Close	Closes the **STP Connection Configuration Menu** window.
Secure Connection (FTRA 4.0)	Enables the FTRA to use a secure IP connection to the STP. To use a secure connection for the FTRA to EAGLE 5 ISS communication, make sure the EAGLE 5 ISS is running release 30.2 or greater and that the Eagle OA&M IP Security Enhancements feature is enabled and activated. This can be verified by entering the **`rtrv-ctrl-feat`** command at the EAGLE 5 ISS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the "Activating the Eagle OA&M IP Security Enhancements Controlled Feature" procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature. **NOTE: This box should be unchecked if the Eagle OA&M IP Security Enhancements feature is not enabled or activated, and will not be enabled or activated.** If this box is checked, the public key fingerprint for the EAGLE 5 ISS specified in this window must be installed onto the FTRA for the FTRA and the specified EAGLE 5 ISS to use a secure connection. After this STP is added to the STP Connection Configuration database, add the public key fingerprint to the FTRA by performing the "Secure EAGLE 5 ISS Host Key Provisioning" procedure on page 46.
Use STP and FTP UserNames, Passwords for all STPs Box	All the STP and FTP user names and passwords of all the provisioned STPs are changed to the user name and password of the displayed STP name. This change occurs only when the Add or Modify buttons are used.

Adding an STP Configuration Record

Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 15 on page 23. The **STP Connection Configuration Menu** window opens. The **Add** button is not enabled when the **STP Connection Configuration Menu** window opens.

2. Enter the STP name in the **STP Name** field of the **STP Connection Configuration Menu** window. The STP name must contain at least one alphanumeric character, with a maximum of 64 upper-case characters (alphanumeric, letters and numbers, and spaces). or Figure 18 on page 27 (FTRA 4.0). The STP Name will always be entered in uppercase regardless of the Caps Lock key setting on your keyboard.

   If characters other then alphanumeric characters or spaces are included in the STP name, the **Invalid STP Name** warning window is displayed. See Figure 17. If the **Invalid STP Name** window appears, click **OK**, and reenter the STP name in the **STP Name** field with the correct characters.

   NOTE: When the new STP name is entered into the STP Name field, the Add button is enabled. If the STP name matches an existing STP name in the STP Connection Configuration database, the Add button is disabled. If you wish to display the existing STP names, go to the "Displaying an Existing STP Configuration Record" procedure on page 31.

   NOTE: If the "Use STP and FTP UserNames and Passwords for all STPs" box is checked when the Add button is clicked, all the user names and passwords for all provisioned STP Names are changed to those of the added STP name.

   NOTE: Existing STP configuration records can be changed. Go to the "Modifying an Existing STP Configuration Record" procedure on page 40 to change an existing STP configuration record.

   Figure 17. Invalid STP Name Error Message

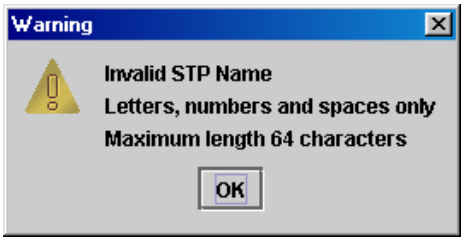
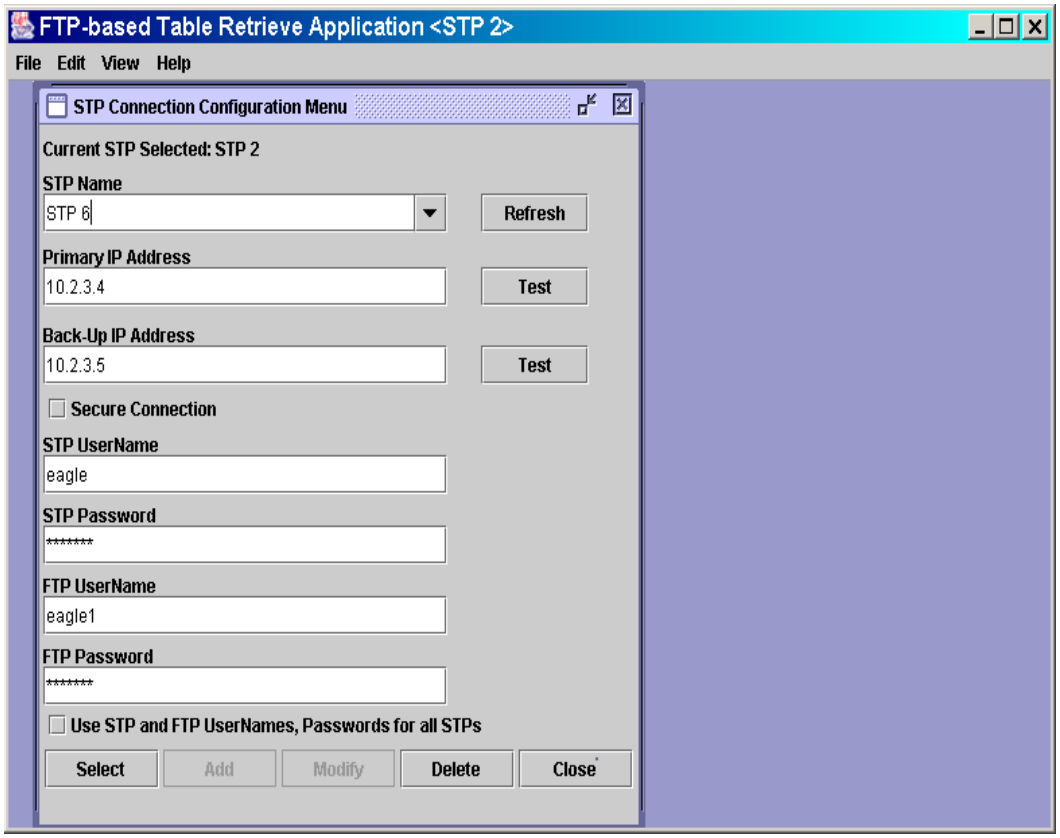


Figure 18. Adding an STP Configuration Record (FTRA 4.0)



3. Enter the IP address want to connect to the STP in the **Primary IP Address** field, and a backup IP address in the **Backup IP Address** field. See Figure 18 on page 27 (FTRA 4.0).

CAUTION: If the backup IP address is not entered for FTRAs running 4.0, the FTRA will not be able to connect to the STP when the connection to the STP using the primary IP address fails. It is recommended that you specify a backup IP address for the STP.

If the primary and backup IP addresses (FTRA 4.0) are not entered correctly, the **Invalid IP Address** warning window is displayed. See Figure 19. If the **Invalid IP Address** window appears, click **OK**, and re-enter the IP address in the primary or

backup IP addresses box (FTRA 4.0) in the **Primary IP Address** or **Backup IP Address** fields in the correct format.

Figure 19. Invalid IP Address Error Message

4. Enter the STP user name for this STP in the **STP UserName** field. The user name is assigned to the user by the STP system administrator for telnet sessions. See Figure 18 on page 27 (FTRA 4.0). If the format of the STP user name is not correct, the **Invalid STP User Name** warning window is displayed. See Figure 20. If the **Invalid STP User Name** window appears, click **OK**, and re-enter the STP user name in the **STP UserName** field.

Figure 20. Invalid STP User Name Error Message

5. Enter the STP password for this STP in the **STP Password** field. The password is assigned to the user by the EAGLE 5 ISS system administrator for telnet sessions. See Figure 18 on page 27 (FTRA 4.0). If the format of the STP password is not correct, the **Invalid STP Password** warning window is displayed. See Figure 21. If the **Invalid STP Password** window appears, click **OK**, and re-enter the STP password in the **STP Password** field.

NOTE: The STP Password field does not check for invalid EAGLE 5 ISS passwords. The passwords are validated by the EAGLE 5 ISS when the FTRA attempts a connection to the EAGLE 5 ISS. The requirements for the format of EAGLE 5 ISS passwords is shown in the output of the EAGLE 5 ISS's `rtrv-secu-dflt` command.

Figure 21. Invalid STP Password Error Message

6. Enter the FTP user name assigned by the FTP server administrator in the **FTP UserName** field. See Figure 18 on page 27 (FTRA 4.0). Any FTP user name with symbols must be enclosed within double quotation marks (for example, to specify the FTP user name **mylogin#1**, you would enter **"mylogin#1"**). If the format of the FTP user name is not correct, the **Invalid FTP User Name** warning window is displayed. See Figure 22. If the **Invalid FTP User Name** window appears, click **OK**, and re-enter the FTP user name in the **FTP UserName** field.

   NOTE: Any firewall between the FTRA and the FTP server configured in the FTP Server Configuration Menu window (Figure 45 on page 53), must allow FTPs to the IP address specified in the FTP Server Configuration Menu window.

Figure 22. Invalid FTP User Name Error Message

7. Enter the FTP password assigned by the FTP server administrator in the **FTP Password** field. See Figure 18 on page 27 (FTRA 4.0). If the format of the FTP password is not correct, the **Invalid FTP Password** warning window is displayed. See Figure 23. If the **Invalid FTP Password** window appears, click **OK**, and re-enter the FTP password in the **FTP Password** field.

Figure 23. Invalid FTP Password Error Message

NOTE: If you are running FTRA 4.0 and not enabling a secure connection to the STP, skip this step and go to step 9.

8. To enable a secure connection between the FTRA and the STP being added in this procedure, click in the **Secure Connection** box.

   Make sure the EAGLE 5 ISS is running release 30.2 or greater and that the Eagle OA&M IP Security Enhancements feature is enabled and activated. This can be verified by entering the **rtrv-ctrl-feat** command at the EAGLE 5 ISS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the "Activating the Eagle OA&M IP Security Enhancements Controlled Feature" procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature.

---

9. Click the **Add** button. See Figure 18 on page 27 (FTRA 4.0). The newly entered STP Name and associated data is added to the STP Connection Configuration database, and the **STP Added** window (Figure 24) is displayed. Click **OK** to continue.

Figure 24. STP Added Window

10. Verify the addition of the new STP name. See the “Displaying an Existing STP Configuration Record” procedure on page 31.

Displaying an Existing STP Configuration Record

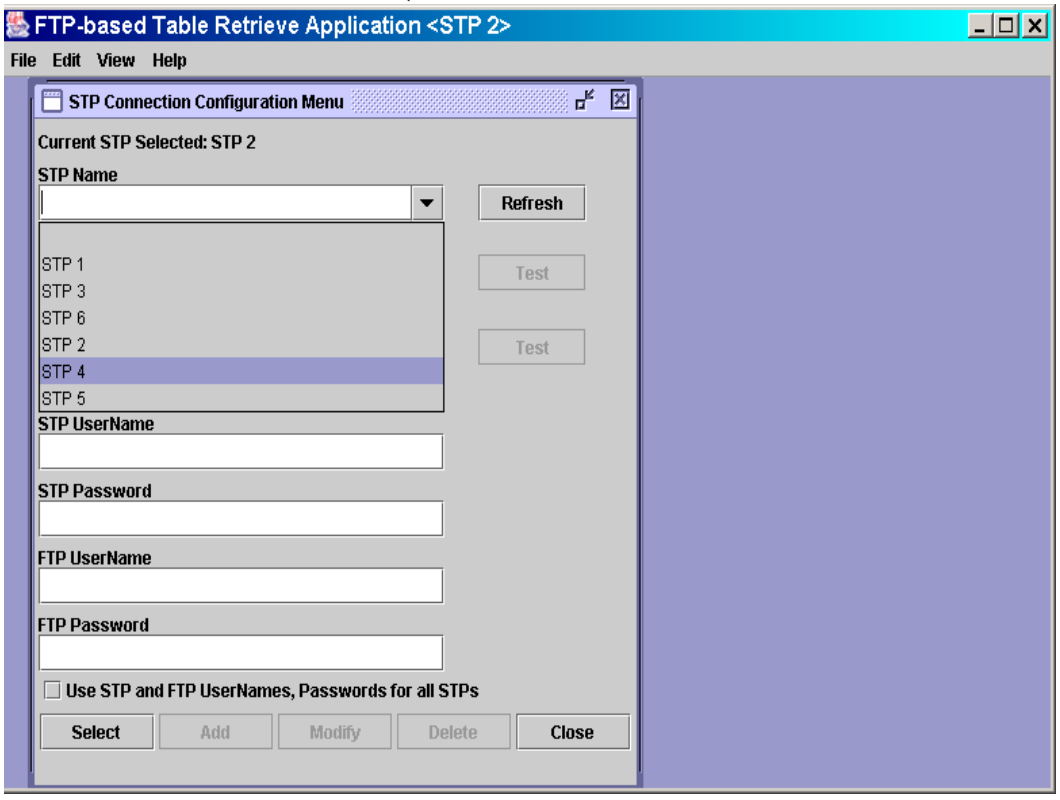
An existing STP configuration record can be displayed by either selecting the STP Name from the STP Name drop down list, or by re-entering the STP name in the **STP Name** field in the **STP Connection Configuration Menu** window and clicking the **Refresh** button.

To Use the STP Name Drop Down List

Procedure

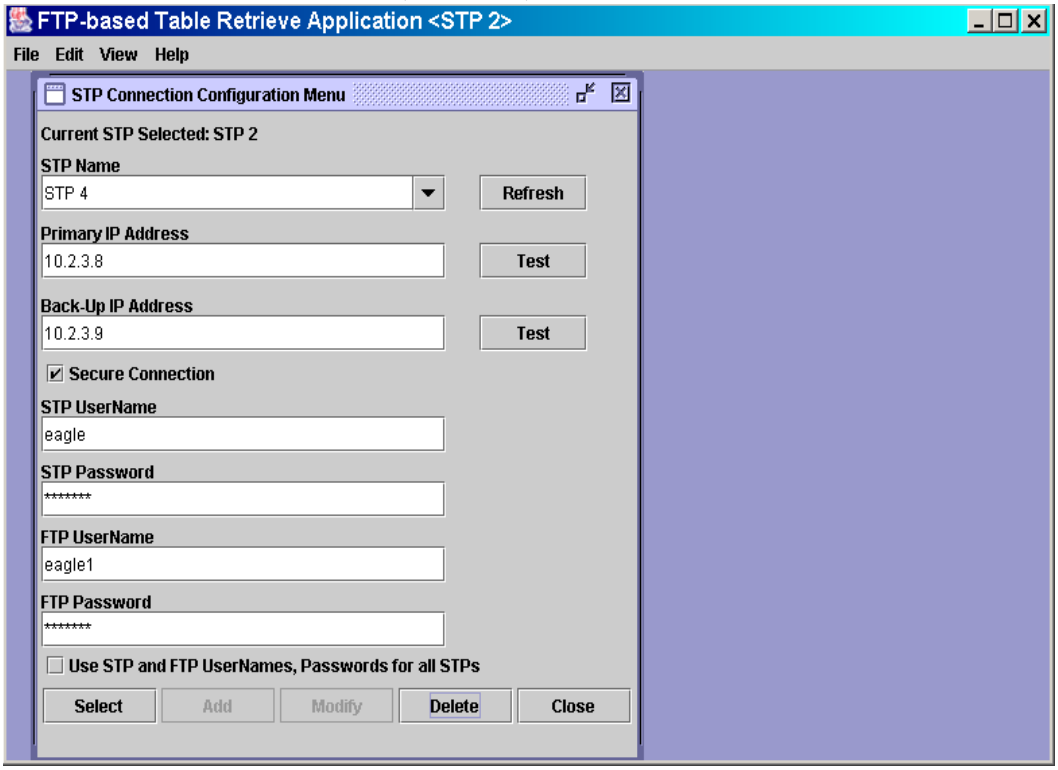
1. In the **STP Connection Configuration Menu** window, click on the **STP Name** drop down list. The **STP Name** drop down list opens. Move the cursor to the STP name to be selected. Click on the desired STP name in the drop down list. See Figure 25 on page 31 (FTRA 4.0).

Figure 25. Selecting an STP Name from the STP Name Drop Down List (FTRA 4.0



2. When the STP name is selected in step 1, the STP configuration record for the specified STP is displayed. See Figure 26 on page 32 (FTRA 4.0). The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

Figure 26. STP Name Selected from the STP Name Drop Down List (FTRA 4.0)

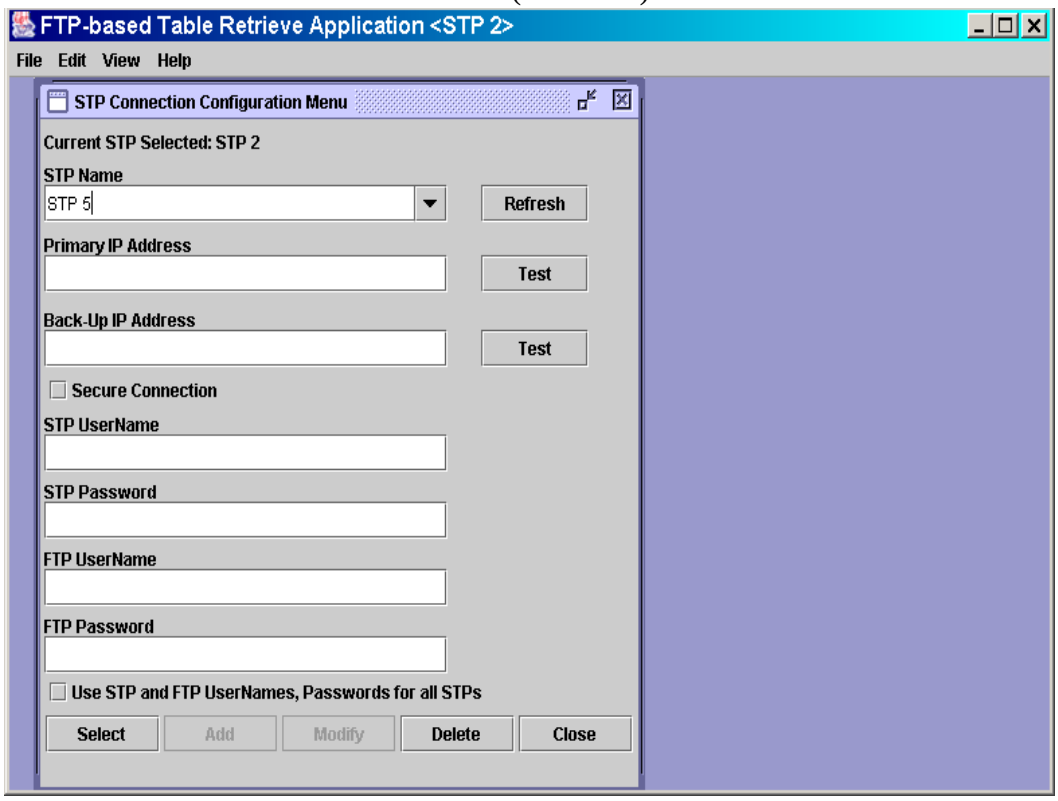


To Enter the STP Name

Procedure

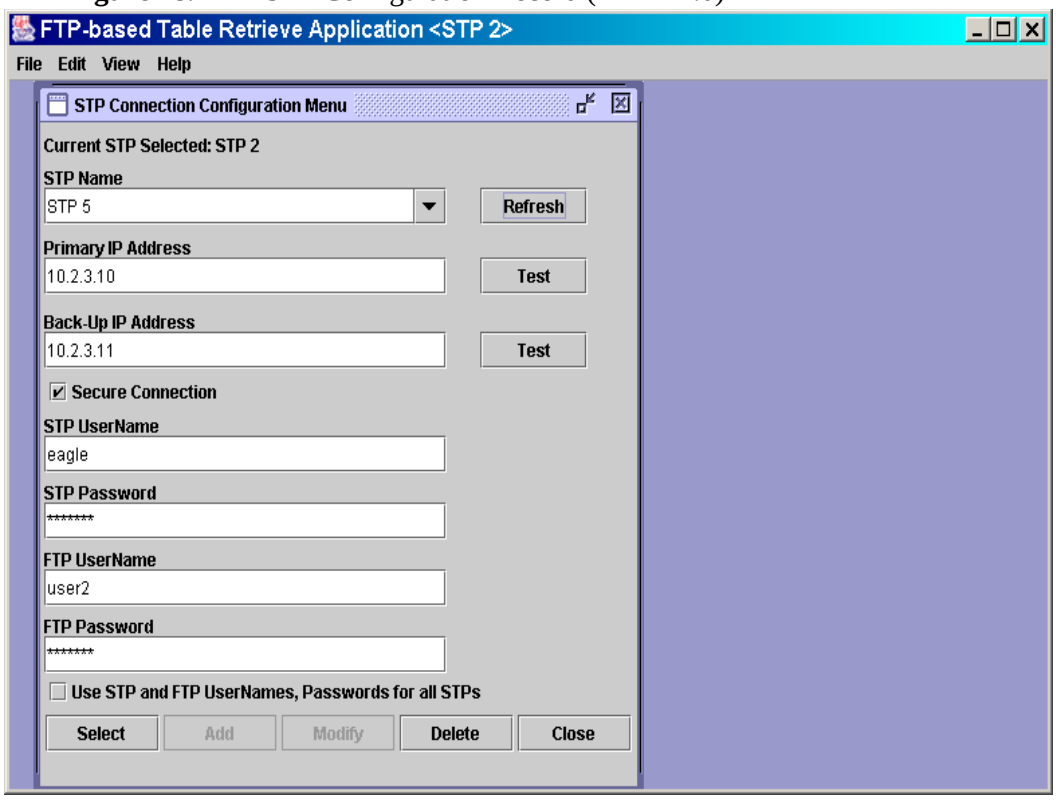
1. Type the STP name in the **STP Name** field in the **STP Connection Configuration Menu** window. See Figure 27 on page 33 (FTRA 4.0). The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

   Figure 27. Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 4.0)



2. Click the **Refresh** button. The STP configuration record for the specified STP is displayed. See Figure 28 on page 34 (FTRA 4.0).

Figure 28. STP Configuration Record (FTRA 4.0)



3. If the STP name was entered incorrectly, or is not in the STP configuration record database, the “STP Name does not exist” error message is displayed. See Figure 29.

Figure 29. STP Name Does Not Exist Error Message

Testing an STP Configuration Record

Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 15 on page 23. The **STP Connection Configuration Menu** window opens.

2. Display the STP configuration record being modified. Go to the "Displaying an Existing STP Configuration Record" procedure on page 31.

3. Click the **Test** button. The **Connectivity Test Log** window opens. See Figure 30 and Figure 31 on page 36. The Connectivity Test Log contains the events of the Test process and any error messages that may have occurred. The **Connectivity Test Log** window opens at the start of the Test process and is automatically cleared whenever a subsequent Test process is initiated.

Figure 30. Connectivity Test Log Window with No Errors

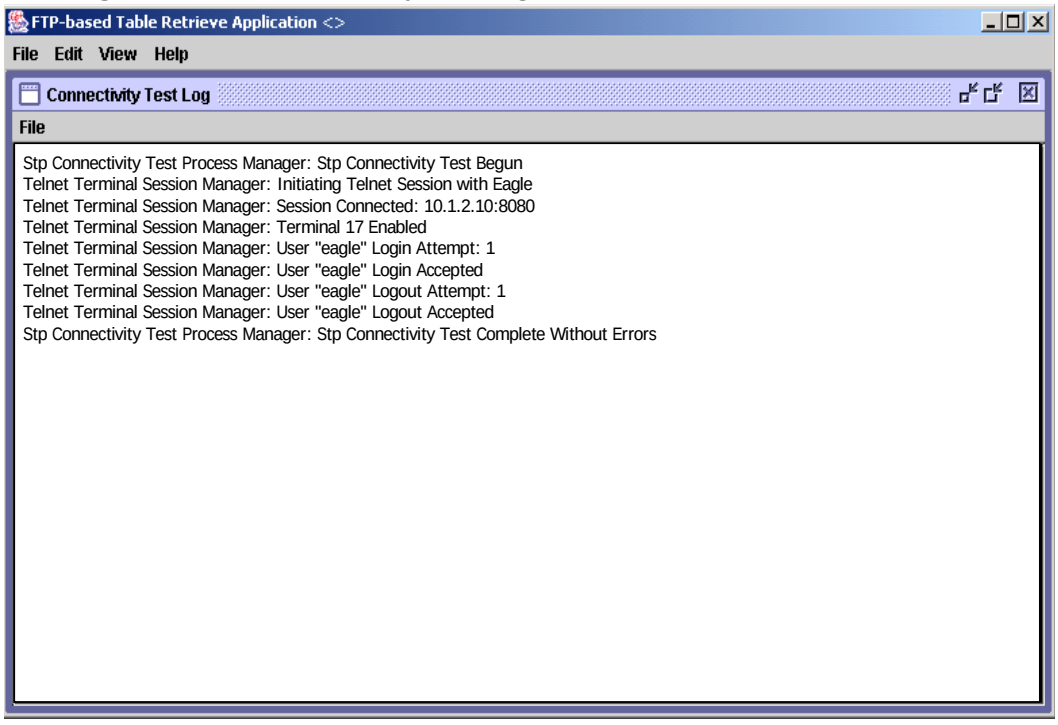
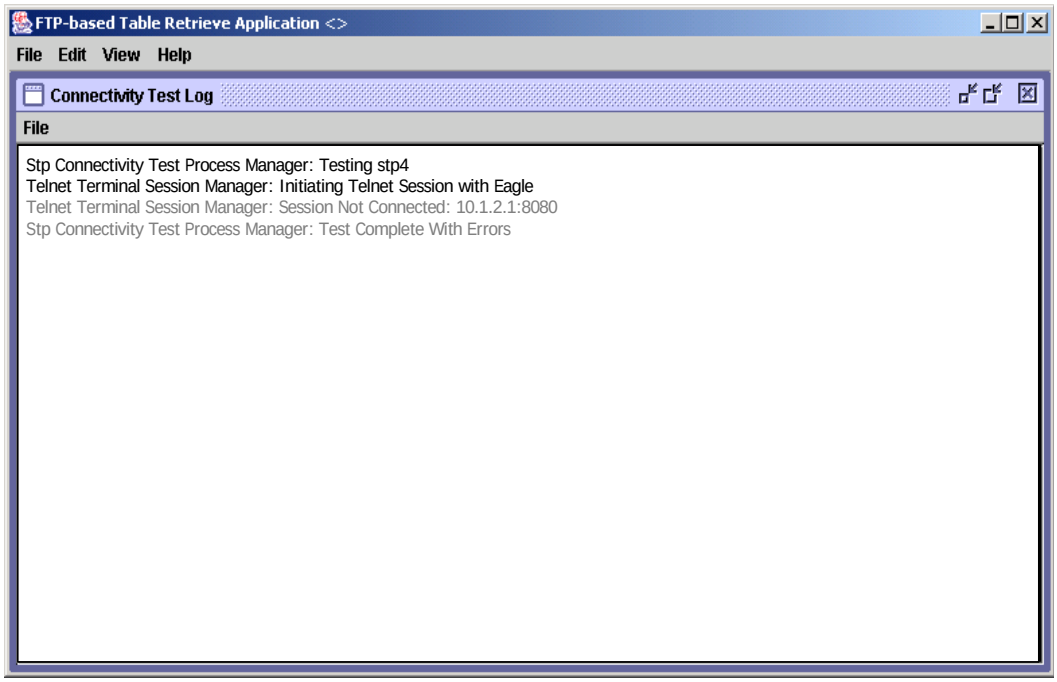
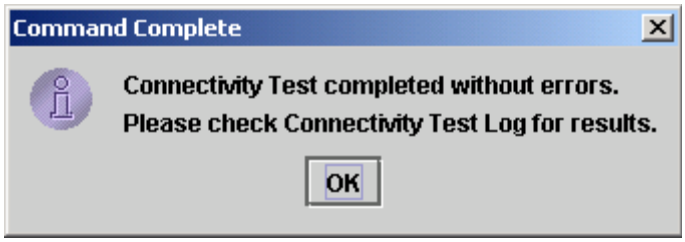


Figure 31. Connectivity Test Log Window with Errors



4. When the test is complete, the **Command Complete** window opens. See Figure 32. Click **OK** to continue.

Figure 32. Command Complete Connectivity Test Window

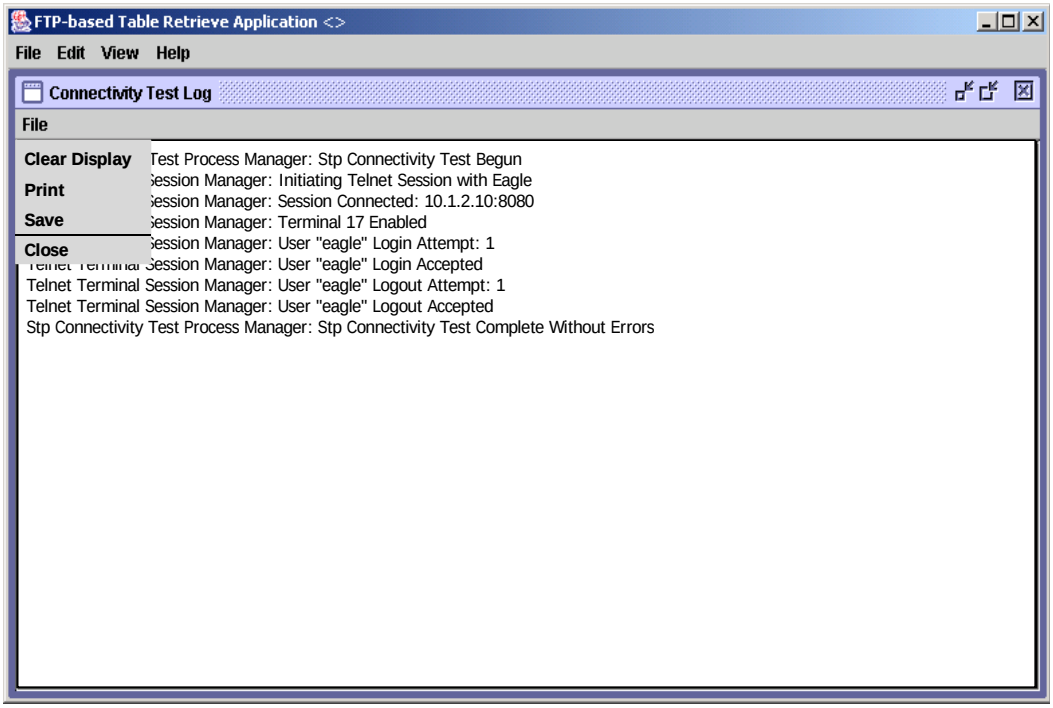


Connectivity Test Log File Menu

The **File** menu in the **Connectivity Test Log** window, shown in Figure 33 on page 37, provides these selections:

- Clearing the Connectivity Test Log display
- Printing the Connectivity Test Log
- Saving the Connectivity Test Log to a file
- Closing the **Connectivity Test Log** window.

Figure 33. File Menu in the Connectivity Test Log Window



Clearing the Connectivity Test Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is save to a file or printed before the display is cleared.

Procedure

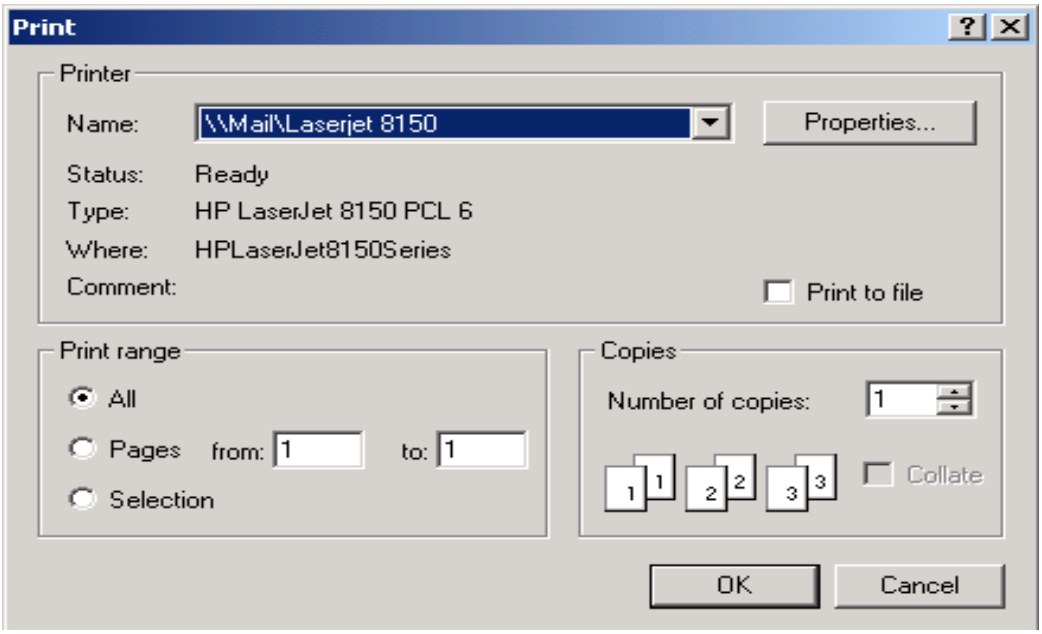
1. Select **File > Clear Display** in the **Connectivity Test Log** window. See Figure 33. The Connectivity Test Log display clears.

Printing the Connectivity Test Log

Procedure

1. Select **File > Print** in the **Connectivity Test Log** window. See Figure 33 on page 37. The **Print** window opens. See Figure 34.

Figure 34. Print Window



2. Configure the printer settings.

3. To print the Connectivity Test Log, click the **OK** button in the **Print** window. The current contents of the Connectivity Test Log are printed.

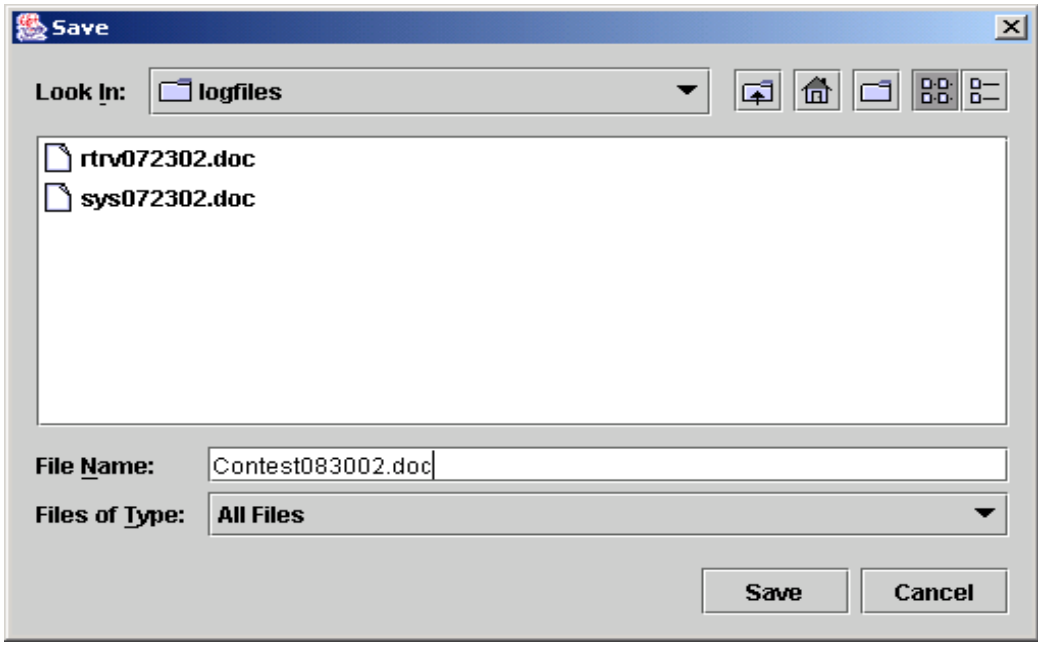
4. If you decide not to print the Connectivity Test Log, click the **Cancel** button in the **Print** window.

Saving the Connectivity Test Log to a File

Procedure

1. Select **File > Save** in the **Connectivity Test Log** window. See Figure 33 on page 37. The **Save** window opens. See Figure 35.

Figure 35. Save Window



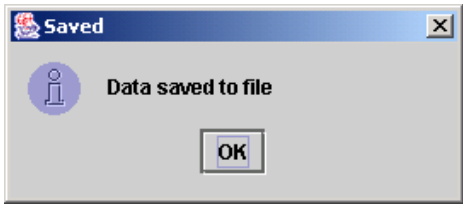
2. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.

NOTE: If you decide not to save the file, do not perform steps 3 and 4, but click Cancel in the Save window.

3. Click the **Save** button. A **Saved** file confirmation window opens with "Data saved to file." See Figure 36.

Figure 36. Saved File Confirmation Window



4. To save the file, click **OK** in the **Saved** file confirmation window to continue.

Closing the Connectivity Test Log Window

Procedure

1. Select **File > Close** in the **Connectivity Test Log** window, or click the close window button in the upper right hand corner of the **Connectivity Test Log** window. See Figure 33 on page 37. The **Connectivity Test Log** window closes.

Modifying an Existing STP Configuration Record

Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 15 on page 23. The **STP Connection Configuration Menu** window opens.

2. Display the STP configuration record being modified. Go to the “Displaying an Existing STP Configuration Record” procedure on page 31.

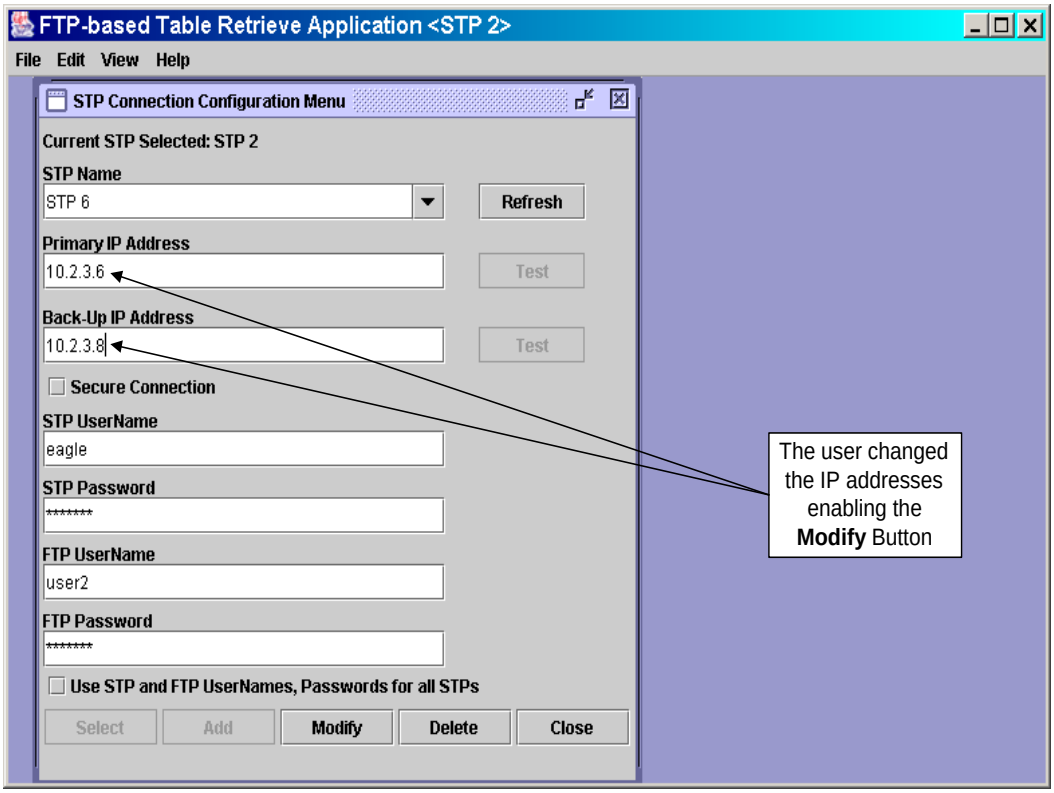
3. Select and change the STP configuration record parameters. The **Modify** button is enabled when new data is entered into any of the fields, or when the **Use STP and FTP UserNames and Passwords for all STPs** box is checked.

   NOTE: The STP name cannot be changed.

   If the IP address, STP user name, or STP password is not entered correctly, an error message is displayed. See Figure 19 on page 28, Figure 20 on page 28, or Figure 21 on page 28. If the FTP user name and FTP password are not entered, an error message is displayed. See Figure 22 on page 29 or Figure 23 on page 29

4. To apply the changes, click the **Modify** button. See Figure 37 on page 41 (FTRA 4.0). The displayed STP configuration record is modified, and all fields are cleared. To confirm that the STP configuration data has been modified, the **STP Data Modified** window is displayed (Figure 38 on page 42). Click **OK** in the **STP Data Modified** window to continue.

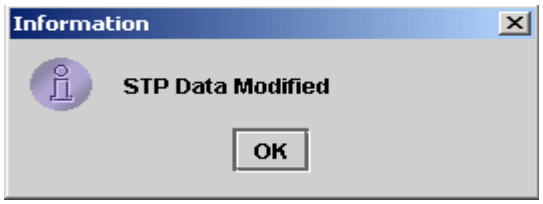
Figure 37. Modifying STP Configuration Record Parameters (FTRA 4.0)



CAUTION: If the Use STP and FTP UserNames and Passwords for all STPs box is checked, then all user names and passwords for all STPs in the STP Configuration database are changed to the user name and password for the displayed STP.

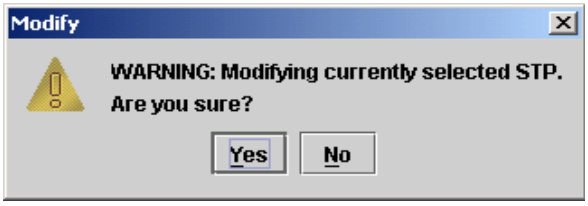
CAUTION: It is recommended that the setting for the Secure Connection box is not changed, unless you have verified that the new setting for the Secure Connection box will match the state of the Eagle OA&M IP Security Enhancements feature on the STP. The state of the Eagle OA&M IP Security Enhancements feature can be verified by entering the `rtrv-ctrl-feat` command at the EAGLE 5 ISS. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, the Secure Connection box should be unchecked. If the Eagle OA&M IP Security Enhancements feature is enabled and activated, the Secure Connection box should be checked. To change the state of the Eagle OA&M IP Security Enhancements feature, perform the "Activating the Eagle OA&M IP Security Enhancements Controlled Feature" procedure in the *Database Administration Manual - System Management.*

Figure 38. STP Data Modified Window



NOTE: If the STP configuration record being changed is shown in the Current STP Selected: field, a Modify Warning window is displayed. See Figure 39.

Figure 39. Modify Warning Window



Click **Yes** to continue.

If you do not wish to apply the changes, click the **Refresh** button in the **STP Connection Configuration Menu** window. This resets the STP configuration record values.

---

5. Verify that the changes were made. See the "Displaying an Existing STP Configuration Record" procedure on page 31.

Deleting an STP Configuration Record

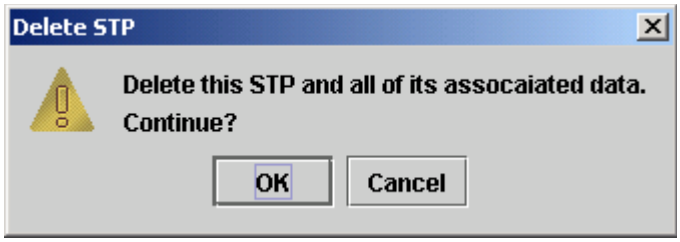
Procedure

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 15 on page 23. The **STP Connection Configuration Menu** window opens.

2. Display the STP configuration record being deleted. Go to the "Displaying an Existing STP Configuration Record" procedure on page 31. The **Delete** button is enabled when an existing STP configuration record is displayed.

3. To delete the STP configuration record, click the **Delete** button. The **Delete STP** window opens. See Figure 40.

   Figure 40. Delete STP Window

   Click **OK**, to delete the STP configuration record. The STP configuration record is deleted.

   If you do not wish to delete the STP configuration record, click **Cancel**.

4. Verify the STP name is no longer in the STP Connection Configuration database. Go to the "Displaying an Existing STP Configuration Record" procedure on page 31.

Selecting the Current STP

Before retrieving database tables from an EAGLE 5 ISS, or sending commands to an EAGLE 5 ISS, that STP name must be shown in the **STP Connection Configuration Menu** window as the current STP. The **Current STP Selected:** indicator in the **STP Connection Configuration Menu** window shows which STP is the current STP.

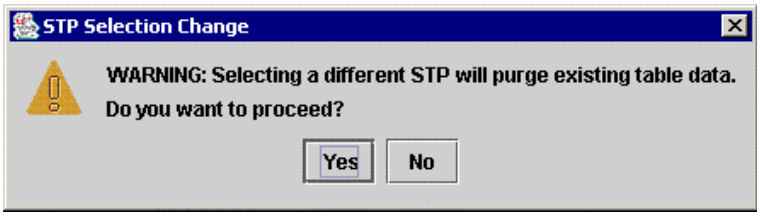
Procedure

1. Display an existing STP configuration record. Go to the “Displaying an Existing STP Configuration Record” procedure on page 31.

2. Click the **Select** button.

   If the selected STP is different from the STP shown as the current STP, the **STP Selection Change** window opens and displays “Warning: Selecting a different STP will purge existing table data. Do you want to proceed?” See Figure 41.

   Figure 41. STP Selection Change Window

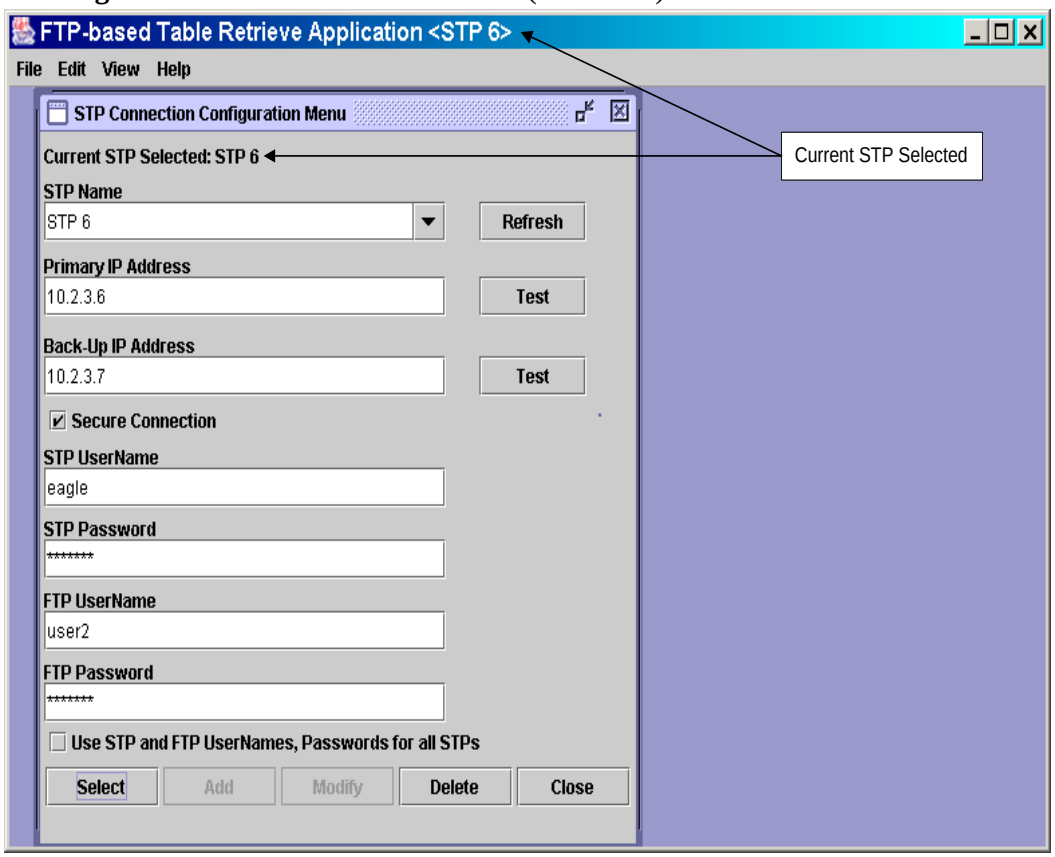


3. To proceed and select the STP name as the current STP, click the **Yes** button in the **STP Selection Change** window. The existing data table is purged.

   NOTE: To purge the data tables, a flag is set so that any of the existing table data already stored in the offline database will not be used.

   The selected STP name appears in the title bar of the window, and **Current STP Selected:** <*STP Name*> appears in the **STP Connection Configuration Menu**. See Figure 42 on page 45 (FTRA 4.0).

Figure 42. Current STP Selected (FTRA 4.0)



4. If you do not wish to use the STP name selected in step 2, click the **No** button in the **STP Selection Change** window. The current STP configuration record is displayed.

Secure EAGLE 5 ISS Host Key Provisioning

An EAGLE 5 ISS using secure connections has a unique host key for each IPSM in the EAGLE 5 ISS. This key is used by the FTRA (FTRA 4.0) to positively identify or authenticate each IPSM's telnet server on the EAGLE 5 ISS. The FTRA will not connect to an unauthenticated server. The FTRA authenticates the server by matching it's pre-installed host key with the key received from the EAGLE 5 ISS when the connection between the EAGLE 5 ISS and the FTRA is made.

This procedure installs the public host key fingerprint, generated when the IPSM is installed into the EAGLE 5 ISS, re initialized using the **`init-card`** command, or when the IPSM is brought into service with the **`alw-card`** or **`rst-card`** commands, into the FTRA. This procedure must be performed for each IPSM on each EAGLE 5 ISS that the FTRA will connect to, but only for EAGLE 5 ISSs using secure connections to connect to the FTRA. This procedure must be performed before any secure connection between the EAGLE 5 ISS and the FTRA can be initiated.

NOTE: Once the IPSM is installed into the EAGLE 5 ISS, the public host key fingerprint for the IPSM will change only when power to the IPSM is disrupted by removing the IPSM from the shelf, then reinserting the IPSM into the shelf, or as the result of any event that interrupts power to the IPSM. Re initializing the IPSM will not change the public host key fingerprint for the IPSM. This procedure will have to be performed for each public host key fingerprint on the EAGLE 5 ISS that has changed.

The public host key fingerprint is added to the FTRA's **hosts.xml** file. If the public host key fingerprint has not been added to the FTRA's **hosts.xml** file, and you try to initiate a secure connection to the EAGLE 5 ISS, you will receive the following warning message (Figure 43).

Figure 43. IP Address Warning Message

If the warning message shown in Figure 43 is received, either clear the **Secure Connection** check box in the STP Configuration Record for the STP (see the "Modifying an Existing STP Configuration Record" procedure on page 40), or add the public host key fingerprint to the FTRA's **hosts.xml** file using the procedure on page 48.

The verification that the keys are installed on the FTRA is called strict host key checking. By default, strict host key checking is on. This enforces server (EAGLE 5 ISS) strong authentication, designed to provide security between the FTRA and the EAGLE 5 ISS. This also prevents a hostile server from tricking the FTRA into exposing any EAGLE 5 ISS login and password combinations.

CAUTION: Do not set strict host key checking to off, unless your network is in a controlled and secure environment. If you set strict host key checking to off, the Connectivity Test Log will warn you each time you try to connect that the EAGLE 5 ISS public host key fingerprint has not been added to the hosts.xml file on the FTRA.

To set the strict host key flag:

1. Open the application start file using any text file editor. On the Windows platform, open the **`ftra.bat`** file. On the UNIX platform, open the **`ftra`** file.

2. Insert into the application start file, one of these text strings, depending on whether you want strict host key checking on or off.

   - **`-DstrictHostKeyChecking=1`** for setting strict host key checking to on (this is the default setting).
   - **`-DstrictHostKeyChecking=0`** for setting strict host key checking to off

   This text string can be inserted anywhere between the **`%JRE_HOME%\bin\java`** and **`-cp`** text strings as shown in the following example.

   ```
   %JRE_HOME%\bin\java -Dstricthostkeychecking=1 -Ddebuglevel=2
   -Dsshtools.home=%FTRA2_HOME% -Dftra2rootdir=%FTRA2_HOME% -cp ftra3.jar
   com.tekelec.ftra.gui.InterfaceSelector %1
   ```

3. Save the changes and close the application start file.

Procedure

1. On the EAGLE 5 ISS, enter the **rtrv-trm** command. The location of the IPSM is shown in the **LOC** column with the **TELNET** terminal type.

This is an example of the possible output.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
TRM  TYPE     COMM         FC    TMOUT MXINV DURAL
1    VT320    9600-7-E-1   SW    30    5     99:59:59
2    KSR      9600-7-E-1   HW    30    5     INDEF
3    PRINTER  4800-7-E-1   HW    30    0     00:00:00
4    VT320    2400-7-E-1   BOTH  30    5     00:30:00
5    VT320    9600-7-O-1   NONE  30    5     00:00:30
6    VT320    9600-7-E-2   SW    30    9     INDEF
7    PRINTER  9600-7-N-2   HW    30    5     00:30:00
8    KSR     19200-7-E-2   BOTH  30    5     00:30:00
9    VT320    9600-7-E-1   SW    30    7     00:30:00
10   VT320    9600-7-E-1   HW    30    5     00:30:00
11   VT320    4800-7-E-1   HW    30    5     00:30:00
12   PRINTER  9600-7-E-1   HW    30    4     00:30:00
13   VT320    9600-7-O-1   NONE  30    5     00:30:00
14   VT320    9600-7-E-2   SW    30    8     00:30:00
15   VT320    9600-7-N-2   HW    30    5     00:30:00
16   VT320    9600-7-E-2   BOTH  30    3     00:30:00

TRM  TYPE      LOC              TMOUT MXINV DURAL      SECURE
17   TELNET    1111             60    5     00:30:00   yes
18   TELNET    1111             60    5     00:30:00   yes
19   TELNET    1111             60    5     00:30:00   yes
20   TELNET    1111             60    5     00:30:00   yes
21   TELNET    1111             60    5     00:30:00   yes
22   TELNET    1111             60    5     00:30:00   yes
24   TELNET    1111             60    5     00:30:00   yes

TRM  TRAF LINK SA  SYS PU  DB  UIMRD
1    NO   YES  NO  YES NO  YES YES
2    NO   NO   NO  NO  NO  NO  NO
3    YES  YES  YES NO  YES YES YES
4    YES  NO   NO  NO  NO  NO  NO
5    NO   YES  NO  NO  NO  NO  YES
6    NO   NO   YES NO  NO  NO  NO
7    YES  YES  YES YES YES YES YES
8    NO   NO   NO  NO  YES NO  YES
9    NO   YES  NO  NO  NO  YES NO
10   NO   NO   NO  NO  NO  NO  YES
11   YES  YES  YES YES YES YES YES
12   YES  YES  YES YES YES YES YES
13   NO   YES  NO  NO  NO  NO  YES
14   NO   NO   YES NO  NO  NO  NO
15   YES  YES  YES NO  YES YES YES
16   NO   NO   NO  NO  YES NO  YES
17   NO   NO   NO  NO  NO  NO  NO
18   NO   NO   NO  NO  NO  NO  NO
19   NO   NO   NO  NO  NO  NO  NO
20   NO   NO   NO  NO  NO  NO  NO
21   NO   NO   NO  NO  NO  NO  NO
22   NO   NO   NO  NO  NO  NO  NO
23   NO   NO   NO  NO  NO  NO  NO
24   NO   NO   NO  NO  NO  NO  NO
```

2. Display the IP address assigned to the IPSM using the **rtrv-ip-lnk** command, specifying the card location of the IPSM shown in step 1 and the **port=a** parameter. For this example, enter this command.

   rtrv-ip-lnk:loc=1111:port=a

   The following is an example of the possible output.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
LOC   PORT IPADDR          SUBMASK        DUPLEX SPEED MACTYPE AUTO MCAST
1111  A    192.168.54.96    255.255.255.0  HALF   100   DIX     NO   NO
```

NOTE: If the Security Administration (SA) setting for all the terminals assigned to the IPSM specified in this procedure is set to YES, see the rtrv-trm output in step 1, skip this step and go to step 4.

3. Change the Security Administration setting on the terminals assigned to the IPSM with the **chg-trm** command and specifying the number of the terminals whose Security Administration setting is **NO**, and with the **sa=yes** parameter.

   chg-trm:sa=yes:trm=<TELNET terminal number>

   When the **chg-trm** command has successfully completed, this message should appear.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
CHG-TRM: MASP A - COMPLTD
```

NOTE: When the IPSM is installed into the EAGLE 5 ISS, UIM 1493 is generated. UIM 1493 contains the DSA key fingerprint to be added to the hosts.xml file. If you recorded the DSA key fingerprint for the IPSM when UIM 1493 was generated, skip step 4 and go to step 5.

CAUTION: If you are performing step 4 from a telnet terminal, make sure the step is being performed from a telnet terminal that is not assigned to the IPSM being initialized. When the IPSM is initialized, you will lose all telnet connections supported by the IPSM being initialized.

4. Obtain the DSA key fingerprint for the IPSM by performing the init-card command and specifying the location of the IPSM. For this example, enter this command.

   init-card:loc=1111

   After the **init-card** command has been executed, UIM 1494 is generated. The DSA key fingerprint is at the end of the output, in the hexadecimal format, and shown in bold in this output example.

```
rlghncxa03w 05-09-17 15:08:45 GMT EAGLE5 34.0.0
0021.1494    CARD 1111     INFO    SSH Host Keys Loaded
             DSA Server Host Key FTRA-formatted Fingerprint=
             84 7c 92 8b c 7c d8 19 1c 6 4b de 5c 8f c5 4d
             Report Date:05-03-17  Time:15:08:45
```

NOTE: If you wish to change the public host key fingerprint on the IPSM, remove and reinsert the IPSM. The public host key fingerprint does not change until the IPSM loses power. However, contact the Customer Care Center before removing and reinserting the IPSM. Refer to page 5 for the contact information.

5. Edit the FTRA **hosts.xml** file (in the **$FTRA_HOME/cfg** directory on Unix or **%FTRA_HOME%\cfg** folder on Windows), using any text file editor. Add the:

   - IPSM IP address from the **rtrv-ip-lnk** output shown in step 2
   - DSA public key fingerprint, shown in either the output of UIM 1493, when the IPSM was installed, or from the output of UIM 1494 when the **init-card** command was performed in step 4 in the following format:

```
<AllowHost HostName="<IPSM IP Address>" Fingerprint="767: <DSA public key fingerprint>"/>
```

NOTE: The value 767 preceding the DSA public key fingerprint is the length of the key in bytes. On your EAGLE 5 ISS, this value may be different. refer to the FTRA Connectivity Test Log to verify this value. The outputs of UIM 1493 or 1494 do not contain this value.

The following is a sample **/ftra/cfg/hosts.xml** file before the new DSA fingerprint information is added.

```
====================================
<?xml version="1.0" encoding="UTF-8"?>

<HostAuthorizations>
<AllowHost HostName="192.168.54.36" Fingerprint="767: 4a 9 ec d3 70 34 d2 91
f7 8b 75 a8 95 37 98 35"/>
<AllowHost HostName="192.168.54.216" Fingerprint="767: bc 76 ac 53 1e fd 72 16
3e 9c dc d7 23 25 6 59"/>
///-----
/// Add new fingerprints HERE, after last allowed host in the above list.
///-----
</HostAuthorizations>
====================================
```

The sample **/ftra/cfg/hosts.xml** file after the new DSA fingerprint information is added.

```
========================================
<?xml version="1.0" encoding="UTF-8"?>

<HostAuthorizations>
<AllowHost HostName="192.168.54.36" Fingerprint="767: 4a 9 ec d3 70 34 d2 91
f7 8b 75 a8 95 37 98 35"/>
<AllowHost HostName="192.168.54.216" Fingerprint="767: bc 76 ac 53 1e fd 72 16
3e 9c dc d7 23 25 6 59"/>
<AllowHost HostName="192.168.54.96" Fingerprint="767: 84 7c 92 8b c 7c d8 19
1c 6 4b de 5c 8f c5 4d"/>
///-----
/// Add new fingerprints HERE, after last allowed host in the above list.
///-----
</HostAuthorizations>
========================================
```

NOTE: There should be no duplicate IP addresses in this file.

6. Save the file and exit the text editor.

---

7. A secure connection can now be established to the IP address used in this procedure. Either add the STP containing the IP address to the STP Configuration Record (see the "Adding an STP Configuration Record" procedure on page 26), or if the IP address is already defined in the STP Configuration Record, change the existing record for this STP with the IP address used in this procedure (see the "Modifying an Existing STP Configuration Record" procedure on page 40). Whether adding a new STP record, or changing an existing STP record, make sure the **Secure Connection** check box is checked.

---

8. After the STP record has been added or changed to use a secure connection, test the connection by performing the "Testing an STP Configuration Record" procedure on page 35. If the connection test is passed, the public host key fingerprint is successfully installed.

   If the connection is refused, make sure that the key information for the EAGLE 5 ISS and the FTRA shown in the Connectivity Test Log match. The Connectivity Test Log shows both the key received from the EAGLE 5 ISS host and the key contained in the **hosts.xml** file for the EAGLE 5 ISS host. The following is an example from the Connectivity Test Log containing a host key mismatch. The key received from the EAGLE 5 ISS host is shown in bold. The key contained in the **hosts.xml** file is shown in bold underline.

```
2003-07-11 14:22:56.117: Stp Connectivity Test Process Manager: Testing STP11805011201
2003-07-11 14:22:56.227: Telnet Terminal Session Manager: Initiating Secure Telnet
Session with Eagle: 192.168.53.71:22
2003-07-11 14:22:56.808: HostKeyVerification: ERROR: Host 192.168.53.71 cannot be
authenticated due to a mismatched entry for this host in the hosts.xml file. The host key
supplied by 192.168.53.71 is: 768: bb 7d 79 a2 7d ae 5d 5a 45 e2 44 58 cd 8a bd 83.
The current allowed key for 192.168.53.71 is: 768: ab 7d 79 a2 7d ae 5d 5a 45 e2 44 58 cd
8a bd 83.

2003-07-11 14:22:56.828: HostKeyVerification: Connection rejected...onHostKeyMismatch
```

FTP Server Configuration

An FTP server must be configured on the EAGLE 5 ISS using the **FTP Server Configuration** menu before database tables can be retrieved from the EAGLE 5 ISS, or command files can be sent to the EAGLE 5 ISS.

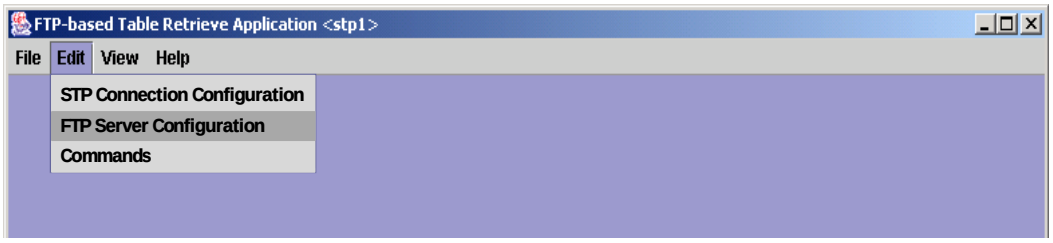
NOTE: If the Secure Connection box in the STP Connection Configuration Menu window is checked, the IP address specified in the FTP Server Configuration menu must be the IP address of a secure FTP server. If the Secure Connection box in the STP Connection Configuration Menu window is not checked, the IP address specified in the FTP Server Configuration menu must be the IP address of a FTP server.

NOTE: Any firewall between the FTRA and the FTP server configured in the FTP Server Configuration Menu window (Figure 45 on page 53), must allow FTPs to the IP address specified in the FTP Server Configuration Menu window.

Procedure

1. Select **Edit > FTP Server Configuration** from the **FTP-based Table Retrieve Application** menu. See Figure 44.

   Figure 44. FTP Server Configuration Menu in the FTP-Based Table Retrieve Application Window



   The **FTP Server Configuration Menu** window opens. See Figure 45 on page 53 and Table 3 on page 53.

Figure 45. FTP Server Configuration Menu Window

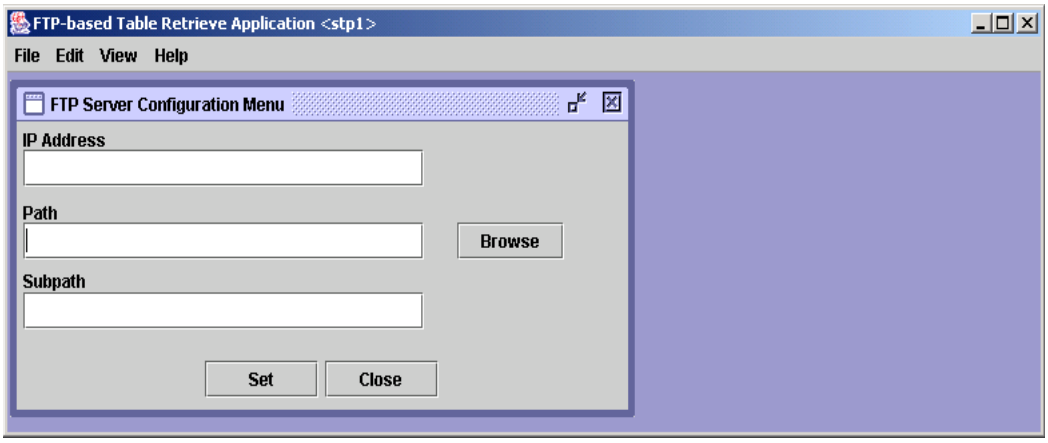


Table 3. FTP Server Configuration Menu Window Descriptions

Item	Description
Fields	
IP Address	The IP Address of the associated STP
Path	The complete path to the data tables transfer directory on the STP. This directory must be given complete read/write/execute permissions for all users. From Windows, this is commonly administered from within the FTP server software. From Unix, this is done with the **`chmod`** command. Please refer to your PC system documentation or Unix **`man`** pages for full details on setting directory permissions.
Subpath	The value used by the **`path`** parameter of the EAGLE 5 ISS **`ent-ftp-serv/chg-ftp-serv`** commands. The subpath is relative to the user's default directory upon FTP login. A file separator ('\' or '/') is not used to begin the subpath string.
Buttons	
Browse	Opens the **Select Starting Directory** window to initiate a directory/file selection dialog for the data tables.
Set	Stores the FTP server configuration data.
Close	Closes the **FTP Server Configuration Menu** window.

2. Enter the IP address of the STP in the **IP Address** field.

   NOTE: If the format is not entered correctly, the Invalid IP Address warning window is displayed. See Figure 46 on page 54.

Figure 46. Invalid IP Address Error Message

3. Enter the path for the FTP temporary data table storage area or click the **Browse** button.

   If the **Browse** button is clicked, the **Select Starting Directory** window opens to select the location for the temporary data table storage area to be entered in **Path** field. See Figure 47 and Table 4 on page 55.

   This directory must be given complete read/write/execute permissions for all users. From Windows, this is commonly administered from within the FTP server software. From Unix, this is done with the **`chmod`** command. Please refer to your PC system documentation or Unix **`man`** pages for full details on setting directory permissions.

Figure 47. Select Starting Directory Window

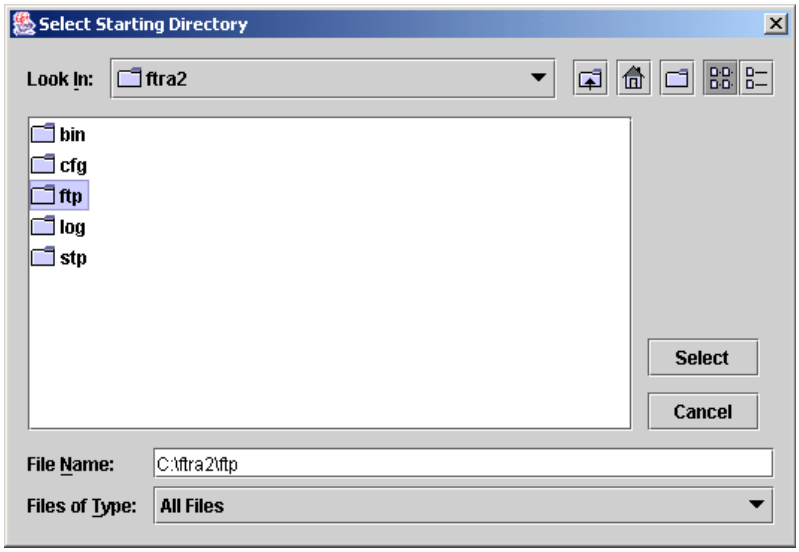
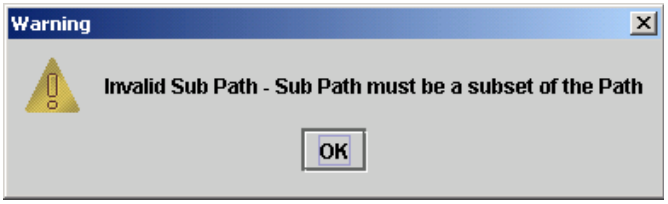


Table 4. Select Starting Directory Window Descriptions

Item	Description
Fields	
Look in:	A drop down menu that allows the user to browse through the directory structures.
File Name:	The name of the file to be selected.
Files of type:	A drop down menu that allows the user to select all files of a particular type.
Buttons	
Select	Takes the contents of the **File Name** field and loads it into the **Path** field of the menu
Cancel	Closes the **Select Starting Directory** window.

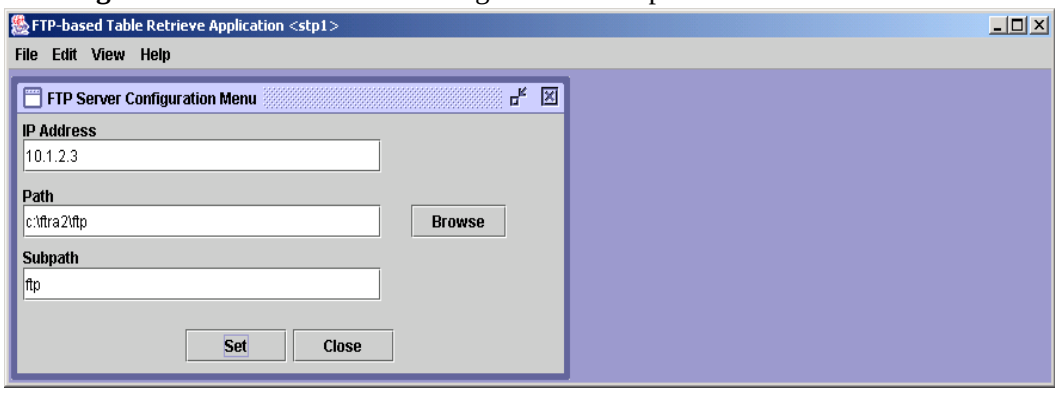
4. Enter the Subpath. The subpath must always be the last part of the path. The subpath is relative to the user's default directory upon FTP login. A file separator ('\' or '/') is not used to begin the subpath string. If an invalid Subpath is entered, a warning window opens. See Figure 48.

Figure 48. Invalid Subpath Window



5. Click the **Set** button. See Figure 49

Figure 49. FTP Server Configuration Example



The **FTP Server Data Set** window opens. See Figure 50.

Figure 50. FTP Server Data Set Window

Click **OK** to continue.

Retrieve Database Tables from an STP

Retrieve Tables Window

The **Retrieve Tables** window (see Figure 52 on page 58) is used to select the database tables you wish to retrieve from the selected STP. The **Retrieve Tables** window contains a list of predefined retrieve commands. Any number of the retrieve commands can be selected from the **Command List** box and moved to the **Selected Commands** box. Clicking the **Retrieve** button causes the database tables associated with the selected retrieve commands to be transferred from the selected STP.

The **Retrieve from STP** and **Retrieve from Local Database** buttons determine whether new database tables are retrieved from the selected STP or if existing tables already retrieved from that STP will be used. If no tables exist for the selected STP, the **Retrieve from Local Database** button will be grayed out.

The output from the retrieve commands is converted to CSV files. When the retrieve operation is completed, the **Command Complete** window opens notifying the user if the retrieve was executed with or without errors. The Retrieve Tables Log opens allowing the user to view the events.

CAUTION: With FTRA 4.0, if you attempt to retrieve and convert the database tables for these GTT commands (`rtrv-tt`, `rtrv-gtt`) and these EGTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`) in the same retrieve tables request, you will receive a warning (Figure 51) that errors can be caused by attempting to retrieve and convert the GTT and EGTT database tables from the same EAGLE 5 ISS.

You may only retrieve and convert the tables corresponding to which feature is on, GTT or EGTT. If the EGTT feature is on, shown in the `rtrv-feat` output, the database tables for the `rtrv-gttsel`, `rtrv-gttset`, and `rtrv-gta` commands can be retrieved and converted. If the EGTT feature is off, the database tables for the `rtrv-tt` and `rtrv-gtt` commands can be retrieved and converted.

The errors will be caused when the retrieved GTT and EGTT database tables are converted to CSV files. Because only one set of the database tables, GTT or EGTT, can be retrieved, only that set of the database tables can be converted. The error will occur when the attempt is made to convert that database tables that could not be retrieved.

Figure 51. GTT Warning Window

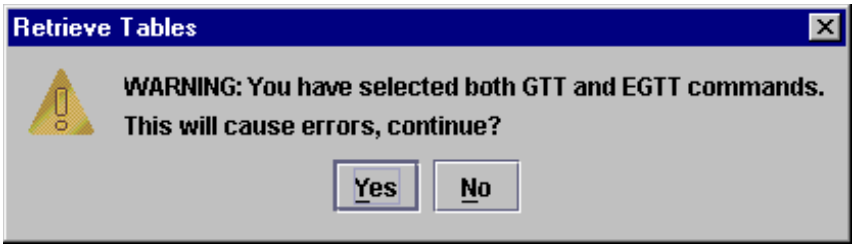


Figure 52. Retrieve Tables Window

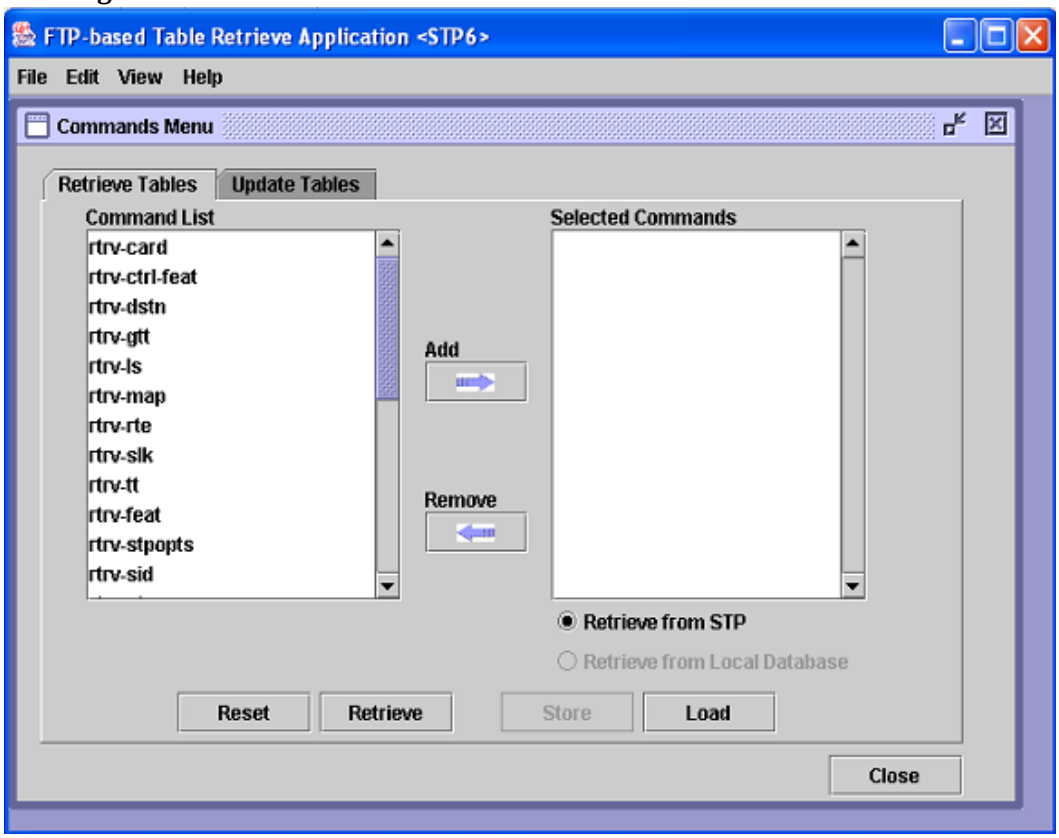


Table 5 on page 59 shows the description of the fields and buttons in the **Retrieve Tables** window.

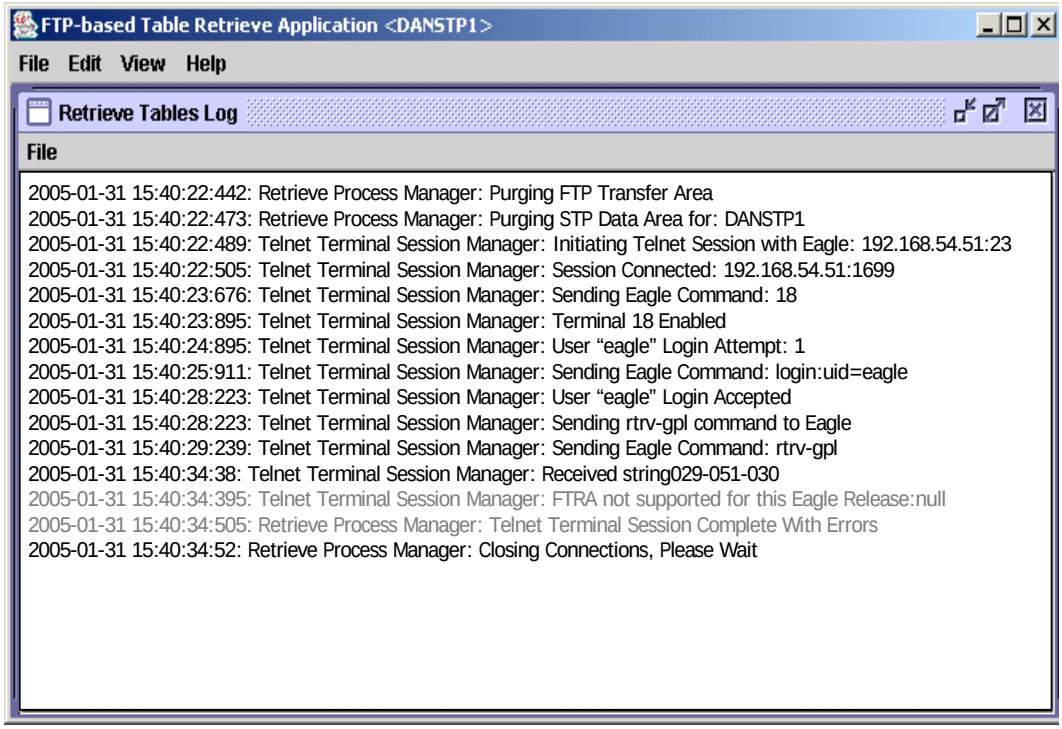
Table 5. Retrieve Tables Window Description

Item	Description
Fields	
Command List	Contains a predefined list of retrieve commands.
Selected Commands	These commands are used to determine which database tables are retrieved from the selected STP. From one to all of the retrieve commands can be selected for retrieval.
Buttons	
Add	Moves the highlighted commands from the **Command List** box to the **Selected Commands** box.
Remove	Moves any highlighted commands in the **Selected Commands** box back to the **Command List** box and places them in the **Command List** box in alphabetical order.
Reset	Moves all commands in the **Command List** box to the **Selected Commands** box. All highlights in the **Selected Commands** box are removed.
Retrieve	Initiates the retrieval of all the selected database tables represented by the selected retrieve commands. The database tables are transferred using an FTP connection and converted to CSV files.
Store	Stores the commands in the **Selected Commands** box which will be used by the Command Line Interface. This list is maintained even when the FTRA is shut down and restarted.
Load	Loads the commands into the **Selected Commands** box which are currently stored for Command Line Interface usage. This allows the user to verify **`rtrv`** commands which will be executed by the Command Line Interface.
Retrieve from STP	Retrieves the database tables, based on the selected retrieve commands, from the selected STP instead of using the tables previously retrieved.
Retrieve from Local Database	When selected, the FTRA uses the database table previously retrieved from the selected STP.
Close	Closes the **Commands Menu** window.

In FTRA 4.0 the EAGLE 5 ISS release 32.0 and later are supported if that release supports CSV file output.

When a Retrieve Tables command is performed, FTRA 4.0 verifies that the EAGLE 5 ISS is running one of the supported releases. If the EAGLE 5 ISS release is not supported, an error message is displayed and the Retrieve Tables command is terminated. See Figure 53.

Figure 53. Retrieve Table Log - Release Not Compatible Error

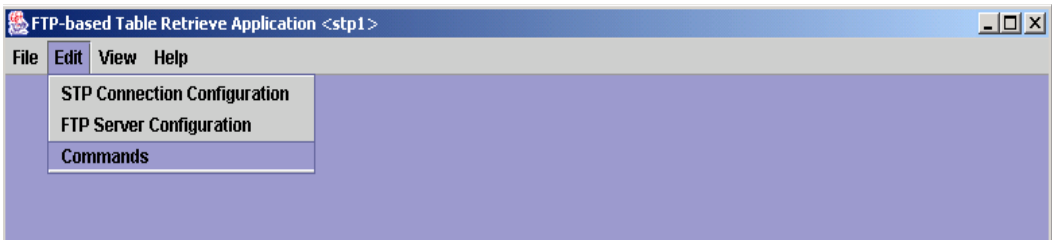


If the EAGLE 5 ISS release is supported, the Retrieve Tables command is performed and operations on the FTRA can continue.

Procedure

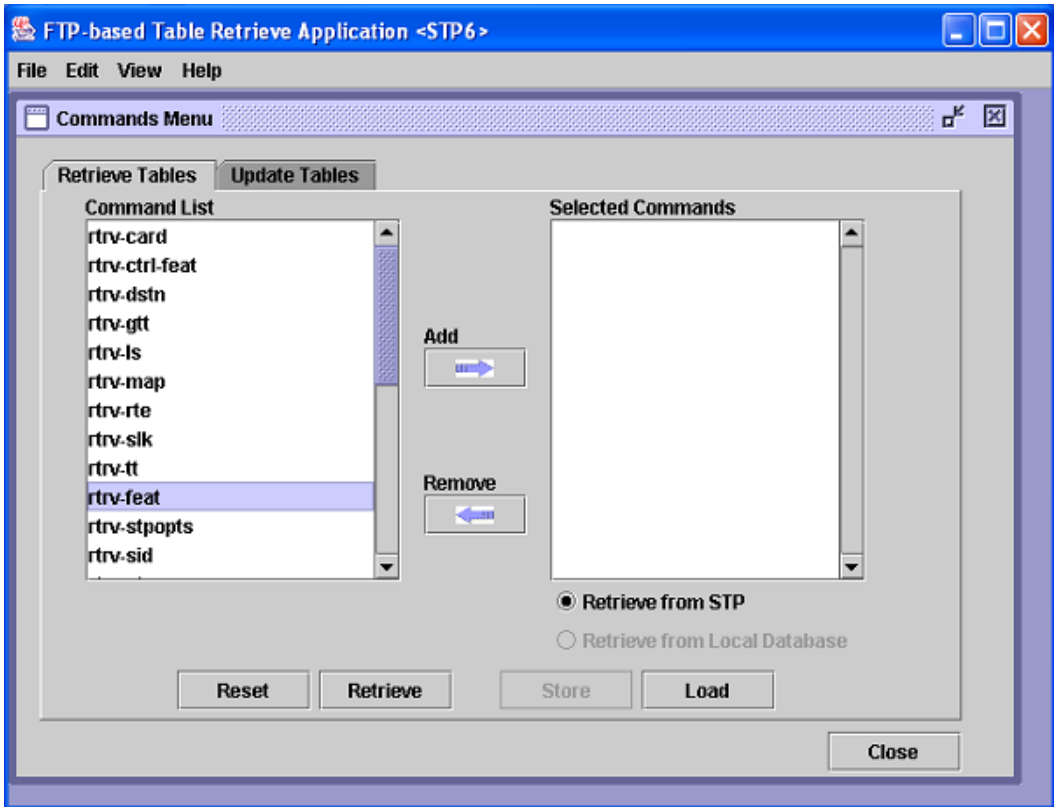
1. Select **Edit > Commands > Retrieve Tables** from the **FTP-Based Table Retrieve Application** window. See Figure 54. The **Retrieve Tables** window opens. See Figure 52 on page 58.

Figure 54. Commands Menu in the FTP-Based Table Retrieve Application Window



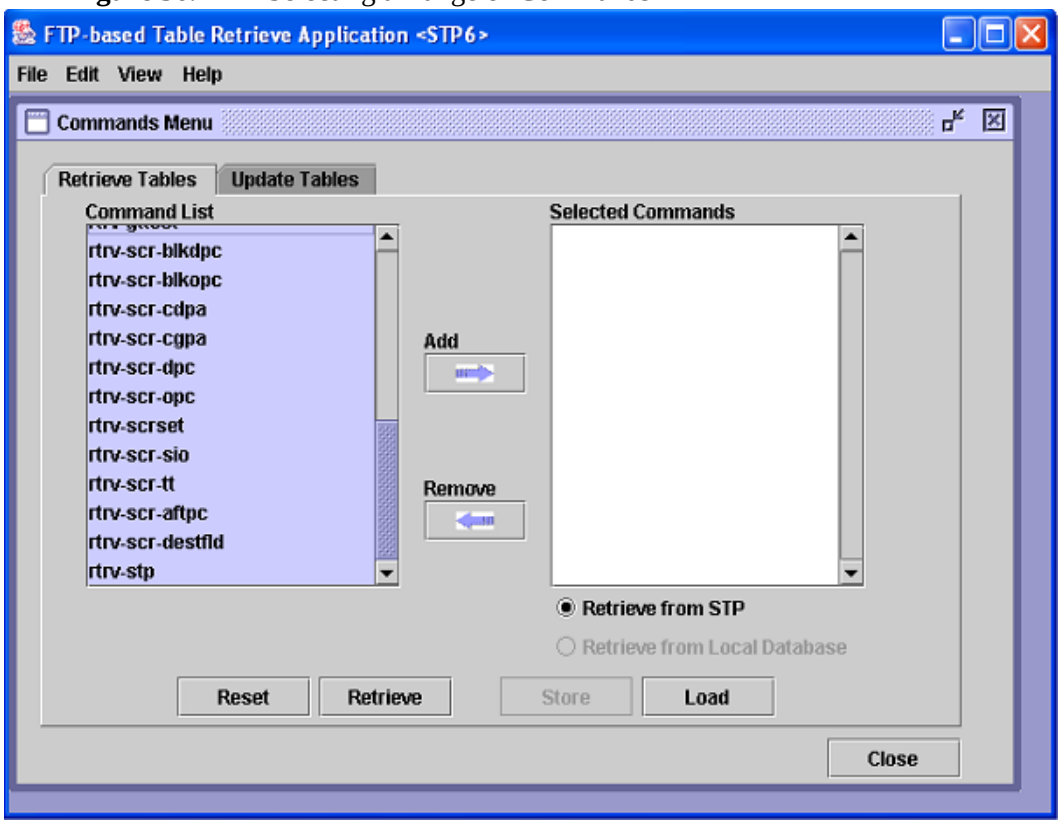
2. To select commands in the **Command List** box of the **Retrieve Tables** window, perform one of these steps:To select a single command, click on the command and it is highlighted. See Figure 55.

Figure 55. Selecting a Command



c. To select a range of commands, click on the first command and while holding down the Shift key, click on the last command to be selected. All the commands in between the selected commands are highlighted, along with the selected commands. See Figure 56.

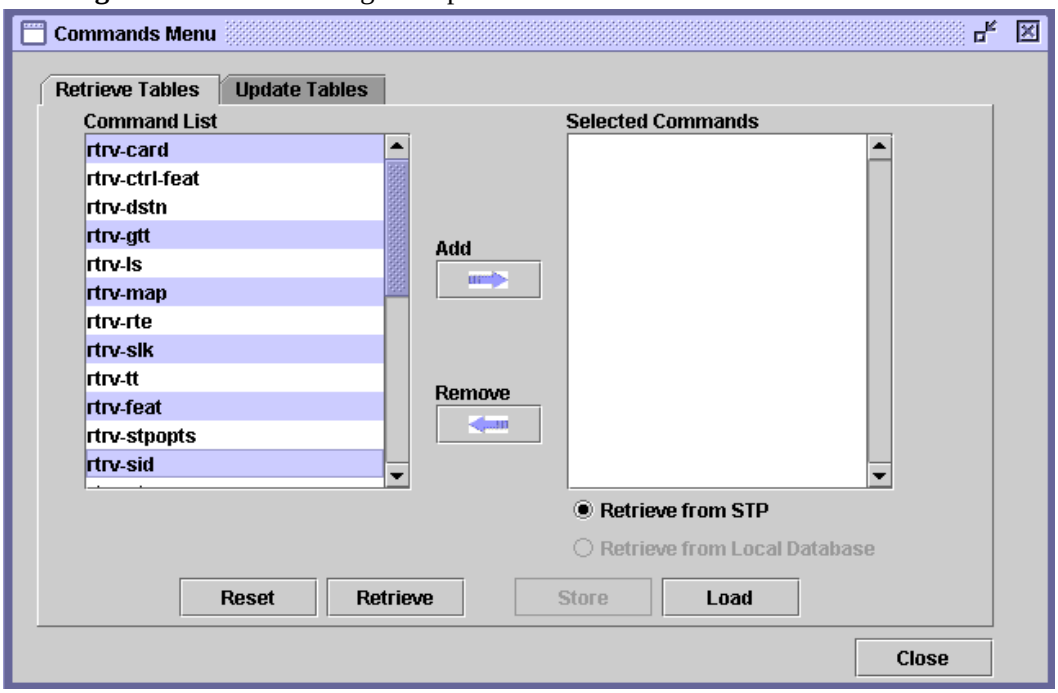
Figure 56. Selecting a Range of Commands



d. To select multiple commands, select the first command, then hold down the Ctrl key and click on each of commands to be selected. The selected commands are highlighted. See Figure 57 on page 63.

NOTE: If you have selected any of these GTT commands (`rtrv-tt`, `rtrv-gtt`) and these EGTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`) in substeps b or c, see the Caution on page 57.

Figure 57. Selecting Multiple Commands



3. To move the commands selected in step 2 to the **Selected Commands** box, click the **Add** button. The commands are moved to **Selected Commands** box. See Figure 58, Figure 59 on page 65, and Figure 60 on page 66.

Figure 58. Adding a Command to the Selected Commands Box

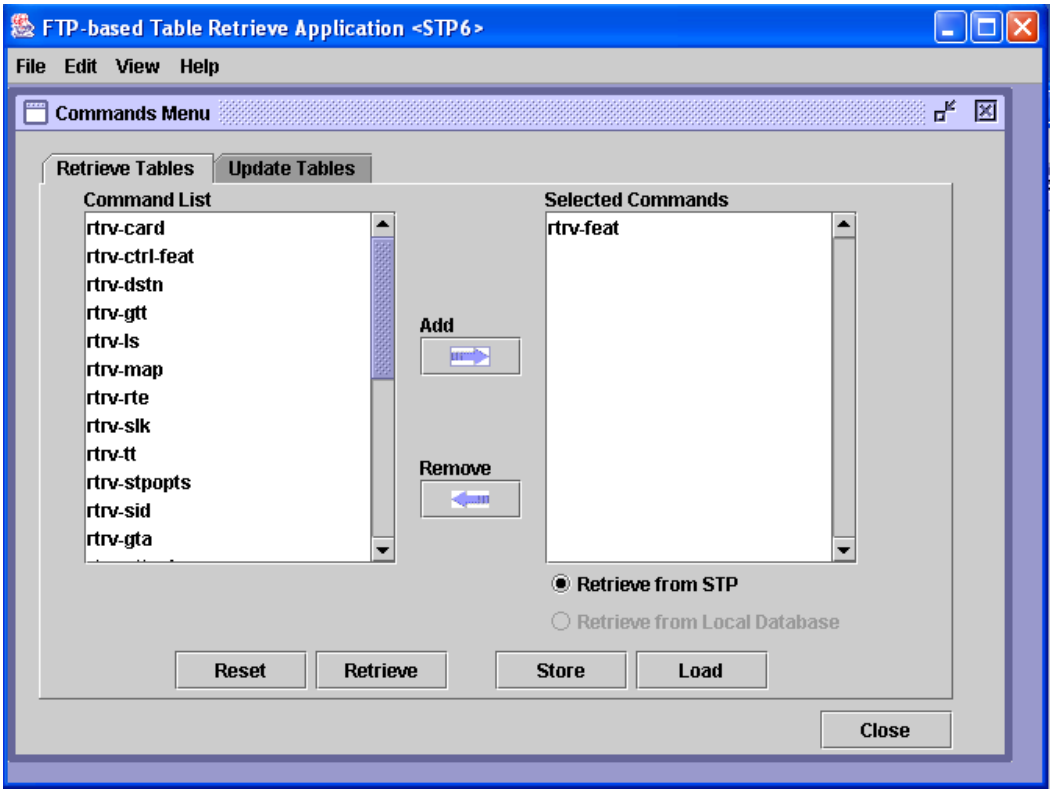


Figure 59. Adding a Range of Commands to the Selected Commands Box

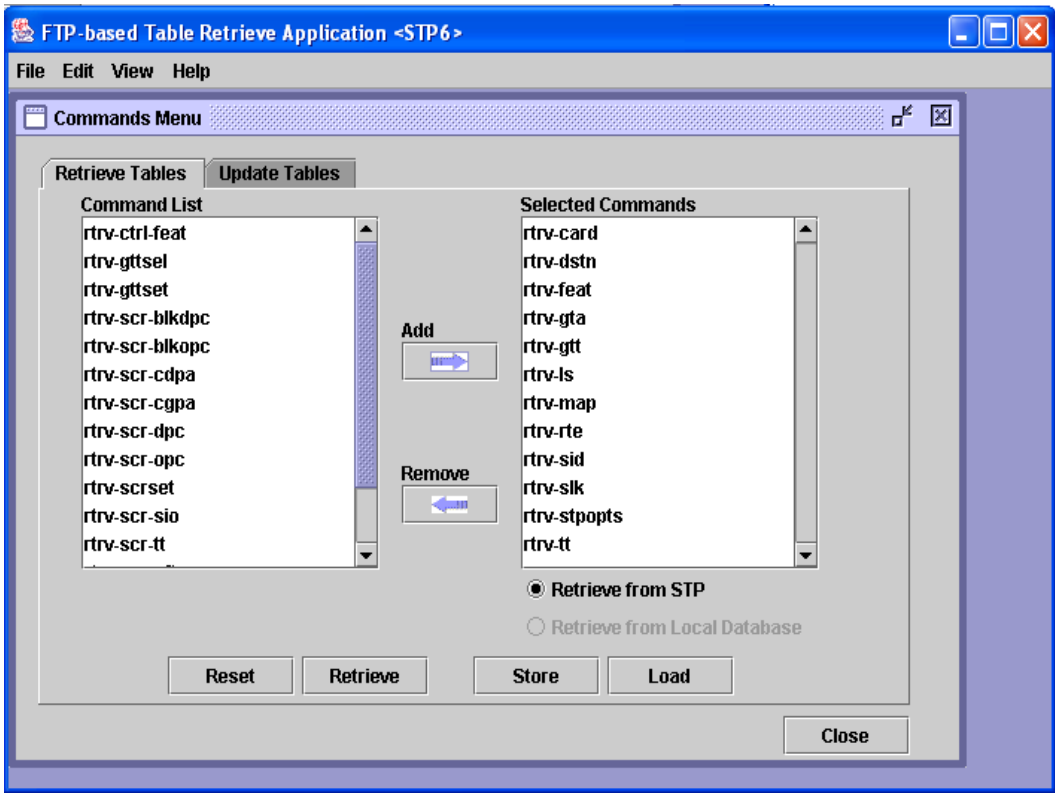
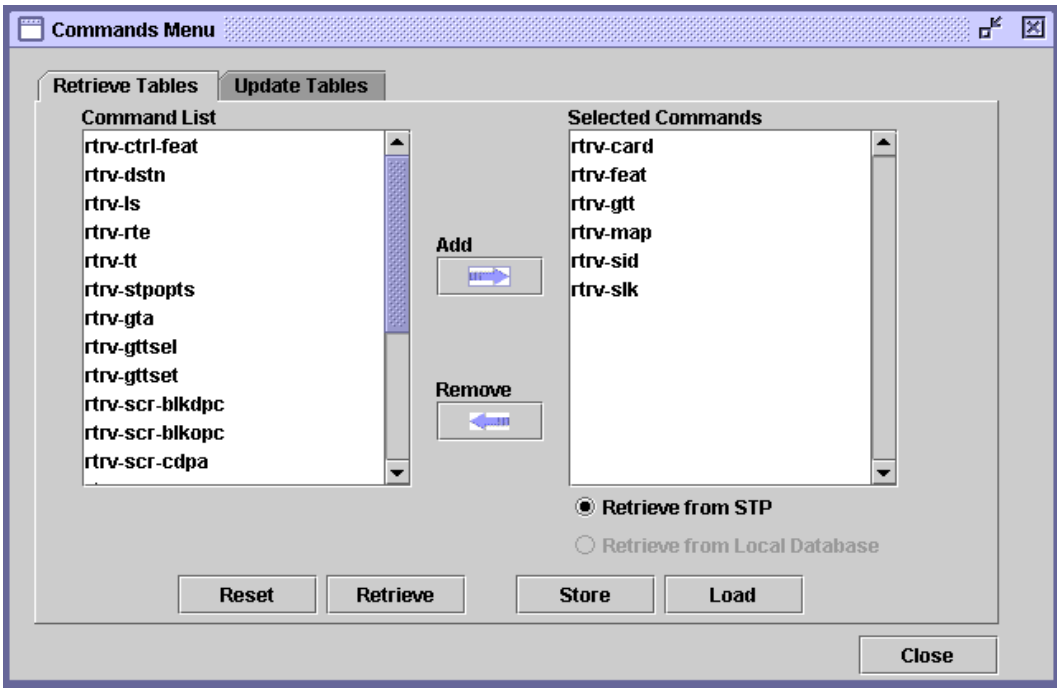


Figure 60. Adding Multiple Commands to Selected Commands Box



NOTE: If no commands are being moved from the Selected Commands box to the Command List box, skip step 4 and go to step 5.

4. To remove commands from the **Selected Commands** box, perform one of these steps:

   a. In the **Selected Commands** box, click on the command to be removed and it is highlighted. Click the **Remove** button. The highlighted command is moved to the **Command List** box. See Figure 61 on page 67.

   b. To select a range of multiple commands to be removed, click on the first command and while holding down the Shift key, click on the last command to be removed. Click the **Remove** button. All highlighted commands are moved to the **Command List** box.

   c. Hold down the Ctrl key and click on each of commands to be removed. Click the **Remove** button. Only the highlighted commands are moved to **Command List** side. See Figure 62 on page 67.

NOTE: When a command is removed from the Selected Commands box, the command is placed in the Command List box in alphabetical order.

   d. Click the **Reset** button. All commands in the **Command List** box are moved to the **Selected Commands** box. All highlights in the **Selected Commands** box are removed.

Figure 61. Command Selected to be Removed in the Selected Commands Box

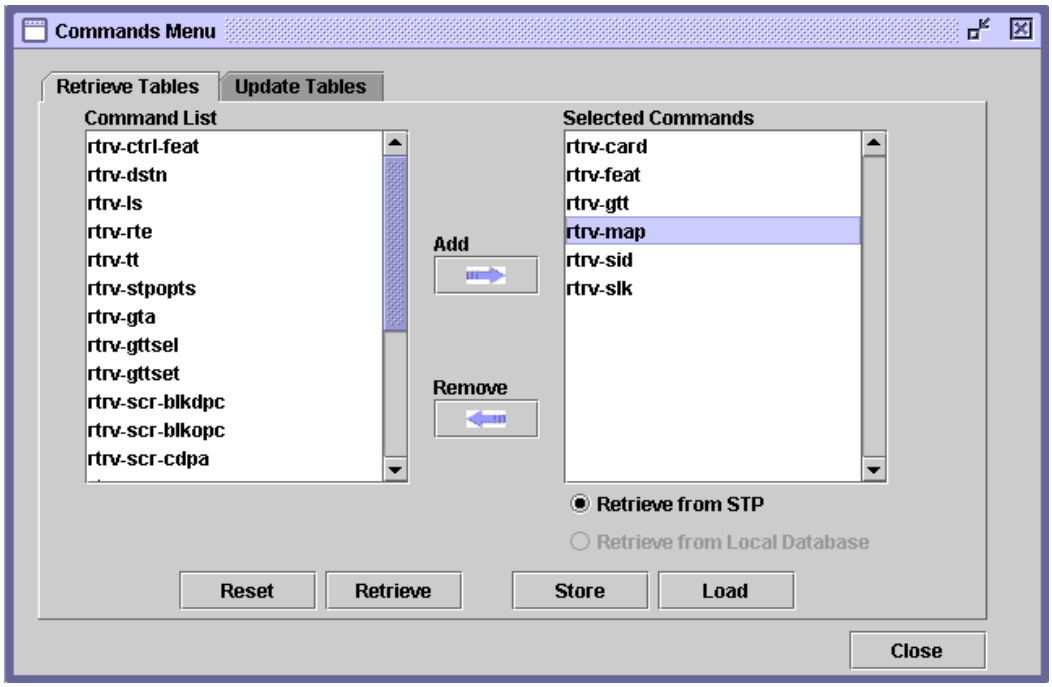
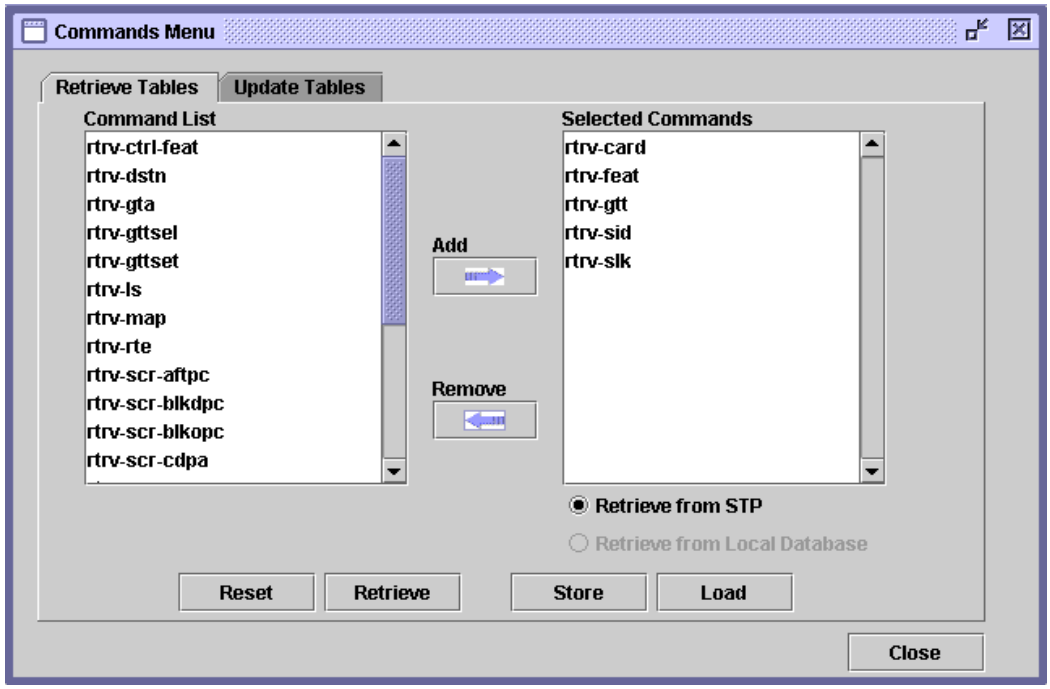


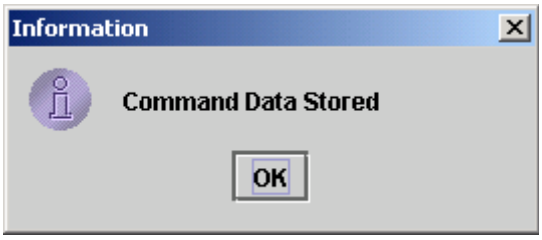
Figure 62. Command Removed from the Selected Commands Box



NOTE: If command information from only the selected STP is being retrieved, and the Command Line Interface is not being used, skip step 5 and go to step 6.

5. To store the selected commands for the Command Line Interface, click the **Store** button on the **Commands Menu** window. The **Command Data Stored** window opens. See Figure 63.

Figure 63. Command Data Stored Window



Click **OK** to continue.

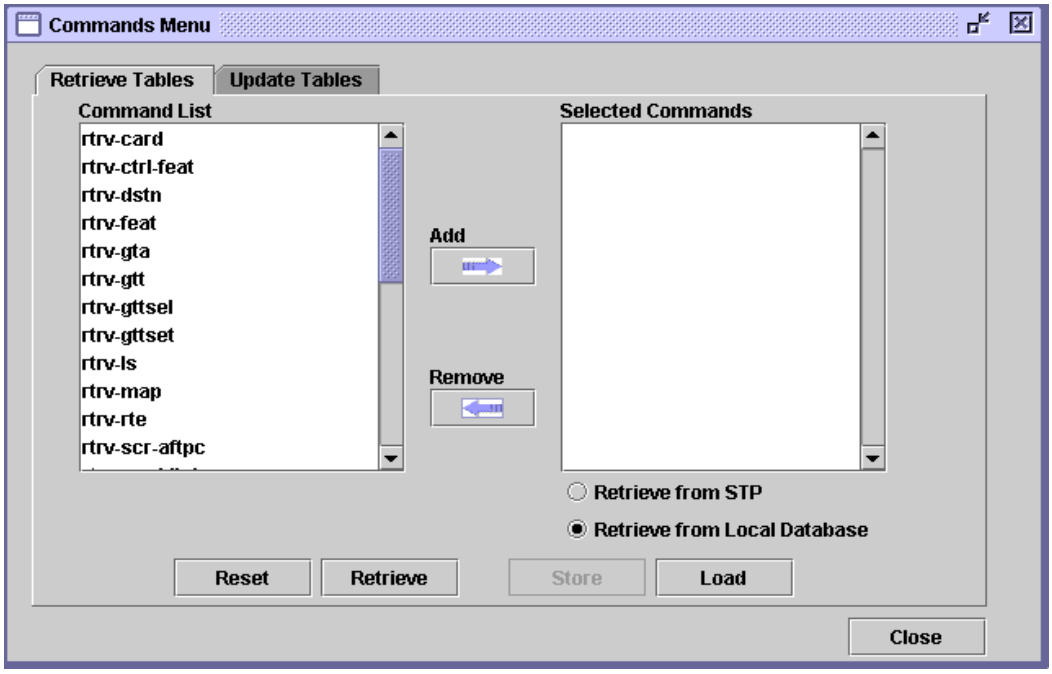
To verify what retrieve commands are stored, click the **Load** button. The stored commands appear in the **Selected Commands** box, as shown in Figure 58 on page 64, Figure 59 on page 65, or Figure 60 on page 66.

To use the Command Line Interface, go to the "Command Line Interface" section on page 79.

NOTE: If database tables are to be retrieved from the selected STP, skip step 6 and go to step 7.

6. To generate CSV files from database tables already retrieved from the selected STP, select the **Retrieve from Local Database** button after selecting the desired commands. See Figure 64 on page 69. Click the **Retrieve** button.

Figure 64. Retrieving Database Tables from the Local Database



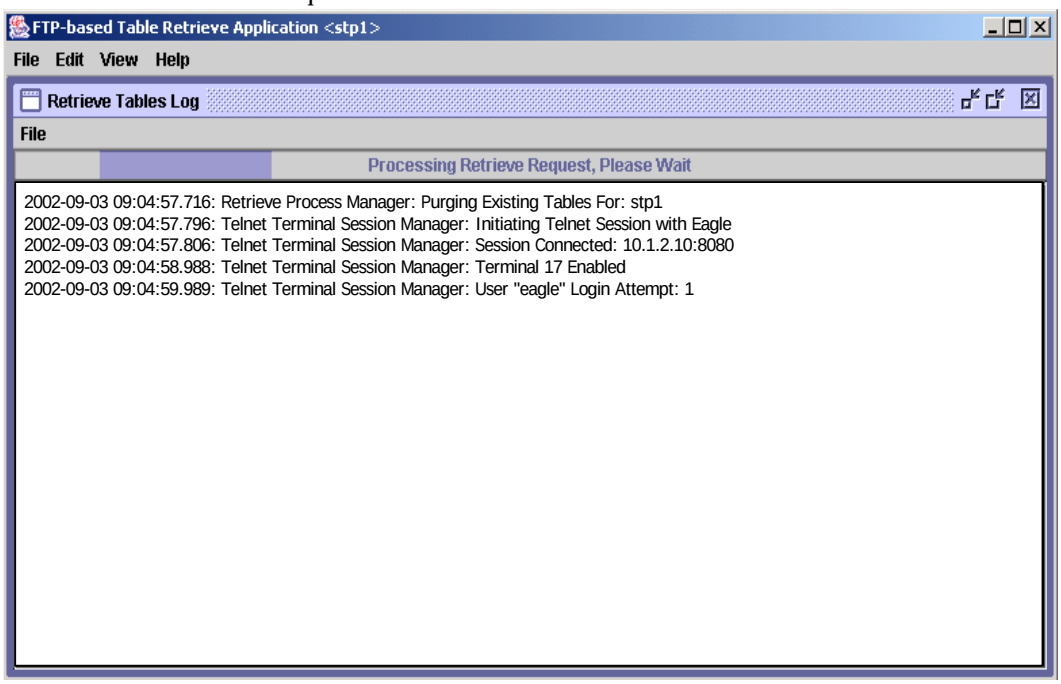
NOTE: If step 6 was performed, skip step 7. This procedure is finished.

7. Retrieve the database tables from the selected STP corresponding to the commands selected in step 2 by selecting the **Retrieve from STP** button, then click the **Retrieve** button. The **Retrieve Tables Log** window opens (see Figure 65 on page 70) and displays the message “Processing Retrieve Request, Please Wait” until the retrieve process completes.

   NOTE: The telnet terminals on the EAGLE 5 ISS to which FTRA will be connecting should have their terminal settings set to `all=no` (use the EAGLE 5 ISS command `chg-trm:trm=<telnet terminal>:all=no` to make this setting; use the EAGLE 5 ISS command `rtrv-trm` to verify the EAGLE 5 ISS terminal settings). On an STP with heavy UIM output, this prevents the FTRA's terminal from being flooded with unrelated output, which could unnecessarily backlog command responses during FTRA operation.

   NOTE: If you are retrieving the database tables for any of these GTT commands (`rtrv-tt`, `rtrv-gtt`) and any of these EGTT commands (`rtrv-gttsel`, `rtrv-gttset`, `rtrv-gta`), see the Caution on page 57.

Figure 65. Retrieve Tables Log Window - Processing Retrieve Request



This message is displayed until the retrieve process completes. The **Command Complete** window opens.

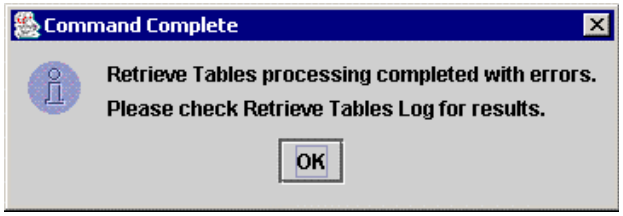
a. If no errors occurred, the text ”Retrieve Tables processing completed without errors.” “Please check Retrieve Tables Log for Results.” appears in the **Command Complete** window. See Figure 66.

Figure 66. Command Complete Window Without Errors

Click **OK**, to continue.

b. If errors occurred, the text ”Retrieve Tables processing completed with errors.” “Please check Retrieve Tables Log for Results.” appears in the **Command Complete** window. See Figure 67 on page 71.

Figure 67. Command Complete Window With Errors



The **Retrieve Table Log** window opens. See Figure 68 on page 72 and Figure 69 on page 73. Click **OK**, to continue.

Retrieve Tables Log

The Retrieve Tables Log contains the events of the retrieve processing and any error messages that may have occurred. The **Retrieve Tables Log** window is opened after database tables have been retrieved from an STP and is displayed until the retrieve processing is complete (see Figure 65 on page 70).

The Retrieve Tables Log displays the information of the CSV files generated for the selected retrieve commands. The filenames of the CSV files are displayed in ascending order except for the filename of the **`rtrv-stp`** CSV file. Since the **`rtrv-stp`** command CSV is not generated by the CSVGEN(X) utility, the CSV filename for the **`rtrv-stp`** command is not displayed in the sorted order with other CSV filenames, but it is displayed as the last entry in the filenames list. Since the Retrieve Tables Log is generated by the CSVGEN(X) utility, no record of processing the **`rtrv-stp`** command is displayed in this log. See Figure 70 on page 73 for an example of the Retrieve Tables Log when the **`rtrv-stp`** command is processed.

The log is automatically cleared when the next set of database tables are retrieved from an STP. Selecting **View > Retrieve Tables Log** from the menu also opens the **Retrieve Tables Log** window. See Figure 68 and Figure 69 on page 73.

Figure 68. Retrieve Tables Log Window without Errors

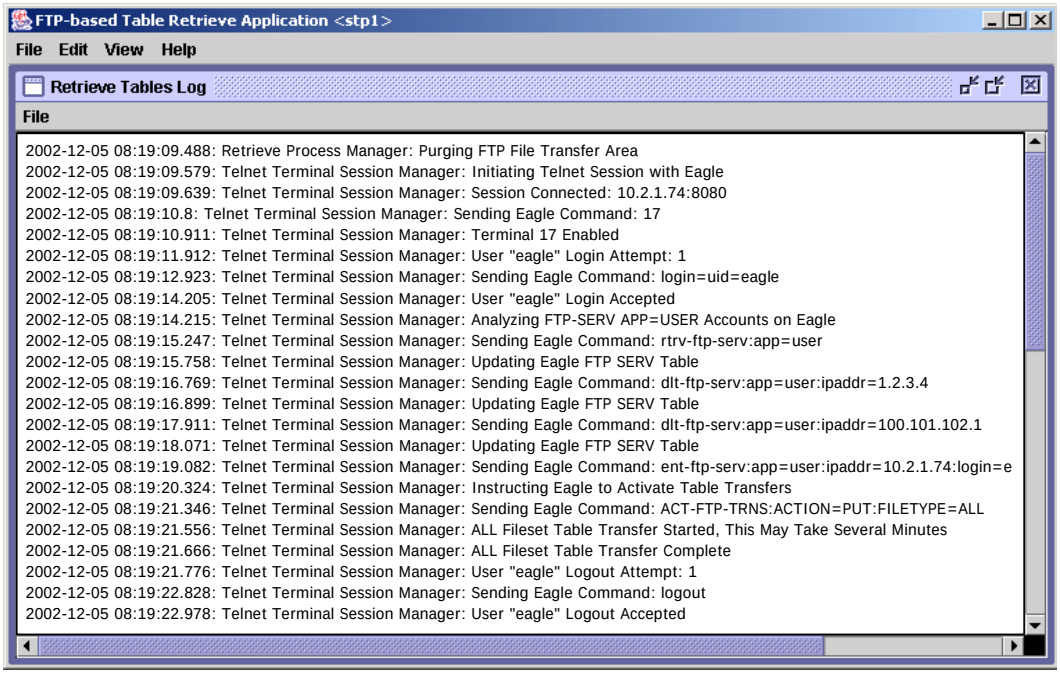


Figure 69. Retrieve Table Log with Errors

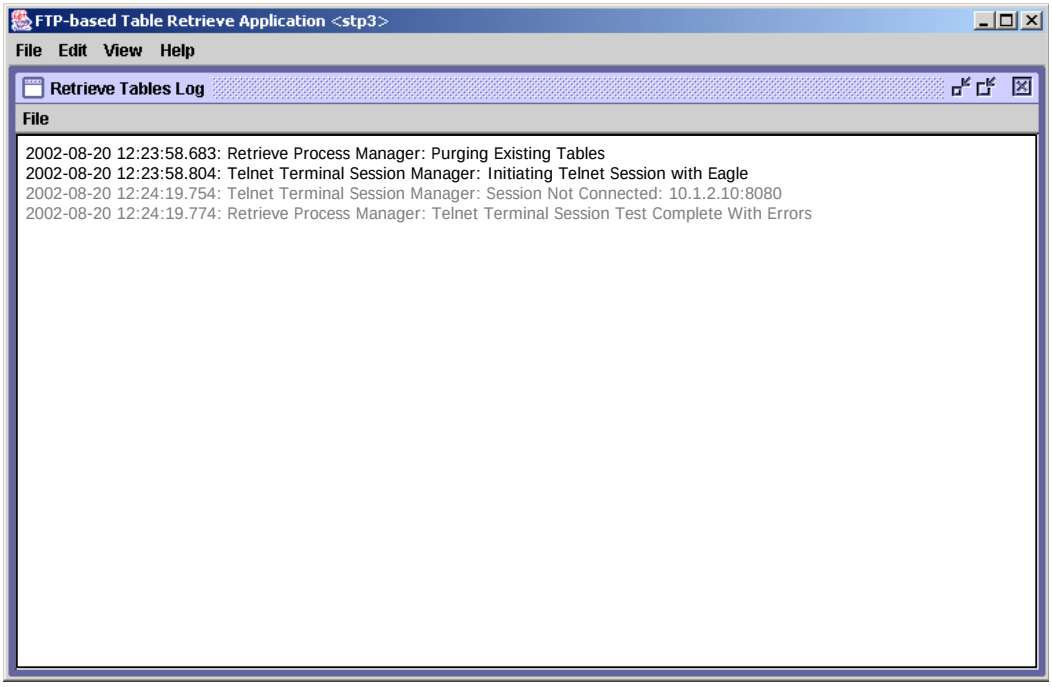
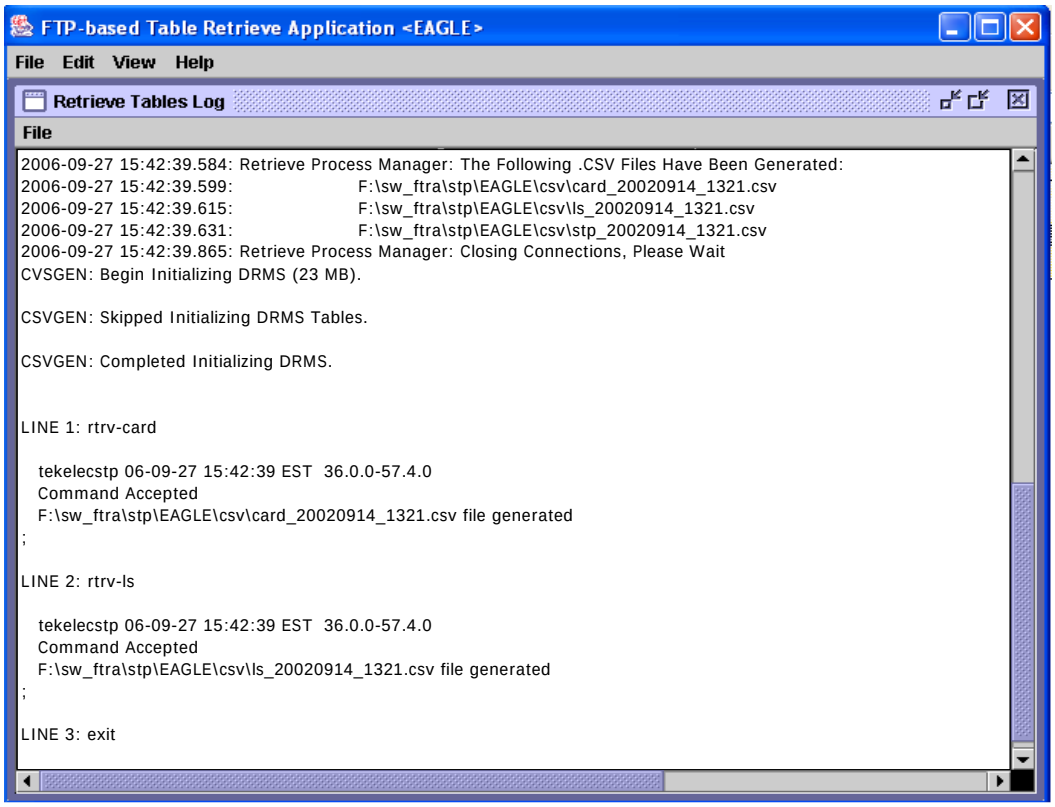


Figure 70. Retrieve Table Log with the RTRV-STP Command

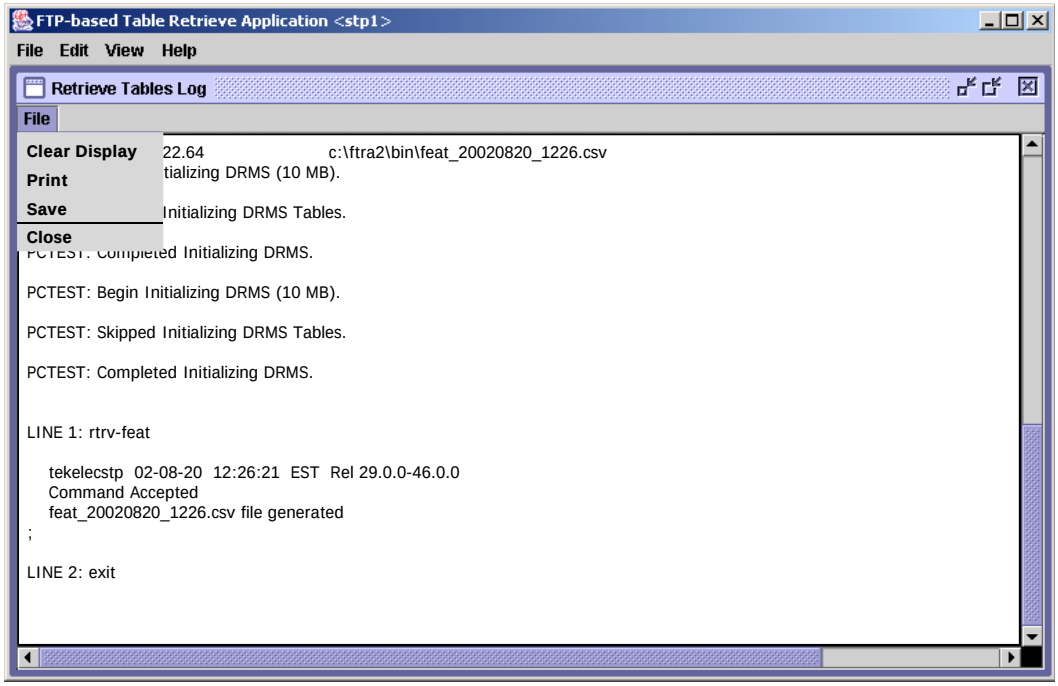


Retrieve Tables Log File Menu

The **File** menu in the **Retrieve Tables Log** window, shown in Figure 71, provides these selections:

- Clearing the Retrieve Tables Log display
- Printing the Retrieve Tables Log
- Saving the Retrieve Tables Log to a file
- Closing the **Retrieve Tables Log** window.

Figure 71. File Menu in the Retrieve Tables Log Window



Clearing the Retrieve Tables Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is saved to a file or printed before the display is cleared.

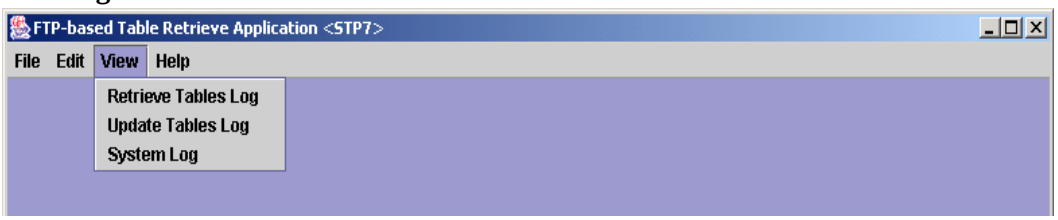
Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Clear Display** in the **Retrieve Tables Log** window. See Figure 71.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 72. The **Retrieve Tables Log** window opens.

Figure 72. View Menu



3. Select **File > Clear Display** in the **Retrieve Tables Log** window. The Retrieve Tables Log display clears.

Printing the Retrieve Tables Log

Procedure

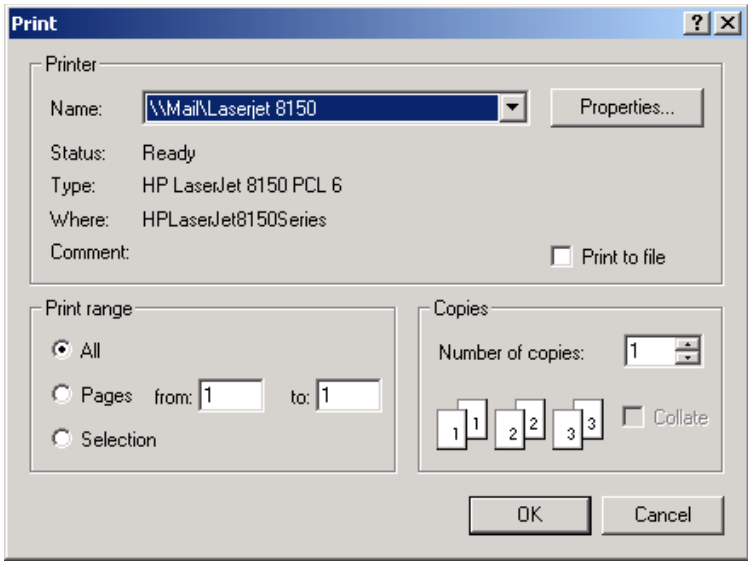
NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Print** in the **Retrieve Tables Log** window. See Figure 71 on page 74.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 72. The Retrieve Tables Log opens.

3. Select **File > Print** in the **Retrieve Tables Log** window. The **Print** window opens. See Figure 73 on page 76.

Figure 73. Print Window



4. Configure the printer settings.

5. To print the Retrieve Tables Log, click the **OK** button in the **Print** window. The current contents of the Retrieve Tables Log are printed.

6. If you decide not to print the Retrieve Tables Log, click the **Cancel** button in the **Print** window.

Saving the Retrieve Tables Log to a File

Procedure

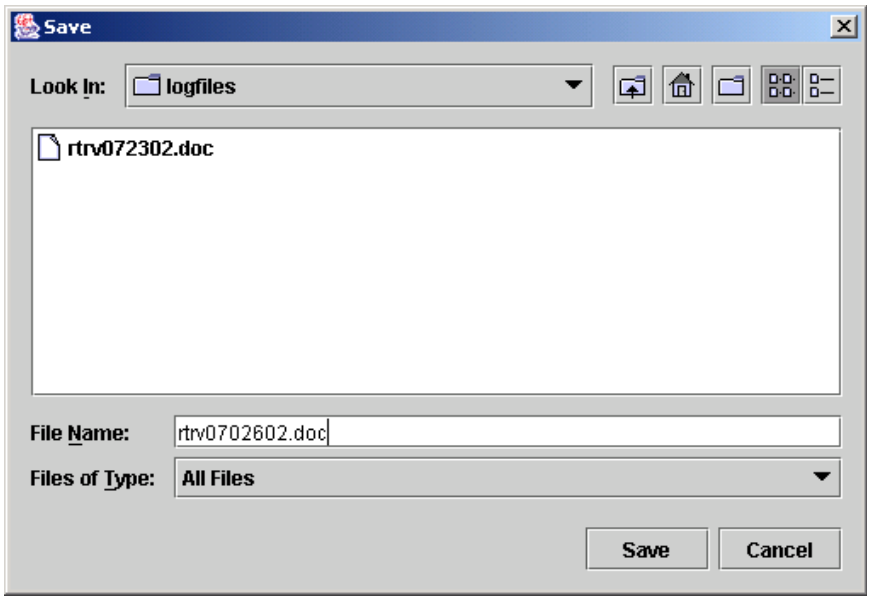
NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Save** in the **Retrieve Tables Log** window. See Figure 71 on page 74.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 72 on page 75. The **Retrieve Tables Log** window opens.

3. Select **File > Save** in the **Retrieve Tables Log** window. The **Save** window opens. See Figure 74 on page 77.

Figure 74. Save Window



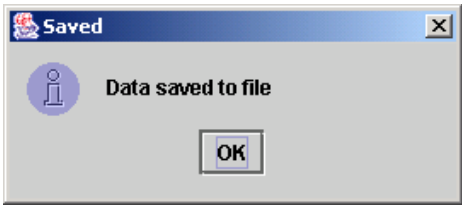
4. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

   NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.

   NOTE: If you decide not to save the file, do not perform steps 5 and 6, but click Cancel in the Save window.

5. Click the **Save** button. A **Saved** file confirmation window opens with "Data saved to file." See Figure 75.

   Figure 75. Saved File Confirmation Window



6. To save the file, click **OK** in the **Saved** file confirmation window to continue.

Closing the Retrieve Tables Log Window

Procedure

1. Select **File > Close** in the **Retrieve Tables Log** window, or click the close window button in the upper right hand corner of the **Retrieve Tables Log** window. See Figure 71 on page 74. The **Retrieve Tables Log** window closes.

Command Line Interface

The FTRA Command Line Interface allows the user to retrieve the same database tables, using the EAGLE 5 ISS's retrieve commands, from all configured STPs in the STP configuration database. The **Store** and **Load** buttons in the **Retrieve Tables** window are used to select these retrieve commands. See "Retrieve Database Tables from an STP" on page 57.

The Command Line Interface for FTRA 4.0 allows the user to change the STP Username and Password for an STP already configured in the system.

Before the Command Line Interface can be started, you must exit the FTRA application. To start the Command Line Interface retrieve process, enter the **`(ftra -c)`** at the DOS command prompt (in Windows) or at a shell command prompt (in UNIX).

For modifying the Username and Password for an STP, three command line arguments have to be specified with the "-c" option (ftra –c stpname username password).

The user can automate this retrieve process through the use of external scheduling software such as Scheduled Task (on the Windows platform) and "cron" (on the Unix platform). Please refer to the platform's scheduling program for specifics on how to use the external scheduling software. For example, on the Unix platform, enter the **`man crontab`** command.

Procedure – Command Line Interface Manual Start

1. Exit the FTRA application. See "Exit the FTRA" on page 21.

2. On the Windows platform, at a DOS prompt, go to the **`\bin`** directory of the FTRA <*install_directory*> location.

3. On the Unix platform, at a shell prompt, go to the **`/bin`** directory of the FTRA <*install_directory*> location.

4. Enter the **`ftra -c`** **stpname username password** command (see Figure 76 on page 80 or Figure 78 on page 81). The stored **`rtrv`** commands are then sent to the provisioned STP. The data tables are retrieved and converted to the CSV file format.

   Result: The username and password shall be modified in the STP configuration for the specified stpname.

   NOTE: The parameters specified in the command line are case sensitive. For example, an stpname specified as EAGLE, Eagle or eagle shall be treated separately.

Figure 76. FTRA Windows Command Line Interface

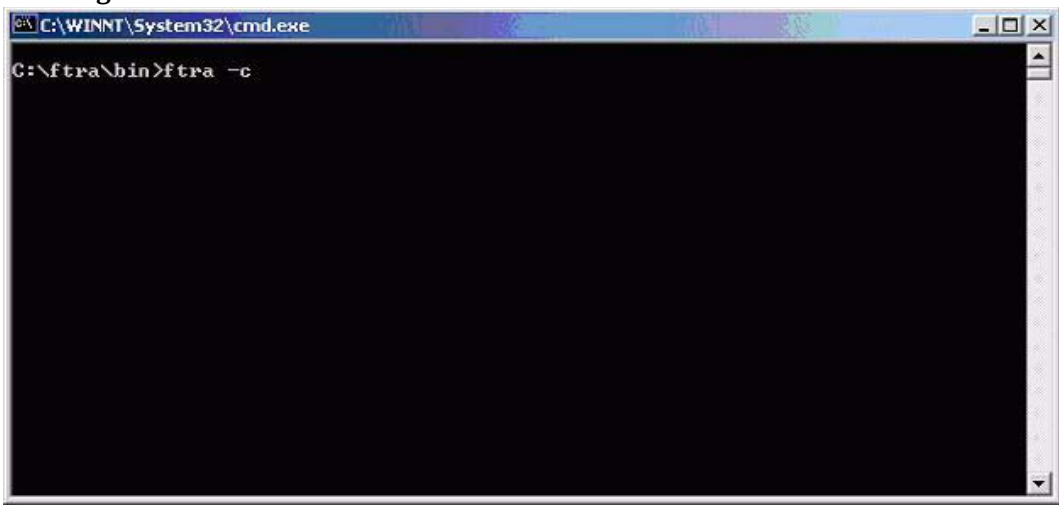


Figure 77. FTRA Windows Command Line Interface to modify STP data.

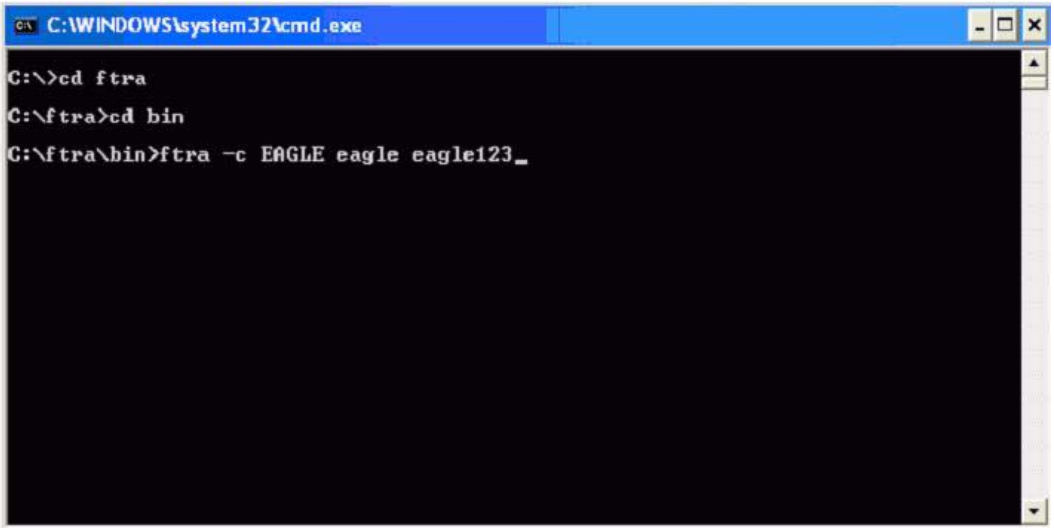


Figure 78. FTRA UNIX Command Line Interface

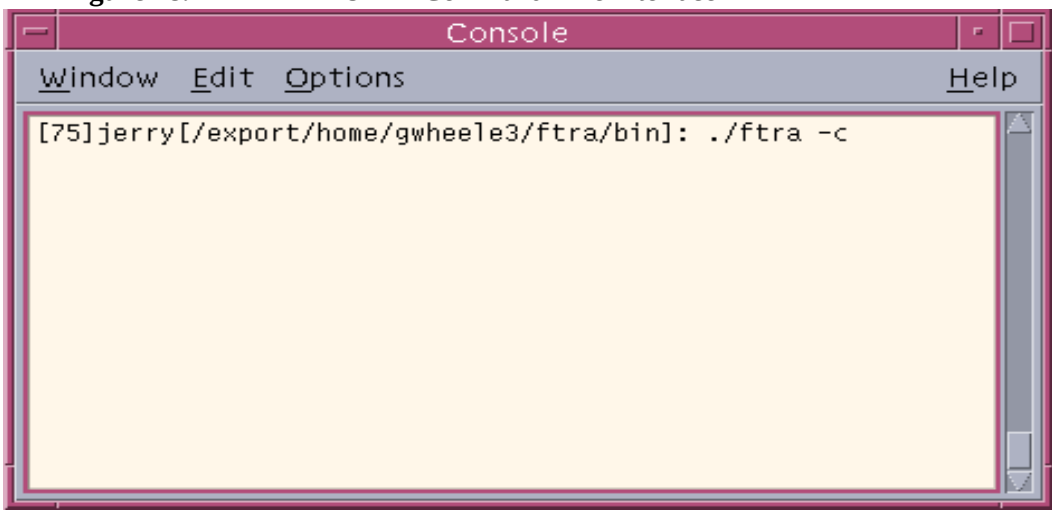


Figure 79. FTRA UNIX Command Line Interface to modify STP data.

Figure 80. FTRA Windows Scheduled Task

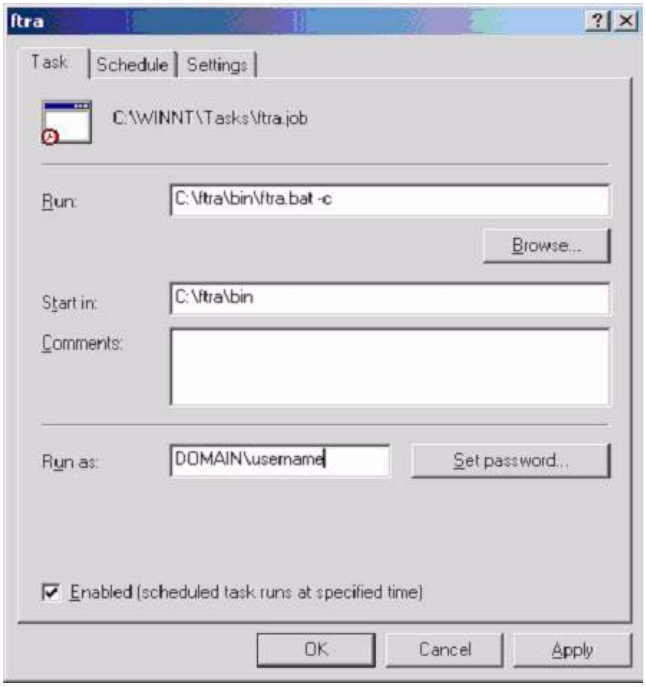


Figure 81. FTRA Windows Scheduled Task to modify STP data

Figure 82. UNIX cron job scheduled via crontab (note: last line shows FTRA scheduled to run at 3am Monday through Friday

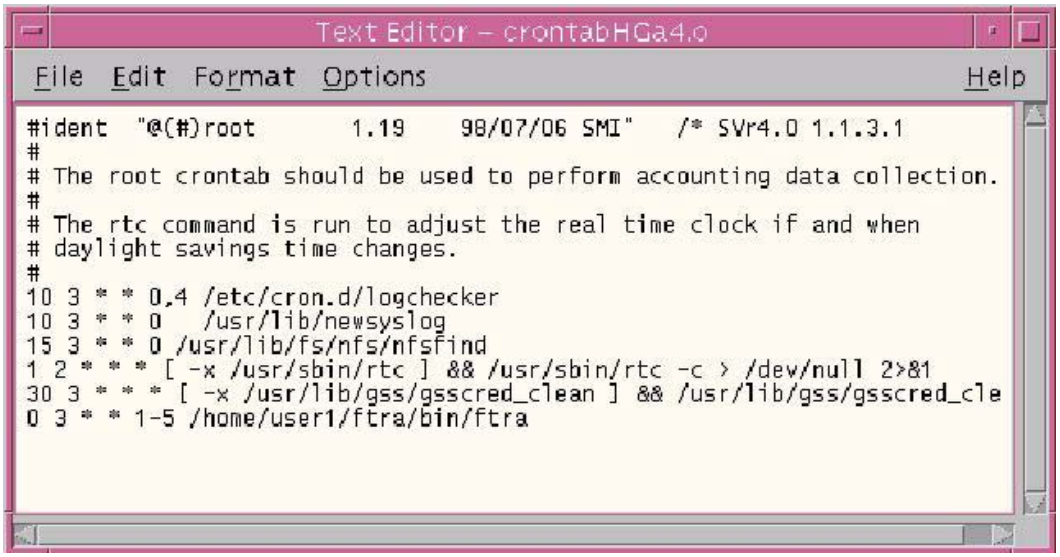


Figure 83. FTRA wrapper script example for Unix (might be necessary if running from cron)

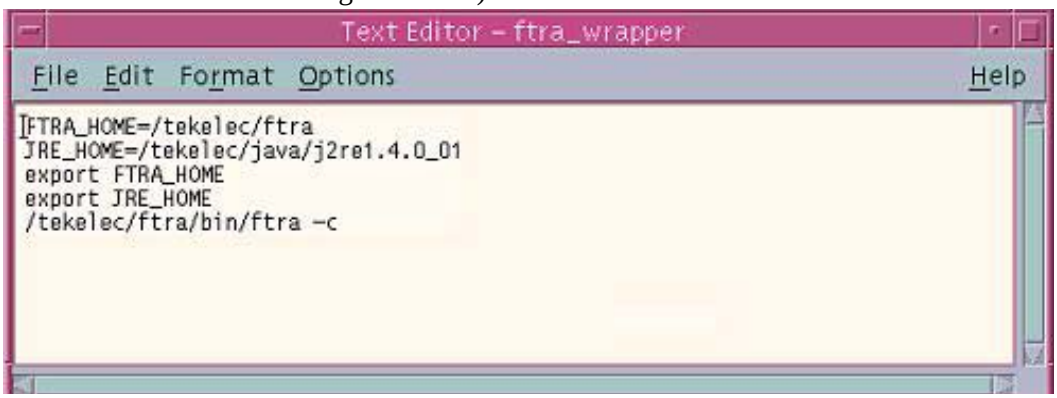
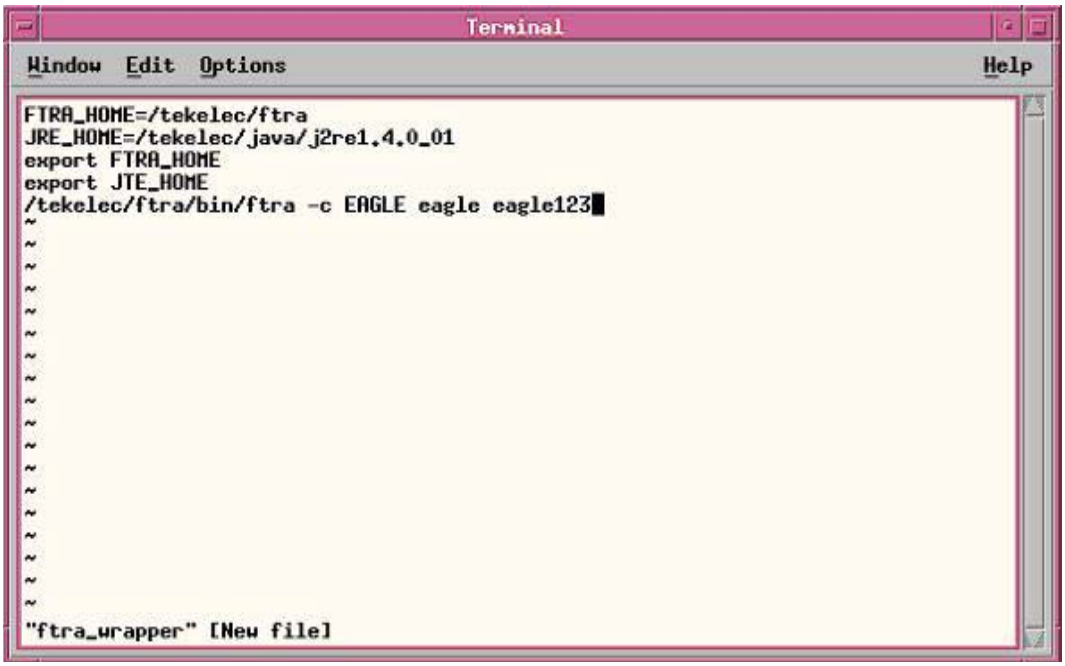


Figure 84. FTRA wrapper script example on Unix for modifying STP configuration (might be necessary if running from cron)



Procedure – Command Line Interface Automatic Start

1. To automate the FTRA retrieve process, enter the "ftra -c" command, the path to the bin directory of FTRA i.e. <install_directory> and the start time in the external scheduling software such as Scheduled Tasks (in Windows, see Figure 112 on page 110) or "cron" (in Unix, see Figure 113 on page 111).

   Result: When the start time is reached, the stored rtrv commands are sent to all the provisioned STPs. The data tables are retrieved and converted to CSV file format for the stored rtrv commands.

   However, to automate the FTRA retrieve process using three command line parameters, enter the **`ftra -c stpname username password`** command, the path to the bin directory of the FTRA such as <install_directory>, and the start time in the external scheduling software such as Scheduled Tasks (on Windows) or "cron" (on Unix).

   Result: The username and password shall be modified in the STP configuration for the specified stpname. When the start time is reached, the stored rtrv commands are sent to all the provisioned STPs. The data tables will be retrieved and converted to csv file format for the stored rtrv commands. See Figure 108 on page 107 for example.

   NOTE: If you are using “cron” on the Unix workstation, it might be necessary to create a wrapper script for FTRA, in order to correctly set environment variables. For an example of the wrapper script, see Figure 87 on page 90.

Table 6. FTRA – Eagle Compatibility Matrix

	FTRA 1.0	FTRA 1.1	FTRA 2.0	FTRA 2.1	FTRA 2.2	FTRA 3.0	FTRA 4.0
Eagle 28.x and earlier	N	N	N	N	N	N	N
Eagle 29.0	Y	N	N	N	N	Y	Y
Eagle 30.0	N	Y	Y	N	N	Y	Y
Eagle 30.2	N	N	Y	N	N	Y	Y
Eagle 31.3	N	N	N	Y	N	Y	Y
Eagle 31.6	N	N	N	N	Y	Y	Y
Eagle 31.9	N	N	N	N	Y	Y	Y
Eagle 32.0	N	N	N	N	N	Y*	Y*
Eagle 35.0 and later	N	N	N	N	N	Y*	Y* Y**

Legend:

N - Not supported.

Y - Supported. (CSVGen installed from FTRA install CD.)

Y* - Supported. (CSVGen transferred from Eagle TDM.)

Y** - Supported. (rtrv-stp command support, command line support for modifying STP data.)

All other releases of Eagle that are not listed are not officially supported by any release of FTRA.

Updating Database Tables in the Selected STP

The **Update Tables** window (see Figure 85) is used to send EAGLE 5 ISS commands to the selected STP. The commands, in the form of a command file, are validated before being sent.

To send the command file to the selected STP, the command file is selected by entering the path and file name of the command file, or by selecting the file name of the command file from the **Select** window. The command file is then validated by clicking the **Validate** button in the **Update Tables** window. When the validation is completed, the **Update Validation Complete** window appears. From the **Update Validation Complete** window the command file can be edited, sent to the selected STP, or the **Update Validation Complete** window can be closed without sending the command file to the selected STP. The Update Tables Log contains the events of the command validation and any error messages that may have occurred.

Figure 85. Update Tables Window

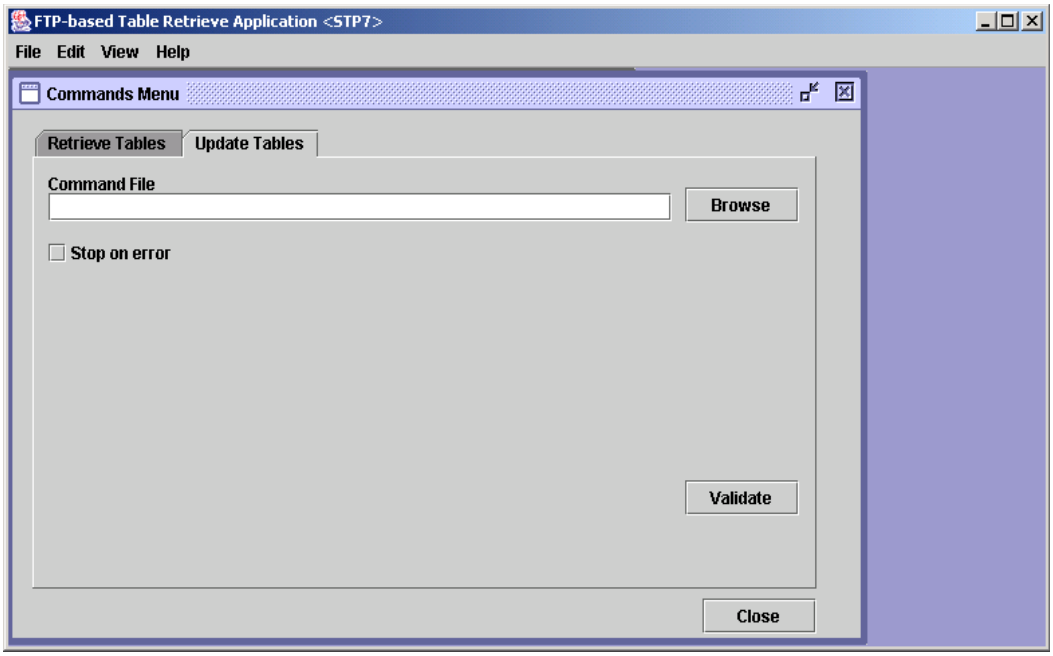


Table 7 shows the description of the fields and buttons in the **Update Tables** window.

Table 7. Update Tables Window Description

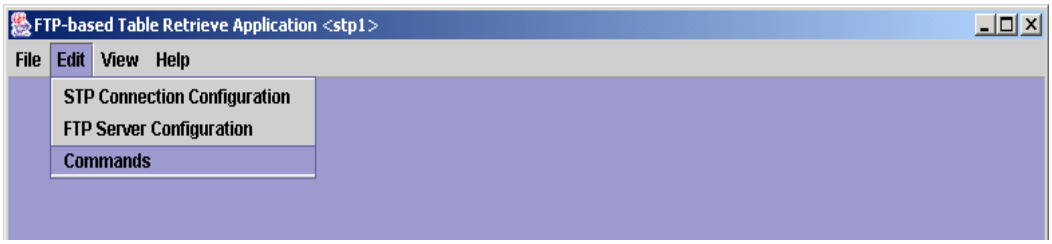
Item	Description
Fields	
Command File	The path and file name of the command file are entered here. A command file contains the EAGLE 5 ISS commands used to modify database tables of the STP.
Stop on error box	If the box is checked, and an error is found during the validation of the commands, the validation stops and no further commands are validated. If the box is not checked, all commands are processed regardless of errors. The error results are displayed in the Update Tables Log.
Buttons	
Browse	Opens the **Select** window to select the command file to send to the selected STP.
Validate	Validates the EAGLE 5 ISS commands using the offline database.
Close	Closes the **Commands Menu** window.

Validating a Command File

Procedure

1. Select **Edit > Commands > Update Tables** in the **FTP-based Table Retrieve Application** window. See Figure 86. The **Update Tables** window opens. See Figure 85 on page 87.

Figure 86. Edit Menu



2. Perform one of these steps.

   a. Enter the path and name of the command file in the **Command File** field. See Figure 87.

   b. Click the **Browse** button. The **Select** window is opened. See Figure 87 on page 90. Find the folder containing the command file and click on the command file name. The command file name is highlighted. Click the **Select** button. The **Select** window disappears and the **Update Tables** window appears with the path and file name of the selected command file entered in the **Command File** field.

      If you wish to cancel the command file selection process in the **Select** window, click the **Cancel** button.

      Table 8 on page 90 shows the description of the buttons in the **Select** window.

Figure 87. Select Window

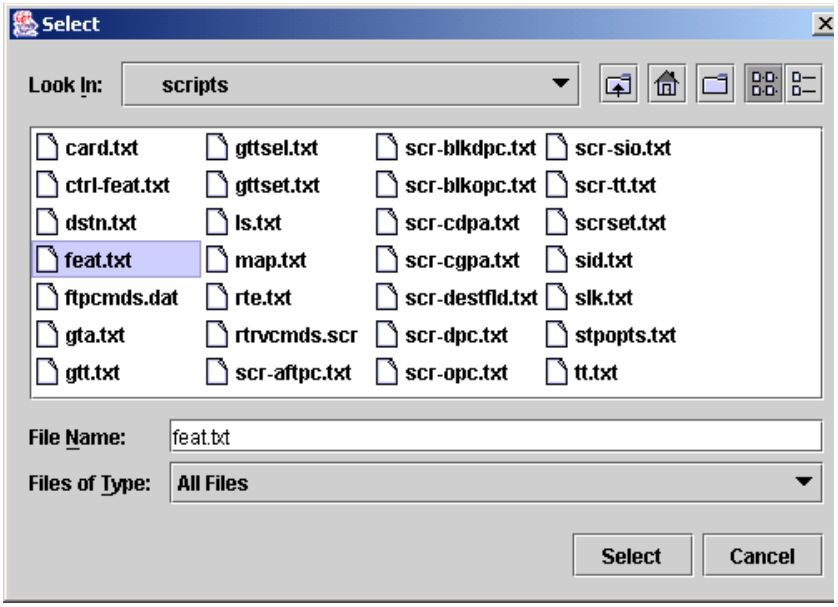
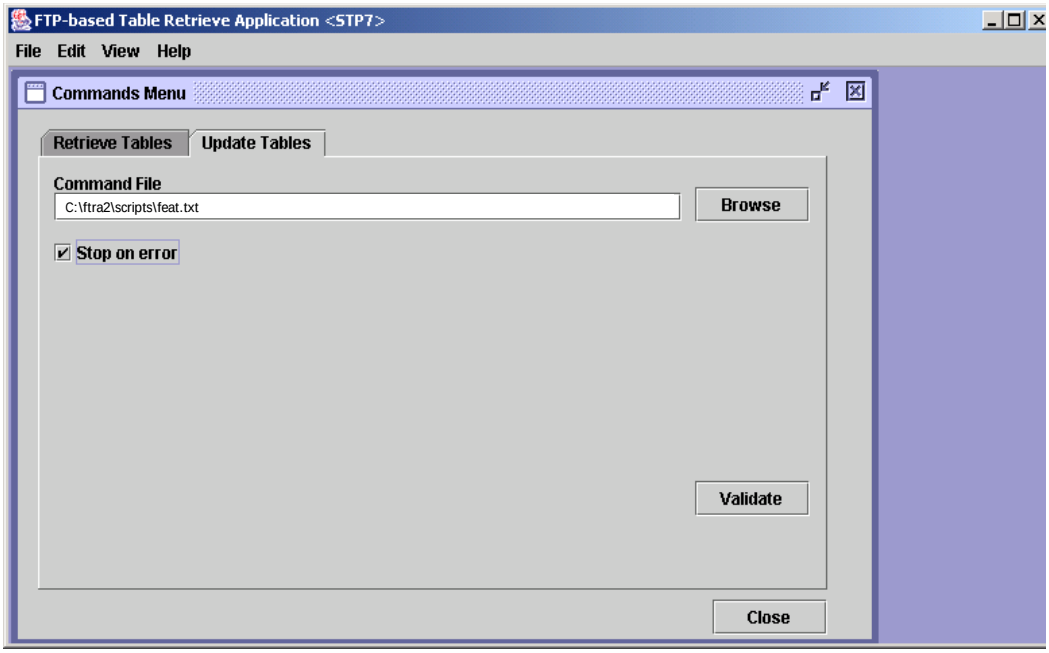


Table 8. Select Window Descriptions

Item	Description
Fields	
Look in:	A drop down menu allowing the user to browse through the directory structures.
File Name:	The name of the file to be selected.
Files of type:	A drop down menu that selects all files.
Buttons	
Select	The contents of the **File Name** field and the path to the filename is loaded into the **Command File** field of the **Update Tables** window.
Cancel	Closes the **Select** window.

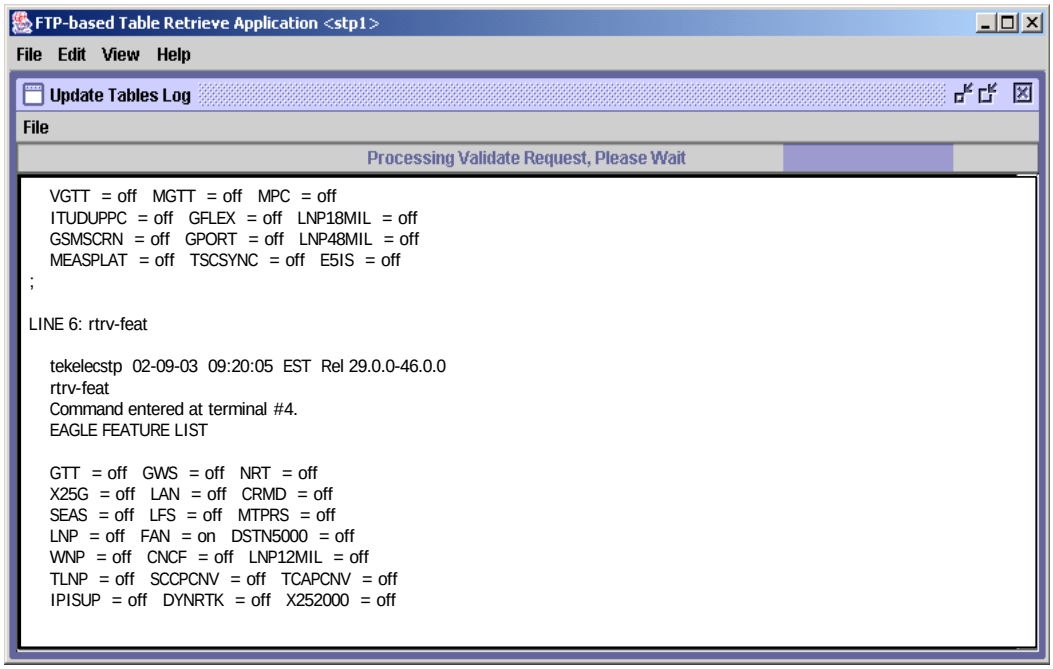
3. If you wish to have the command validation stop if any errors are found, check the **Stop on error** box in the **Update Tables** window. See Figure 88. If you wish to have the command validation processed regardless of any errors, uncheck the **Stop on error** box. The error results are displayed in the Update Tables Log.

Figure 88. Update Tables Window with a Command File Selected and Stop on Error Box Checked



4. Click the **Validate** button. The **Update Tables Log** window opens at the beginning of the validate process and displays the "Processing Validate Request, Please Wait" message until the validation of the command file is complete. See Figure 89.

Figure 89. Update Tables Log Window - Processing Retrieve Request



The **Update Validation Complete** window opens. See the "Update Validation Complete Window" section on page 93.

---

5. The **Update Tables Log** window opens. It contains the events and error messages generated during the validation. See Figure 99 on page 98, Figure 100 on page 99, and Figure 101 on page 100 for Update Tables Log examples.

NOTE: If there is no entry in the Command File field and the Validate button is clicked, a warning message is displayed stating that a command file name must be entered. See Figure 90.

Figure 90. Must Enter Command Script File Name Message

Update Validation Complete Window

When the command validation has completed, the **Update Validation Complete** window opens notifying the user if the commands validated with or without errors. From the **Update Validation Complete** window, the command file can be edited, sent to the selected STP, or the window can be closed without sending the command file to the selected STP. See Figure 91.

Figure 91. Update Validation Complete Window without Errors

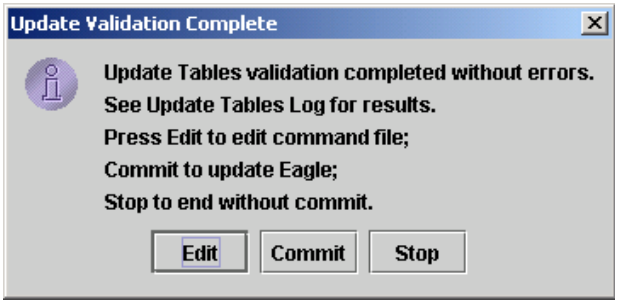


Table 9 shows the description of the buttons in the **Update Validation Complete** window.

Table 9. Update Validation Complete Window Description

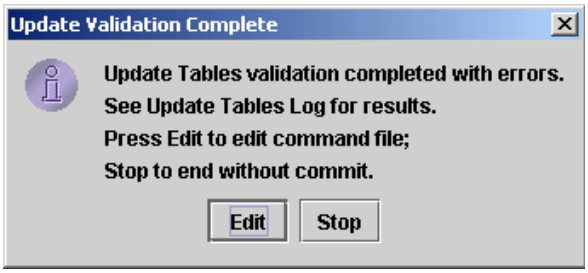
Item	Description
Edit	Opens the Command File Editor window and allows the user to make changes to the command file. To edit a command file, go to the "Editing a Command File" section on page 95.
Commit	Sends the commands in the command file to the STP. A **Command Complete** window opens and the Update Tables Log is updated. See the "Sending a Command File to the Selected STP" section on page 94. If the Update Tables validation completed with errors the **Commit** button is not displayed.
Stop	Closes the **Update Validation Complete** window without sending the commands in the command file to the STP.

Update Validation Complete Window with Errors

If the **Update Validation Complete** window shows that errors have occurred, the command file can be edited or the window can be closed without sending the command file to the selected STP. See Figure 92. There is no **Commit** button in this window; this prevents the sending of invalid commands.

To fix the errors in the command file, click the **Edit** button, then go to the "Editing a Command File" section on page 95.

Figure 92. Update Validation Complete Window with Errors

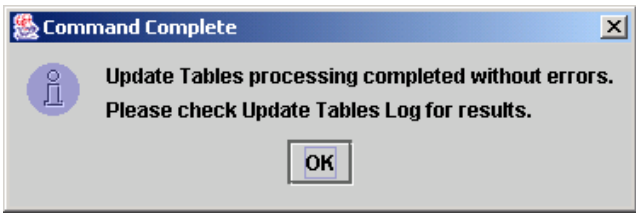


Sending a Command File to the Selected STP

To send the command file, click the **Commit** button in the **Update Validation Complete** window. The **Commit** button is shown only on the **Update Validation Complete without Errors** window. See Figure 91 on page 93. The validated command file is sent to the selected STP.

The **Command Complete** window opens and displays: "Update Tables processing completed without errors" and "Please check Update Tables Log for results." See Figure 93. Click **OK**, to continue. The Update Tables Log contains the commit processing events. See Figure 99 on page 98.

Figure 93. Command Complete Window



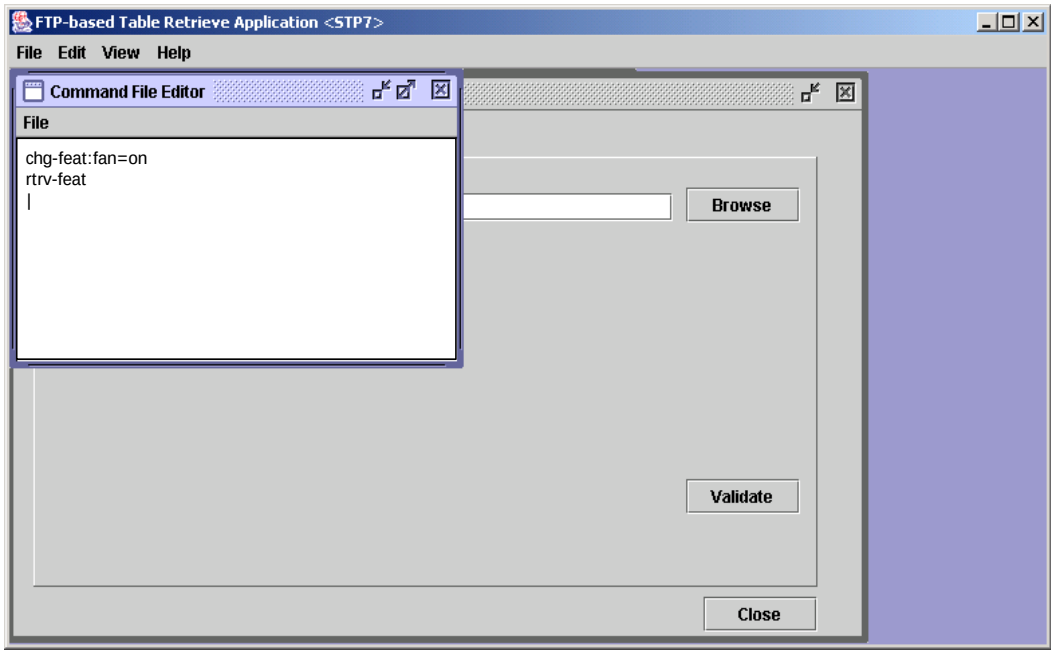
Stop Without Sending or Editing a Command File

To stop the process without sending or editing a command file, click the **Stop** button in the **Update Validation Complete** window. See Figure 91 on page 93. The **Update Validation Complete** window is closed. No changes are made to the command file and the command file is not sent to the selected STP.

Editing a Command File

To edit a command file, click the **Edit** button in the **Update Validation Complete** window. The **Command File Editor** window is opened. See Figure 94.

Figure 94. Command File Editor Window



When the editing is complete, the command file can be saved without sending the command file to the selected STP, saved and sent to the selected STP without any further validation, or the command file can be closed without saving the changes to the command file.

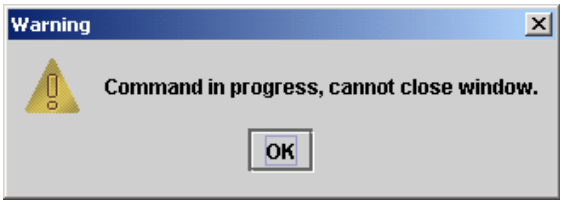
Procedure

1. Click the **Edit** button in the **Update Validation Complete** window. See Figure 91 on page 93. The **Command File Editor** window opens. See Figure 94 on page 95.

   NOTE: The hourglass is displayed until the Command File Editor window is closed.

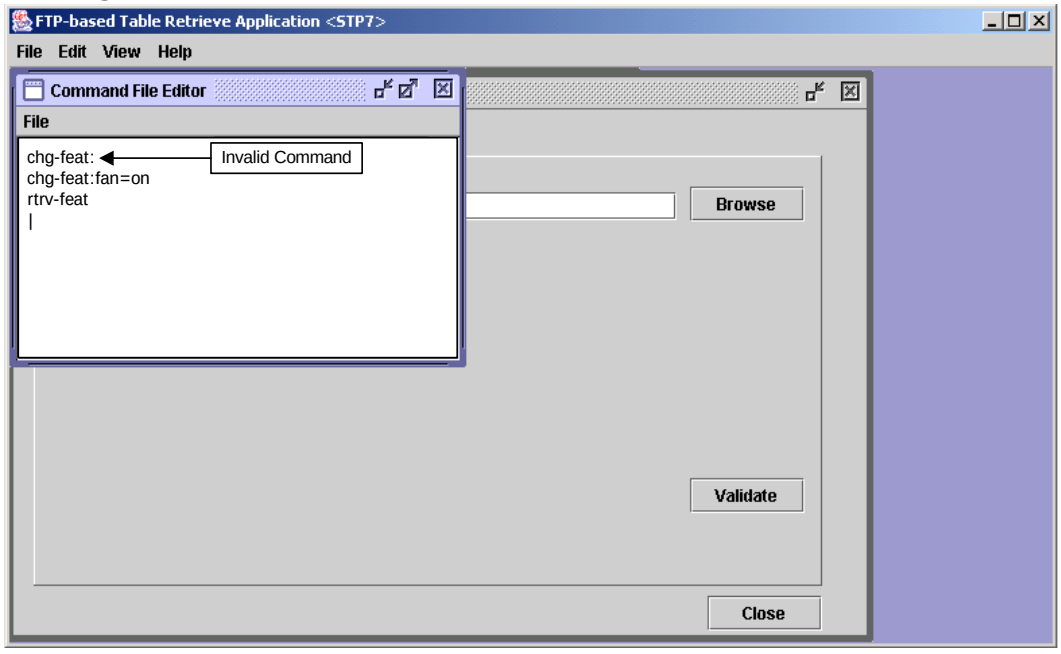
   NOTE: If an attempt is made to close the Update Tables window while the Command File Editor window is opened, the Command In progress, Cannot Close Window warning message is displayed. See Figure 95.

   Figure 95. Command In progress, Cannot Close Window



2. Edit the command file. Figure 96 shows a command file with an invalid command. In this example, the invalid command is `chg-feat:`. This command should be removed from the command file, or have a correct parameter and value added to it.

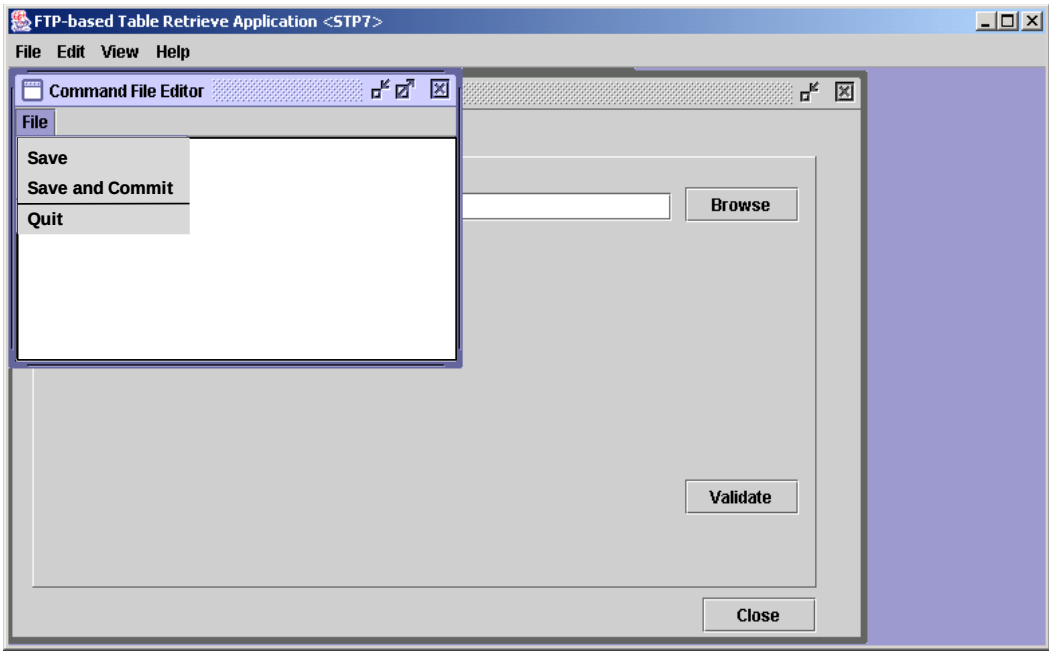
   Figure 96. Command File Editor with Invalid Command



3. When the editing is complete, perform one of these steps.

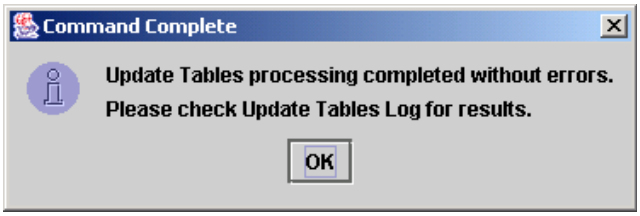
   a. Select **File > Save** from the **Command File Editor** window (see Figure 97). The command file is saved and the **Command File Editor** window remains open. The command file is not sent to the selected STP. The command file can be validated again in the **Update Tables** window.

Figure 97. File Menu in the Command File Editor Window



   b. Select **File > Save and Commit** from the **Command File Editor** window (see Figure 97). The command file is saved and the **Command File Editor** window closes. The **Command Complete** window opens and displays: “Update Tables processing completed without errors. Please check Update Tables Log for results. Click **OK**, to continue. See Figure 98. The command file is sent to the selected STP. The Update Tables Log contains the commit processing events. See Figure 99 on page 98

Figure 98. Command Complete Window



   c. Select **File > Quit** from the **Command File Editor** window (see Figure 97). The **Command File Editor** window closes. The command file is not sent to the selected STP. If changes to the command file have been made, a window is displayed asking if you want to save the changes.

Update Tables Log Window

The Update Tables Log contains the processing events and any error messages that may have occurred during the validation and sending of a command file. The **Update Tables Log** window is opened at the beginning of the validation process and displays “Processing Validate Request, Please Wait” (Figure 89 on page 92) until the command file validation is completed. The **Update Tables Log** window is automatically cleared when the next command file validation is started. Selecting **View > Update Tables Log** from the menu can also open the **Update Tables Log** window.

See Figure 99, Figure 100 on page 99, Figure 101 on page 100, and Figure 102 on page 101 for the **Update Tables Log** window examples.

Figure 99. Update Tables Log Window after the Commit Command Completed

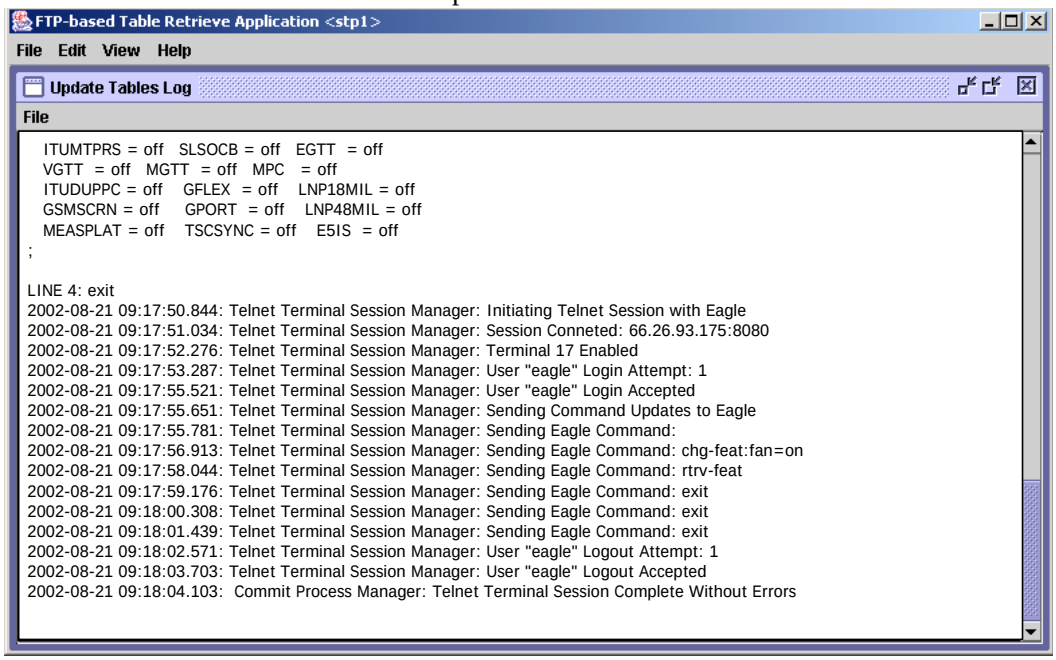


Figure 100. Update Tables Log

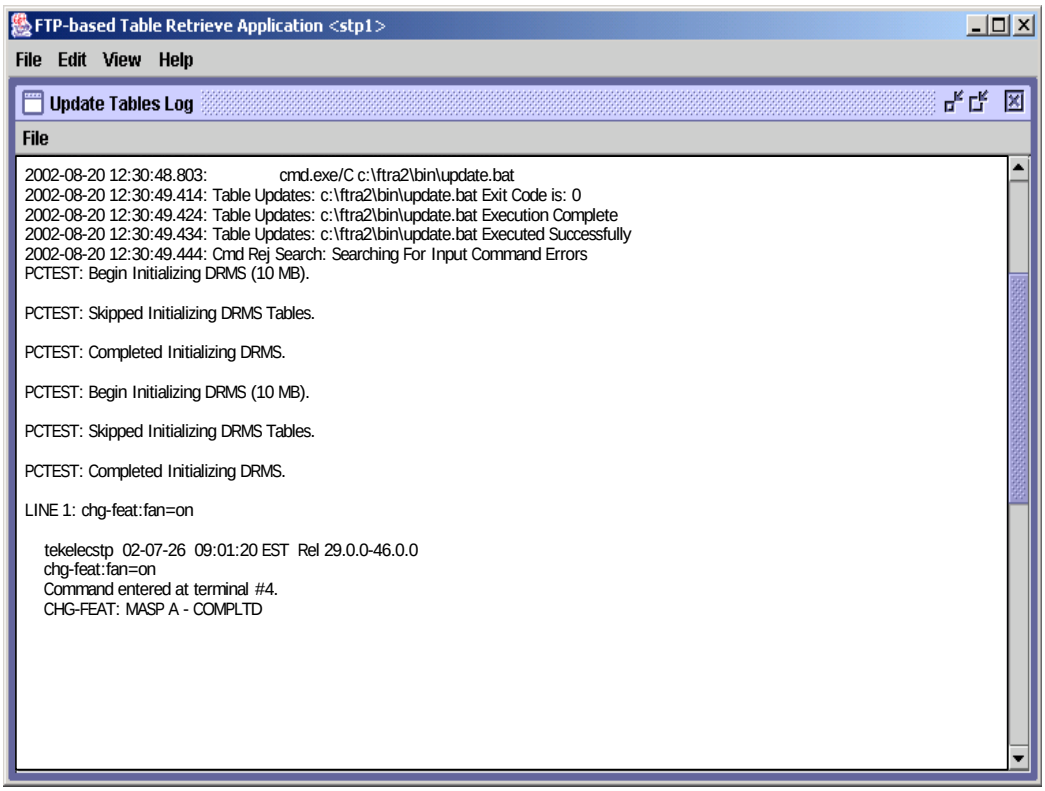


Figure 101. Update Tables Log with Stop on Error Box Checked in the Update Tables Window

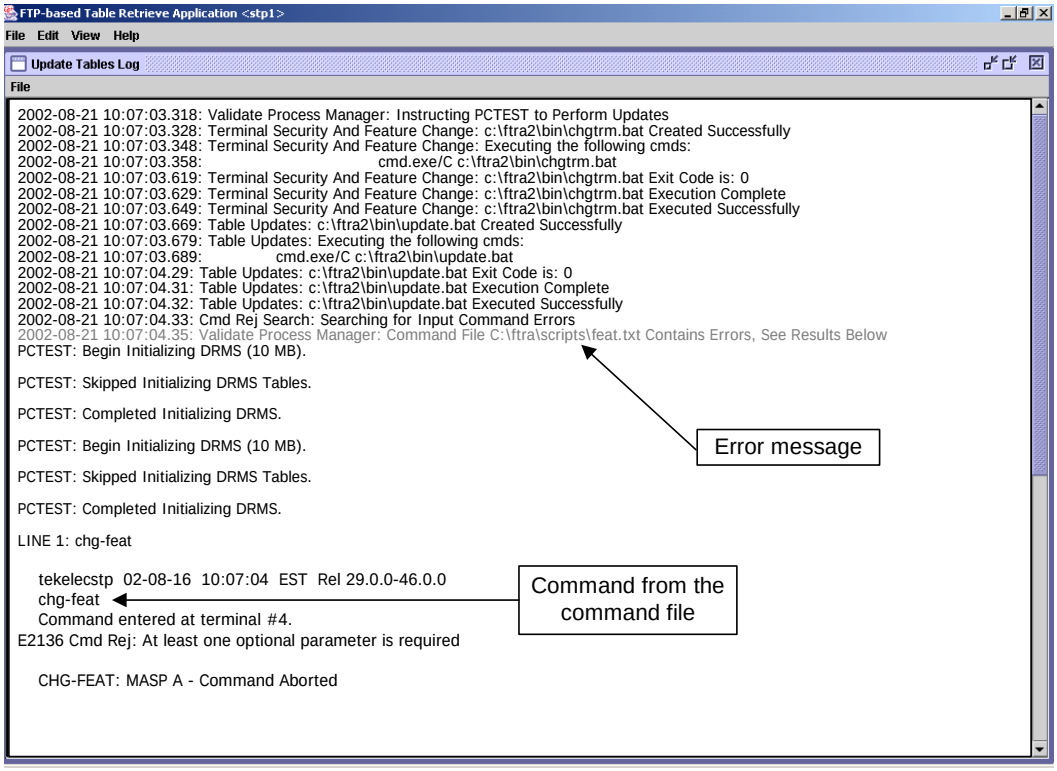


Figure 102. Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window

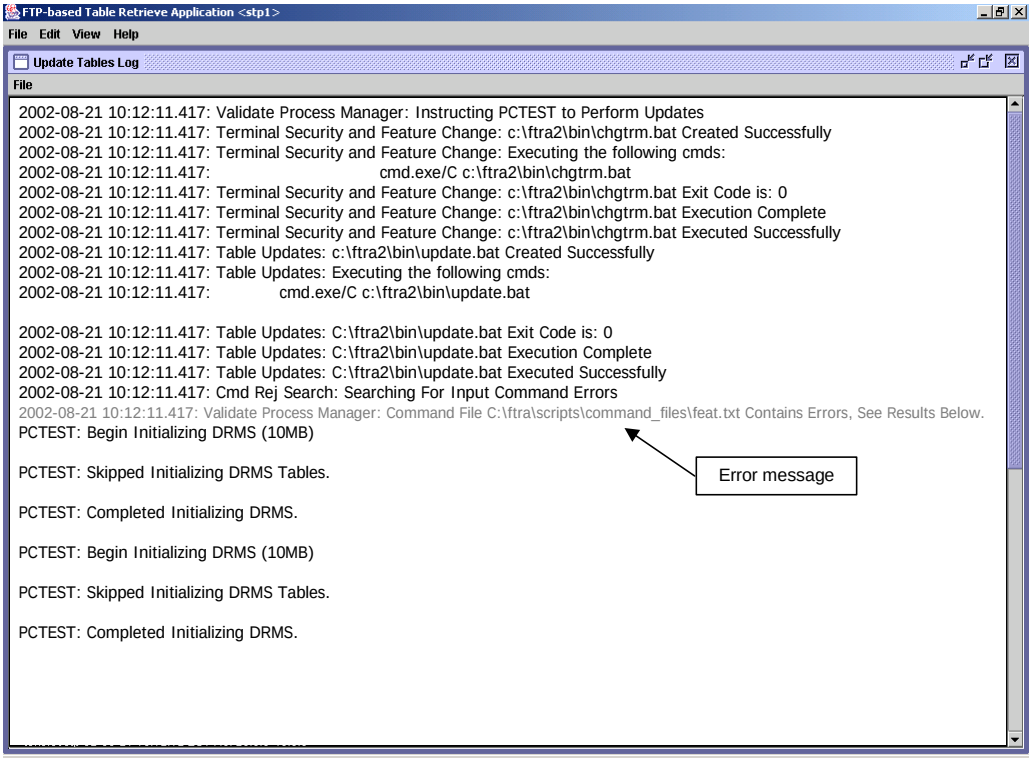
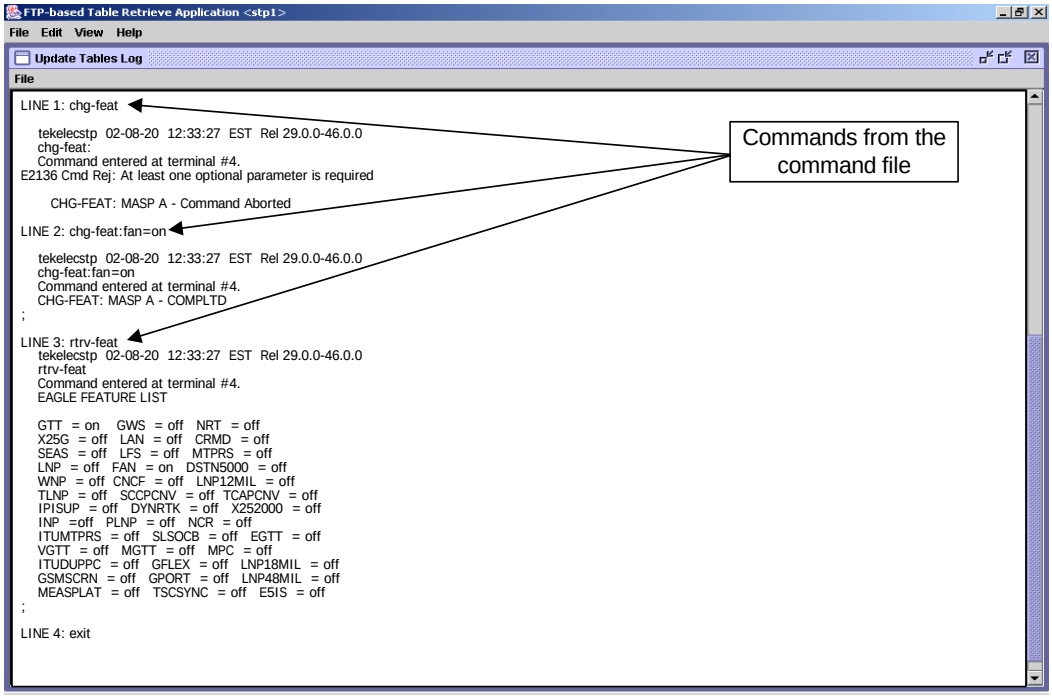


Figure 96 on page 96 shows an example of a command file that produced the error shown in Figure 102.

Figure 102. Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window (Continued)

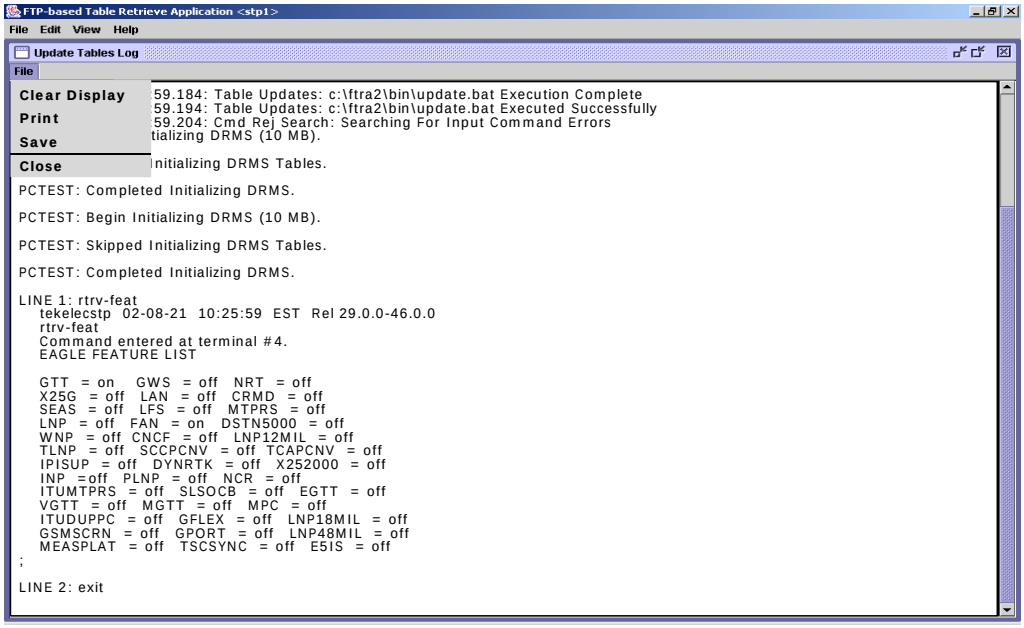


File Menu in the Update Tables Log Window

The **File** menu in the **Update Tables Log** window, shown in Figure 103 on page 103, provides the user with the following selections:

- Clearing the Update Tables Log display.
- Printing the Update Tables Log.
- Saving the Update Tables Log to a file.
- Closing the **Update Tables Log** window.

Figure 103. File Menu in the Update Tables Log Window



Clearing the Update Tables Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is save to a file or printed before the display is cleared.

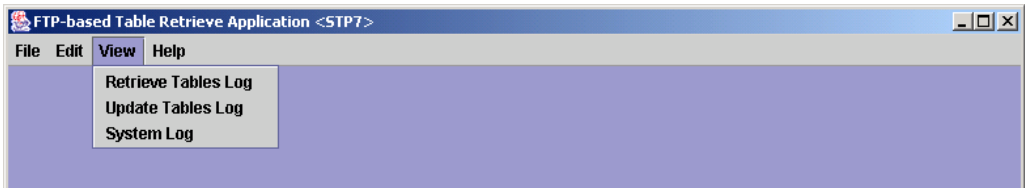
Procedure

NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Clear Display** in the **Update Tables Log** window. See Figure 103.

2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 104. The **Update Tables Log** window opens.

Figure 104. View Menu



3. Select **File > Clear Display** in the **Update Tables Log** window. The Update Tables Log display clears.

Printing the Update Tables Log

Procedure

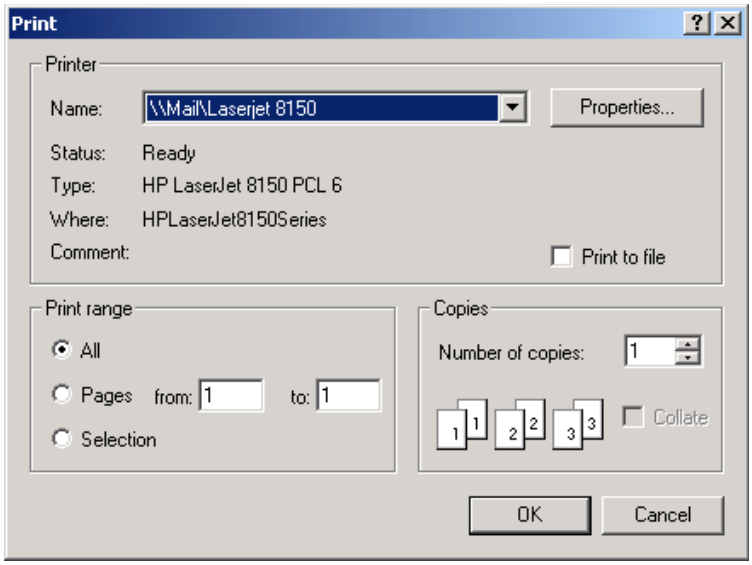
NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Print** from the **Update Tables Log** window. See Figure 103 on page 103.

2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 104 on page 103. The Update Tables Log opens.

3. Select **File > Print** from the **Update Tables Log** window. The **Print** window opens. See Figure 105.

Figure 105. Print Window



4. Configure the printer settings.

5. To print the Update Tables Log, click the **OK** button. The current contents of the Update Tables Log are printed.

6. If you do not wish to print the Update Tables Log, click the **Cancel** button.

Saving the Update Tables Log to a File

Procedure

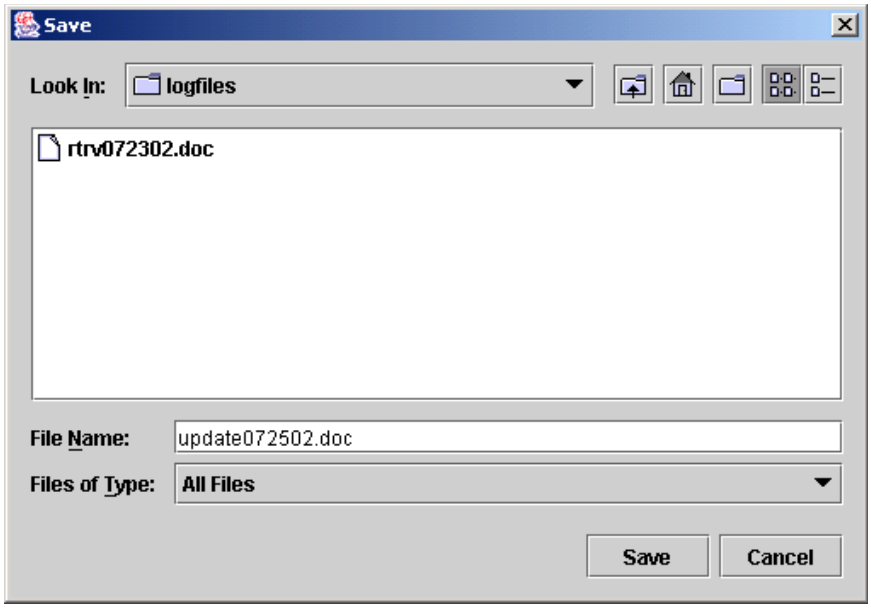
NOTE: Perform either step 1 or steps 2 and 3.

1. Select **File > Save** from the **Update Tables Log** window. See Figure 103 on page 103.

2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 104 on page 103. The Update Tables Log opens.

3. Select **File > Save** in the **Update Tables Log** window. The **Save** window opens. See Figure 106.

Figure 106. Save Window

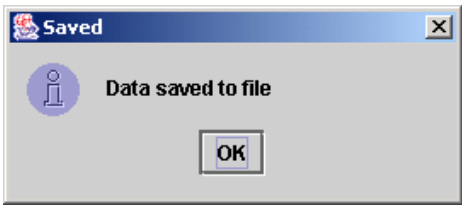


4. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file even if it was saved as a .txt file.

5. To save the file, click the **Save** button. A **Saved** file confirmation window opens with "Data saved to file." See Figure 107. Click **OK**, to continue.

Figure 107. Saved Confirmation Window



6. If you do not wish to save the file, click the **Cancel** button in the **Save** window.

Closing the Update Tables Log Window

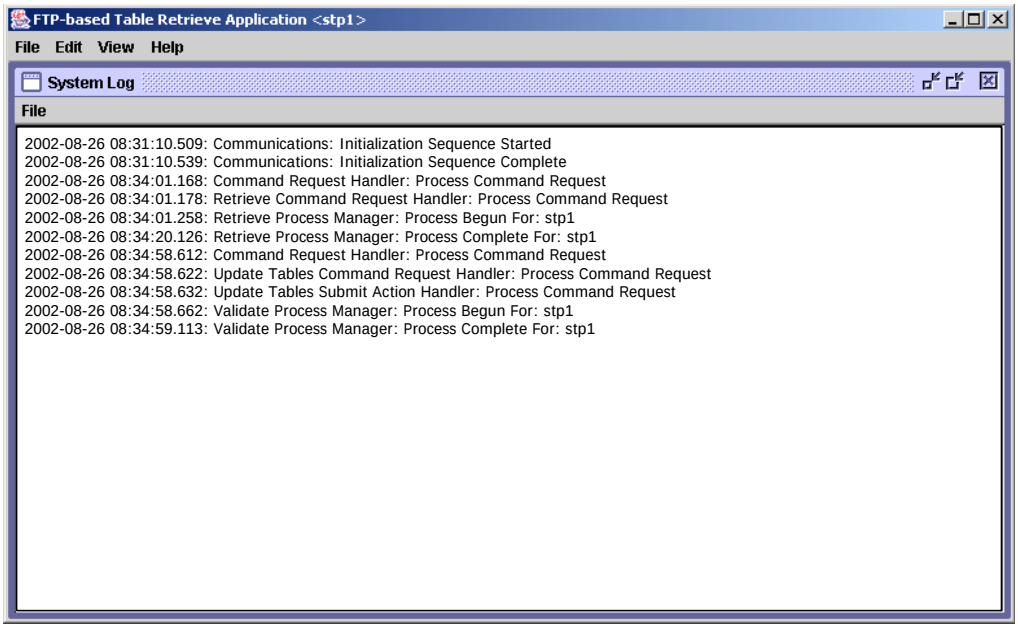
Procedure

1. Select **File > Close** in the **Update Tables Log** window, or click the close window button in the upper right hand corner of the **Update Tables Log** window. See Figure 103 on page 103. The **Update Tables Log** window closes.

The System Log

The System Log contains an event history and any errors that have occurred when database tables are retrieved from an STP, or command files are sent to an STP. See Figure 108.

Figure 108. System Log Window

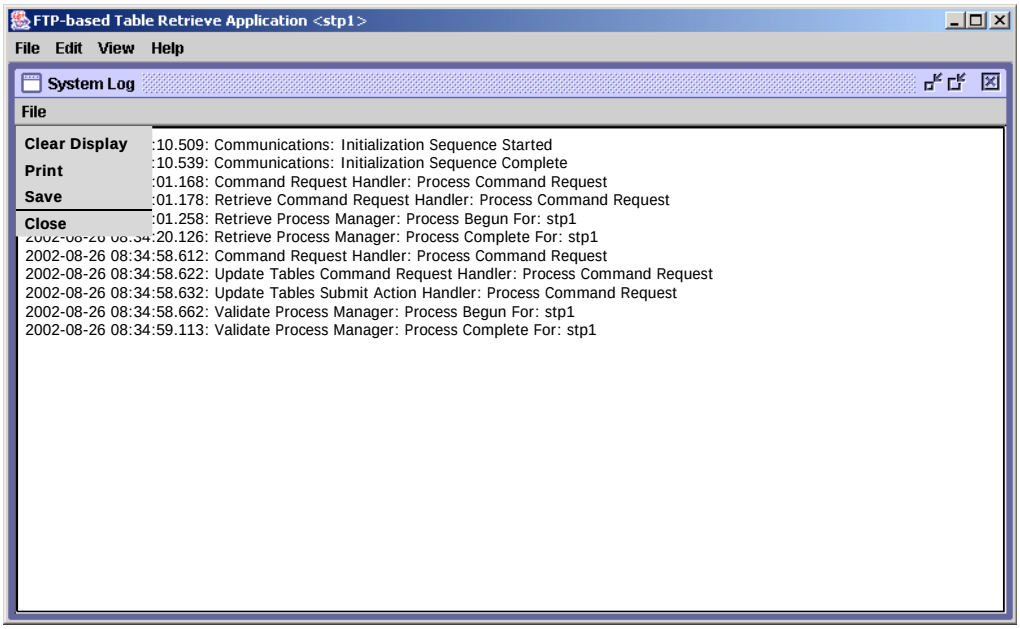


File Menu in the System Log Window

The **File** menu in the **System Log** window, shown in Figure 109 on page 108, provides these selections:

- Clearing the System Log display.
- Printing the System Log.
- Saving the System Log to a file.
- Closing the **System Log** window.

Figure 109. File Menu in the System Log Window



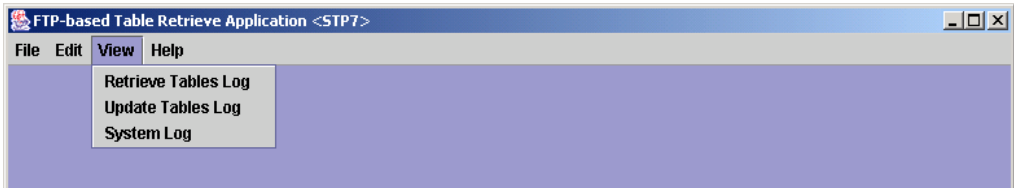
Clearing the System Log Display

The display can be cleared, enabling new entries to be captured to the log. Once the log is cleared, the existing entries are lost unless the log is saved to a file or printed before the display is cleared.

Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 110. The **System Log** window opens.

   Figure 110. View Menu

2. Select **File > Clear Display** in the **System Log** window. See Figure 109. The System Log display clears.

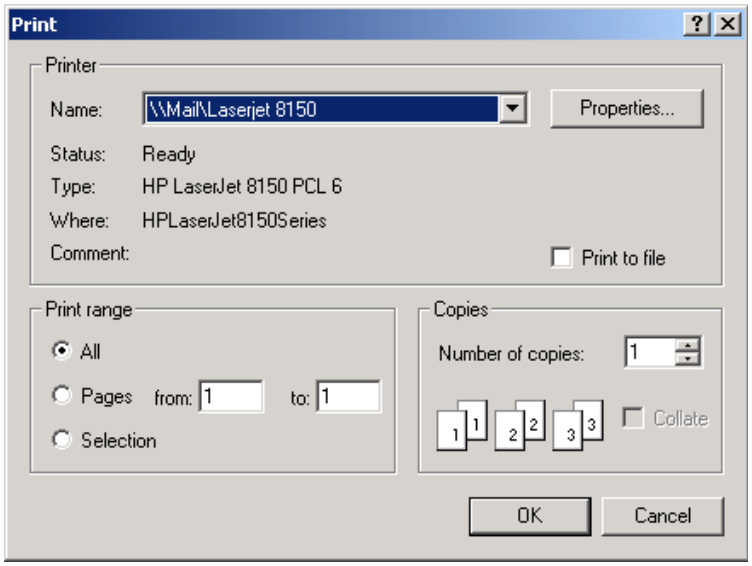
Printing the System Log

Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 110 on page 108. The **System Log** window opens.

2. Select **File > Print** in the **System Log** window. The **Print** window opens. See Figure 111.

Figure 111. Print Window



3. Configure the printer settings.

4. To print the System Log, click the **OK** button. The current contents of the System Log are printed.

5. If you decide not to print the System Log, click the **Cancel** button.

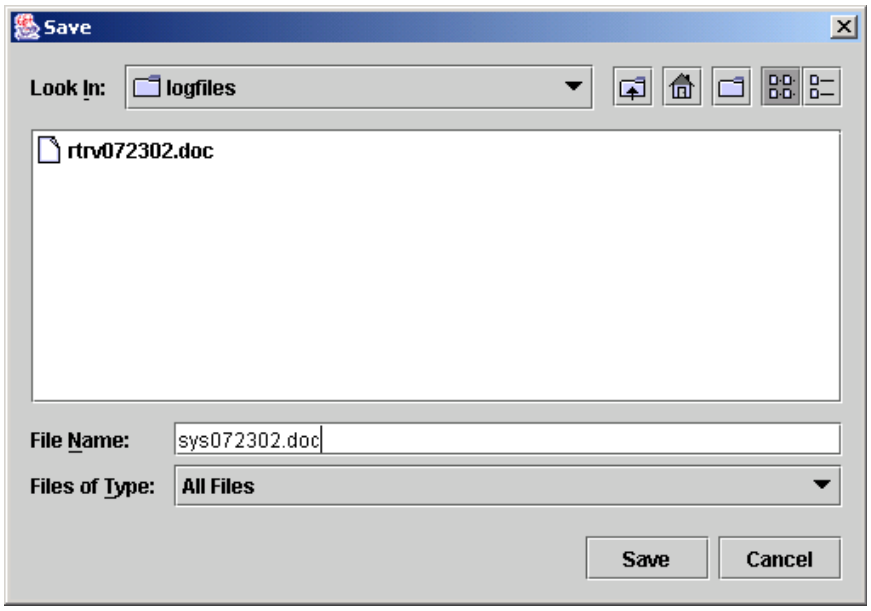
Saving the System Log to a File

Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 110 on page 108. The System Log opens.

2. Select **File > Save** in the **System Log** window. The **Save** window opens. See Figure 112.

Figure 112. Save Window

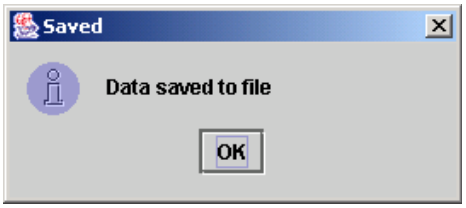


3. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

   NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file even if it was saved as a .txt file.

4. To save the System Log to a file, click the **Save** button. A **Saved** file confirmation opens with “Data saved to file”. See Figure 113. Click **OK** to continue.

Figure 113. Saved Confirmation Window



5. If you do not wish to save the System Log to a file, click the **Cancel** button in the **Save** window.

Closing the System Log Window

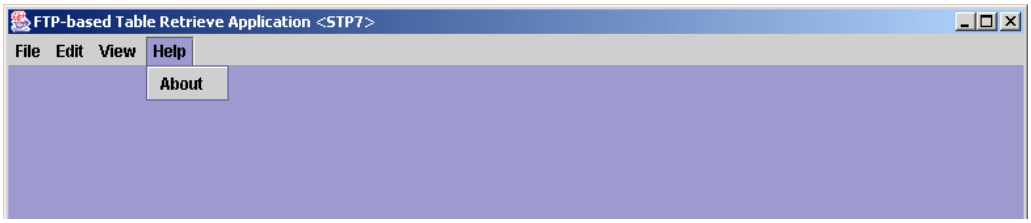
Procedure

1. Select **File > Close** in the **System Log** window, or click the close window button in the upper right hand corner of the **System Log** window. The **System Log** window closes.

About FTRA Window

The **About FTRA** window displays the version level of the FTRA and copyright information. To display the **About FTRA** window, select **Help > About** in the **FTP-based Table Retrieve Application** window. See Figure 114.

Figure 114. Help Menu



The **About FTRA** window opens. See Figure 115. Click **OK**, to continue.

Figure 115. Typical About FTRA Window

FTRA release 4.0

The following sub-sections detail the changes that were made to FTRA Release 4.0.

Change summary.

The following enhancements have been included in FTRA Release 4.0:

1. Support for rtrv-stp command.
2. Support to change the STP Username and Password for an STP whose configuration already exists in the system through the Command Line.

The second identified enhancement has introduced some minor changes to the Command Line Interface.

RTRV-STP Command.

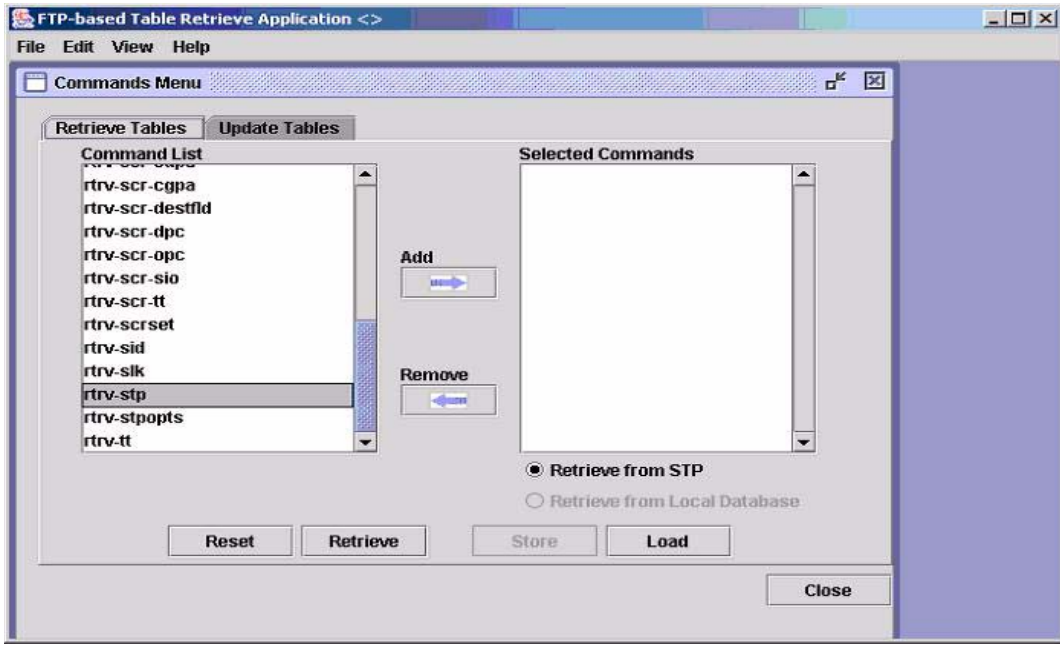
The **rtrv-stp** command is added to the list of rtrv commands supported on FTRA. The rtrv-stp command provides a consolidated report of STP configuration on a system-wide basis.

NOTE: The rtrv-stp functionality is supported on Eagle Release 35.0 or later.

Retrieve Tables

This added functionality provided in FTRA Release 4.0 changes the display of the Retrieve Table Window. A new command rtrv-stp is added to the retrieve command list as shown in Figures 116.

Figure 116. Retrieve Tables window with rtrv-stp command selected for retrieval.



RTRV-STP Command Retrieval Session

The FTRA retrieval session when rtrv-stp command is supported on EAGLE is shown in Figures 117. If the command is not supported on EAGLE, an error will be displayed and the retrieval session will be terminated (refer “STP data modified through CLI.” on page 115).

Figure 117. Successful Retrieval Session for rtrv-stp command

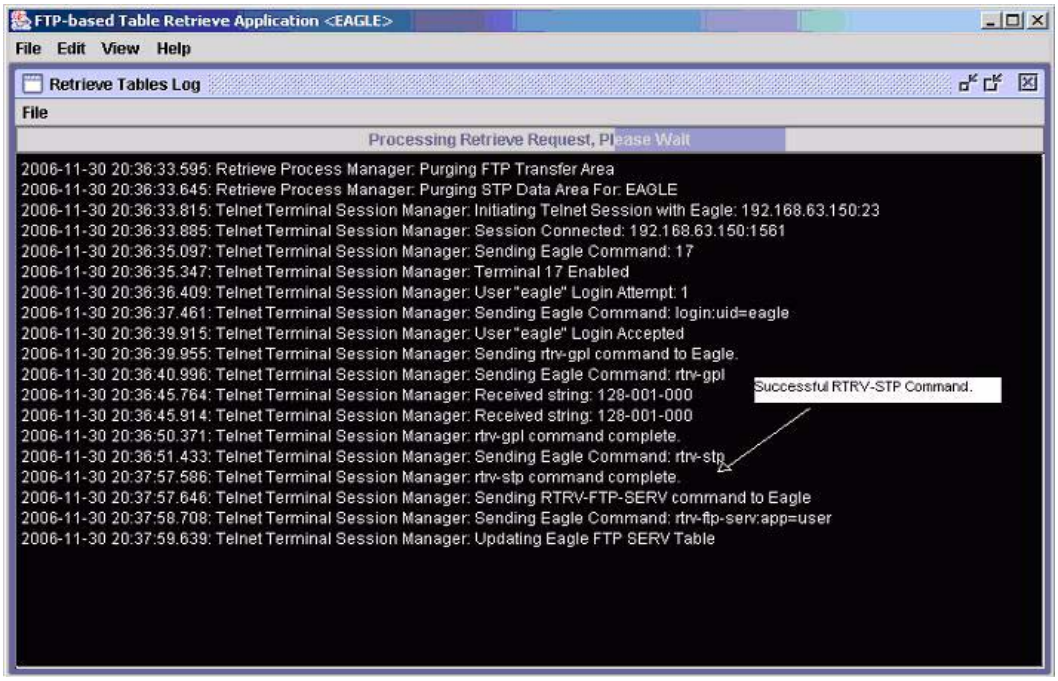
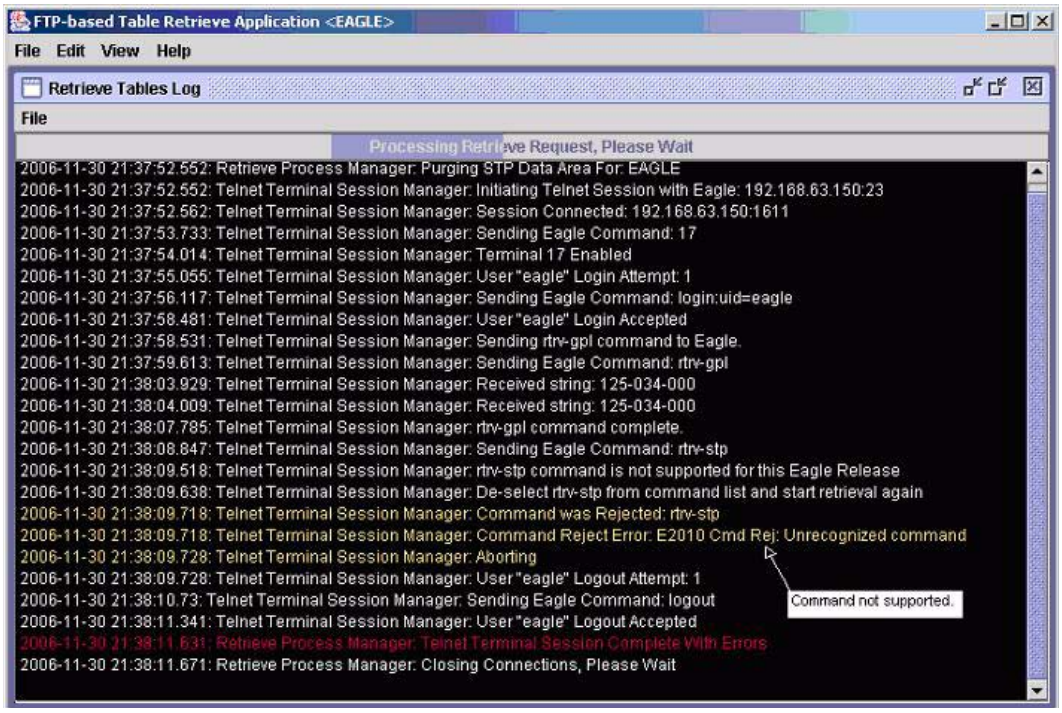


Figure 118. Rtrv-stp Command unsupported on EAGLE release

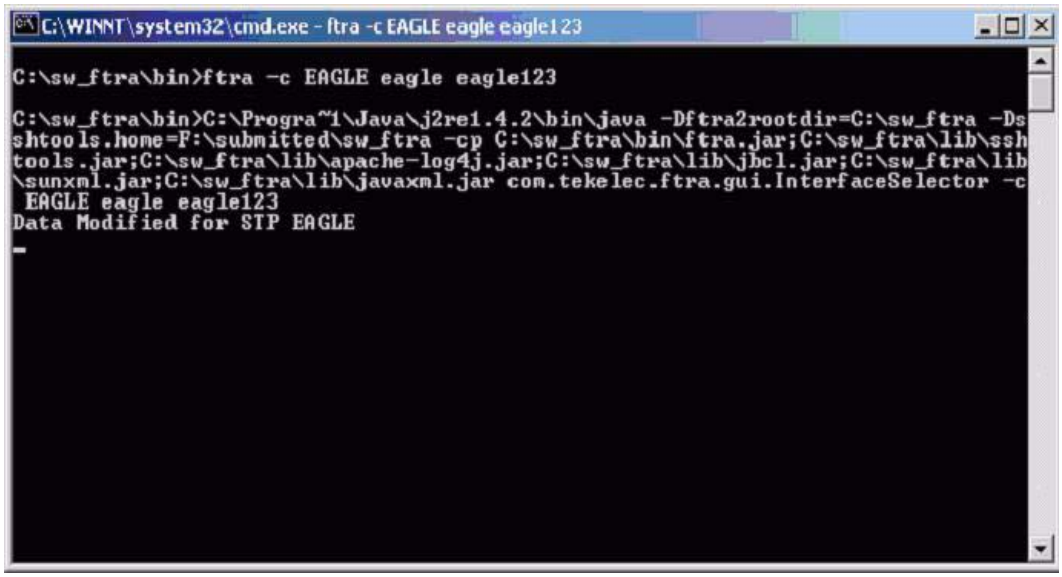


Command line interface

FTRA 4.0 supports modifying the STP Username and STP Password through the CLI for an STP whose configuration already exists in the system. Using the CLI the STP username and password can be modified in the system configuration without interacting with the GUI. Figure 119 shows the FTRA command line interface for modifying the STP Username and STP Password through the CLI for an STP "EAGLE".

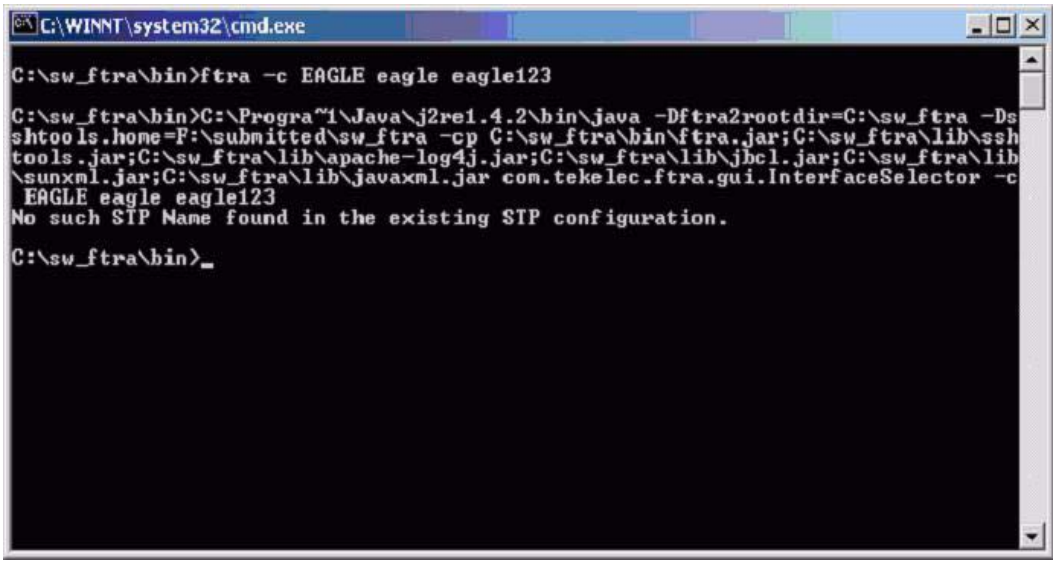
After successfully updating the STP parameters in the system configuration, a message will be displayed as shown in the Figure 119.

Figure 119. STP data modified through CLI.



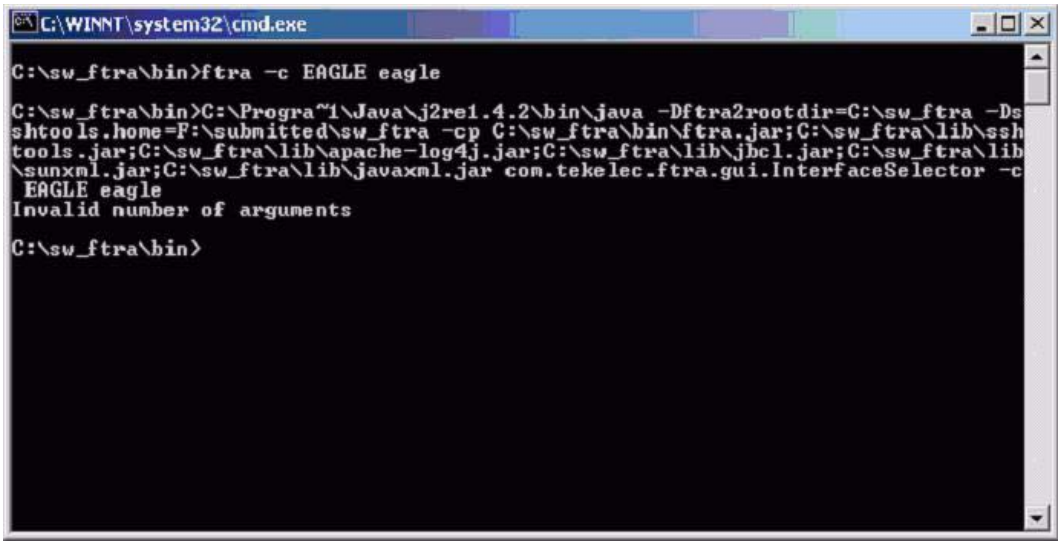
If the user supplied STP name doesn't match with one of the existing STP(s) configured in the system, an error message shall be displayed as shown in Figure 120 on page 116.

Figure 120. Invalid STP name



If the user supplies a wrong number of arguments through the command line then the error message as shown in Figure 121 on page 116 is displayed.

Figure 121. Invalid number of arguments.



Version Information

FTRA Release 4.0 displays an “About FTRA” window. Figure 149 shows the new FTRA Version string and updated copyright information.

Figure 122. About FTRA Display Window

SSH/SFTP Error Codes

Table 10 and Table 11 on page 131 contain a list of the error codes that can be generated when making a secure connection between the FTRA, version 4.0, and the EAGLE 5 ISS. Each error code contains a brief description of the error and the suggested recovery action.

This section also contains procedures, following Tables 10 and 11, for testing connectivity and network problems, and to verify that the setup for making secure connections is correct.

If secure connections to the EAGLE 5 ISS cannot be made, verify that the Eagle OA&M IP Security Enhancements feature is enabled and activated by entering the **`rtrv-ctrl-feat`** command at the EAGLE 5 ISS before performing any of the actions in Tables 10 and 11. If the Eagle OA&M IP Security Enhancements feature is not enabled or activated, perform the "Activating the Eagle O&AM IP Security Enhancements Controlled Feature" procedure in the *Database Administration Manual - System Management* and enable and activate the Eagle OA&M IP Security Enhancements feature.

If any of the errors shown in Table 10 or Table 11 on page 131 are encountered after the recovery procedure is verified, contact the Customer Care Center. Refer to page 5 for the contact information.

Table 10. FTP/SFTP/SSH Error Codes

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
User Errors		
594	Invalid Path	Verify that the path is valid in the **FTP Server Configuration Menu** window (see Figure 45 on page 53).
598	The SSHD daemon is not running on the destination system or the server IP address unavailable.	Verify that the IP address exists on network with a ping (Refer to the "Connectivity Test – I" section on page 134 and the "Connectivity Test - II" section on page 135). If the IP address exists on network then verify that SSHD daemon is running on the destination machine using the **`ps -ef`**|**`grep sshd`** command.
629	The SFTP daemon is not running	Verify that the subsystem entry in the **`sshd_config`** file on the destination station is specified and points to the SFTP daemon.

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
633	User login failure.	Verify that the Username and Password in the **STP Connection Configuration Menu** window, (see Table 2 on page 24) is valid and an account exists for the username and password on the SSHD server host.
SFTP Errors		
595	File open failed.	Invalid file name in the download list, or out of resources. Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
596	The file name is already specified.	Report this issue to the Customer Care Center immediately. (Internal SFTP implementation error). Refer to page 5 for the contact information.
SFTP Client Errors		
597	SFTP client packet send failure	Perform these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
598	The SFTP connection is closed.	
599	SFTP packet read failure	
600	SFTP protocol error. The received message is larger than the expected packet size.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 136. If the error persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
601	Undefined	Notify the Customer Care Center. Refer to page 5 for the contact information.
608	SFTP received a invalid ID in the response received during a read operation on remote directory.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 136. If the error persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
609	SFTP: Handle mismatch error. This error is displayed when there is a failure to receive an expected handle upon successful READ/WRITE/ CREAT/TRUNC/EXCL of a file using SSH_FXP_OPEN on remote server.	
610	Unexpected SSH2_FXP_ATTRS.	
611	Unexpected SSH_FXP_NAME. SFTP using the SSH_FXP_OPENDIR opens a directory for reading. The server responds to this request with either a SSH_FXP_NAME or a SSH_FXP_STATUS message. This error code implies that an unexpected SSH_FXP_NAME is received.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 136.
612	The SFTP client uses the SSH_FXP_REALPATH request to have the server localize any given path name to an absolute path. This is useful for converting path names containing ".." components or relative pathnames without a leading slash into absolute paths. This error implies that there is a failure during this operation	Check if the access to the path specified in the **FTP Server Configuration Menu** window (see Figure 45 on page 53) is accessible and re-try the connection.

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
613	The SSH_FXP_READLINK request is used by the SFTP client to read the target of a symbolic link. The server will respond with a SSH_FXP_NAME packet containing only one name and a dummy attributes value. The name in the returned packet contains the target of the link. This failure implies that there is a failure during the READLINK operation.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing the tests in "Network Outage Trouble Shooting" section on page 136.
614	The SFTP client receives SSH_FXP_DATA as a response to any file operations from the server. This error implies that the client received an unexpected SSH_FXP_NAME from the server.	
615	The SFTP client received more data than expected.	
616	The SFTP client failed to read the data from the file descriptor of the file specified for transfer.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
SSH Client Errors		
617	Excessive identity files. This error means that there are excessive identity files. OpenSSH implementation contains the maximum of 100 identity files or the client configuration file is corrupted.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
624	The debug levels allowed for SSH protocol in openSSH is 0-9. There is either an error in the client configuration file, or the client configuration file is corrupted.	

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
625	Failure to read the client configuration file.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
626	Invalid compression level is specified in the client configuration file.	
627	SSH failure to setup the IO with the server.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
628	SSH failure to open the channel for the SSH connection with the server.	
629	SSH failure to setup the channel for the SSH connection with the server.	
630	SSH failure to verify the SSH client host key.	
631	SSH user authentication failure. Please verify that only the password authentication is set to "yes" in the SSH server configuration file. Refer to the SSHD server configuration provided by vendor of the product. The FTRA and the EAGLE 5 ISS is compatible with **openSSH 3.0.2p1**.	Report the issue to the Customer Care Center if the problem persists after the SSHD configuration file is verified. Refer to page 5 for the contact information.
632	The authentication method is NULL in the client software. This error is a failure to set the null authentication method.	Report this issue to the Customer Care Center. Refer to page 5 for the contact information.

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
633	Permission is denied by the server due to authentication failure.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
640	A bad message was received during the SSH authentication.	
641	Missing authentication context, encountered during the SSH user authorization.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
642	Failure during the public key read/verification operation.	
643	Undefined SFTP/SSH error.	

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
644	Unexpected SSH_FXP_STATUS error. An invalid status was received by the SFTP server.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
645	A bad option was specified in the SSH client on the EAGLE 5 ISS.	
646	An unsupported escape character was used in the SSH client on the EAGLE 5 ISS.	
647	An unsupported cipher type was used in the SSH client on the EAGLE 5 ISS.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
648	An unsupported MAC type was used in the SSH client on the EAGLE 5 ISS.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
649	A bad port was used in the SSH client on the EAGLE 5 ISS.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
656	Bad forwarding was used in the SSH client on the EAGLE 5 ISS.	
657	Bad forwarding ports were specified in the SSH client on the EAGLE 5 ISS.	
658	A bad dynamic port was specified in the SSH client on the EAGLE 5 ISS.	

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
659	The host was not specified in the SSH client on the EAGLE 5 ISS.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
660	An invalid option or argument was specified in the SSH client on the EAGLE 5 ISS.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
661	The hostname was not specified in the SSH client on the EAGLE 5 ISS.	
663	The SSH client was unable to load the cipher type on the EAGLE 5 ISS.	
664	Asynchronous IO is not supported on IPSM, SSH client error.	
665	Compression is already enabled in the SSH client on the EAGLE 5 ISS.	
666	Unknown cipher number on the SSH client on the EAGLE 5 ISS.	
667	The SSH client key length is invalid.	

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
668	No key is available on the SSH client on the EAGLE 5 ISS.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
669	The secure connection was closed by the remote server, refer to the error on the SFTP/SSHD server side.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
670	Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network.	
671	An unexpected packet type was received from the SFTP/SSHD server.	
672	A bad packet length was received from the SSHD/SFTP server.	
673	A cryptographic attack was detected by the SSH client. Please notify the local system administrator.	Report the issue to the Customer Care Center. Refer to page 5 for the contact information. This is not a software problem but there is a security threat. The keys/authentication may have to be updated immediately.

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
674	The SSH/SFTP client on the EAGLE 5 ISS failed to read from the remote side.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
675	Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 ISS.	
676	Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 ISS.	Verify that the **`sshtools.xml`** file provided with FTRA software has the field as shown: <!-- The Message Authentication Code configuration, add or override default mac implementations --> <MacConfiguration> <DefaultAlgorithm>hmac-md5</DefaultAlgorithm> </MacConfiguration>
677	Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 ISS.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
678	SSH/SFTP tried to close a connection that is already closed.	

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
679	The SSH/SFTP client on the EAGLE 5 ISS failed to write to the remote side.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
680	SSH/SFTP tried to set the packet size twice.	Report this issue to the Customer Care Center immediately. Refer to page 5 for the contact information.
681	A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 ISS.	

Table 10. FTP/SFTP/SSH Error Codes (Continued)

SFTP/SSH Generic Network Client Error Code	Description	Action/Recovery
SSH/SFTP Connection/Setup Errors		
682	The connection timed out when SSH tried to connect to SSHD.	Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests: • "FTP Server Verification" on page 134 • "SFTP /SSHD Server Verification" on page 134 • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
683	The SSH connection was refused by the remote server.	
684	The SSHD server is unreachable.	
685	The network has reset.	
686	The SSH/SFTP connection has been aborted.	
687	The SFTP/SSH connection has been reset by the peer.	
688	Failed to allocate network buffers.	
689	The SSH/SFTP socket is already connected.	
690	The SSH/SFTP socket is not connected.	
691	The network channel is down.	
692	The SSHD/SFTP server connection host is down.	
693	SFTP client channel read failure.	
694	SFTP client channel write failure.	
695	SFTP client channel open failure.	

Table 11. Generic Network Error Codes

SFTP/SSH/ Generic Network Client Error Code	Description	Action/Recovery
40	A destination address is required.	Verify that there is an FTP server entry on the EAGLE 5 ISS using the **rtrv-ftp-serv** command, and re-try the connection
41	Protocol wrong type for socket	Report this issue to the Customer Care Center. Refer to page 5 for the contact information.
42	The protocol is not available.	
43	The protocol is not supported.	
44	The socket type is not supported.	
45	The operation is not supported on the socket.	
46	The protocol family is not supported.	
47	The address family is not supported.	
48	The address is already in use.	
49	The requested address cannot be assigned.	
50	Socket operation on non-socket	
51	The network is unreachable.	Verify that the connection tests and network outage numbers match as shown in these sections: • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
52	The network dropped the connection on reset.	
53	Software caused the connection to abort.	Report this issue to the Customer Care Center. Refer to page 5 for the contact information.

Table 11. Generic Network Error Codes (Continued)

SFTP/SSH/ Generic Network Client Error Code	Description	Action/Recovery
54	The connection was reset by the peer.	Verify that the connection tests pass and network outage numbers are within the allowed limits as shown in these sections: • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
55	No buffer space available.	Report this issue to the Customer Care Center. Refer to page 5 for the contact information.
56	The socket is already connected.	
57	The socket is not connected.	
58	Can't send after socket shutdown	
59	Too many references: can't splice	
60	The connection timed out.	Perform these tests and verify that the FTP server address responds to the ping command from the ISPM. • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135
61	The connection was refused.	Verify that there is a FTP server daemon is running on the remote station by performing the "FTP Server Verification" test on page 134.

Table 11. Generic Network Error Codes (Continued)

SFTP/SSH/ Generic Network Client Error Code	Description	Action/Recovery
62	The network is down.	Verify that the connection tests pass and network outage numbers are within the allowed limits as shown in these sections: • "Connectivity Test – I" on page 134 • "Connectivity Test - II" on page 135 • "Network Outage Trouble Shooting" on page 136. Make any fixes necessary and retry the connection. If the problem persists, report the issue to the Customer Care Center. Refer to page 5 for the contact information.
65	There is no route to the host.	
67	The host is down.	
30	Read-only file system	
32	Broken pipe	Report the issue to the Customer Care Center. Refer to page 5 for the contact information.
35	Unsupported value	

Troubleshooting Procedures

FTP Server Verification

Component: The FTP server IP address shown in the **FTP Server Configuration Menu** window (see Figure 45 on page 53).

Supported Version/Specification: Any FTP server compliant with IETF RFC 959.

Test: On the Unix platform, execute the **`netstat -a|grep 21`** command to verify that the FTP server is running on the machine with the IP address shown in the **FTP Server Configuration Menu** window (Figure 45 on page 53).

Expected Result:

```
    Unix>  netstat -a | grep 21
    *.32821              *.*                0      0      0      0 LISTEN
    f5e15218 stream-ord f5ee8880        0 /var/adm/atria/almd    , The system and
process specific variable will change.
```

On the Windows platform, check the Task Manager to verify that the FTP daemon is running.

SFTP /SSHD Server Verification

Component: The SSHD/SFTP server IP address shown in the **FTP Server Configuration Menu** window (see Figure 45 on page 53).

Supported Version/Specification: Version compatible with openSSH 3.0.2p1.

Test: On the Unix platform, execute the **`ps -f|grep sshd`** command. Please refer to Unix MAN pages for help with **`ps`** command.

On the Windows platform, use the Task Manager to verify that the sshd daemon process in running.

Expected Result:

```
    Unix> ps -ef|grep sshd
    user   26912 26886  0 13:28:07 pts/5    0:00 grep sshd
    root   411     1  0   Jul 24 ?        4:35 /usr/local/sbin/sshd  Note: The
user/system/path variables depends on the server.
```

On the Windows platform, check the Task Manager to verify that the FTP daemon is running.

Connectivity Test – I

Component: Connectivity Test - I.

Supported Version/Specification: N/A

Test: To verify that there is a network connection available between the EAGLE 5 ISS and the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 45 on page 53).

On an EAGLE 5 ISS terminal, enter the **pass:loc=xxxx:cmd="ping yy.yy.yy.yy"** command, where **xxxx** is location of IPSM associated with the IP address entered in the **STP Connection Configuration Menu** window, (see Table 2 on page 24), and **yy.yy.yy.yy** is the IP address of the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 45 on page 53).

Expected Result:

NOTE: The RTT time and data sizes may vary.

```
> pass:loc=xxxx:cmd="ping yy.yy.yy.yy"
Command Accepted - Processing
    rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
    pass:loc=xxxx:cmd="ping yy.yy.yy.yy"
    Command entered at terminal #5.
;
    rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
    PASS: Command sent to card
;
    rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
    PING command in progress
;
    rlghncxa03w 05-09-31 13:57:59 GMT  EAGLE5 34.0.0
;
    rlghncxa03w 05-09-31 13:58:01 GMT  EAGLE5 34.0.0
    PING yy.yy.yy.yy: 56 data bytes
    64 bytes from yy.yy.yy.yy: icmp_seq=0. time=10. ms
    64 bytes from yy.yy.yy.yy: icmp_seq=1. time=5. ms
    64 bytes from yy.yy.yy.yy: icmp_seq=2. time=5. ms
    ----yy.yy.yy.yy PING Statistics----
    3 packets transmitted, 3 packets received, 0% packet loss
    round-trip (ms)  min/avg/max = 5/6/10
    PING command complete
```

Connectivity Test - II

Component: Connectivity Test - II.

Supported Version/Specification: N/A.

Test: To verify that there is a network connection available between the EAGLE 5 ISS and FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 45 on page 53).

Execute the **ping -s zz.zz.zz.zz** command on the FTP server machine where **zz.zz.zz.zz** is the IP address of the EAGLE 5 ISS shown in the **STP Connection Configuration Menu** window (see Table 2 on page 24).

Expected Result:

```
ping -s zz.zz.zz.zz
PING zz.zz.zz.zz: 56 data bytes
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=0. time=5. ms
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=1. time=4. ms
```

```
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=2. time=5. ms
64 bytes from e1011501-3-a (zz.zz.zz.zz): icmp_seq=3. time=4. ms

----zz.zz.zz.zz PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 4/4/5
```

Network Outage Trouble Shooting

Component: Network Outage Troubleshooting

Supported Version/Specification: N/A.

Test: To verify the TCP/IP traffic/network statistics are within the Tekelec supported network statistics.

At the EAGLE 5 ISS, enter the **`pass:loc=xxxx:cmd="netstat -p tcp"`** command at the EAGLE 5 ISS terminal, where **`xxxx`** is location of the IPSM associated with the IP address entered in the **STP Connection Configuration Menu** window, (see Table 2 on page 24), and analyze the data from output which is similar to the following example output.

NOTE: The specific information for the command may vary depending upon the system used.

```
> pass:loc=3102:cmd="netstat -p tcp"
Command Accepted - Processing
    rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0
    pass:loc=3102:cmd="netstat -p tcp"
    Command entered at terminal #5.
;
    rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0
    PASS: Command sent to card
;
    rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0
    TCP:
        161 packets sent
                156 data packets (28411 bytes)
                0 data packet (0 byte) retransmitted
                5 ack-only packets (1 delayed)
                0 URG only packet
                0 window probe packet
                0 window update packet
                0 control packet
        161 packets received
                156 acks (for 28255 bytes)
                0 duplicate ack+C2
                0 ack for unsent data
                5 packets (9 bytes) received in-sequence
                0 completely duplicate packet (0 byte)
                0 packet with some dup. data (0 byte duped)
                0 out-of-order packet (0 byte)
                0 packet (0 byte) of data after window
                0 window probe
                0 window update packet
                0 packet received after close
                0 discarded for bad checksum
                0 discarded for bad header offset field
                0 discarded because packet too short
        0 connection request
```

```
            1 connection accept
            1 connection established (including accepts)
            0 connection closed (including 0 drop)
            0 embryonic connection dropped
            156 segments updated rtt (of 157 attempts)
            0 retransmit timeout
                    0 connection dropped by rexmit timeout
            0 persist timeout
            0 keepalive timeout
                    0 keepalive probe sent
                    0 connection dropped by keepalive
            0 pcb cache lookup failed

;

    rlghncxa03w 05-09-31 19:32:52 GMT  EAGLE5 34.0.0

    NETSTAT command complete
```

Expected Result:

The network outage causes the TCP/IP problems like:

- Network latency
- Packet drop
- Duplicate packets.

If the TCP Packet Delay, TCP Packet Loss, TCP Packet Error, or TCP Out of Order values are greater than the values shown in Table 12, fix the network problems and retry the connection.

Table 12. TCP Fault Tolerance Table for FTP/SFTP

Protocol	Fault	Threshold Value
SFTP/FTP	TCP Packet Delay	175 milliseconds
SFTP/ FTP	TCP Packet Loss	40% packet loss
SFTP/ FTP	TCP Packet Errors	10%
SFTP/ FTP	TCP Out of Order	30% of packets with offset of 30 packets

SSH/SFTP/SFTPD/SSHD Protocol Troubleshooting

For more information on SSH/SFTP/SFTPD/SSHD protocol troubleshooting, refer to *SSH, the Secure Shell: The Definitive Guide*, First Edition, Barrett and Silverman, O'Reilly, February 2001.

Index

Symbols

.doc file extension, 39, 77, 105, 110
.txt file extension, 39, 77, 105, 110

Numerics

30 - Read-only file system, 133
32 - Broken pipe, 133
35 - Unsupported value, 133
40 - A destination address is required, 131
41 - Protocol wrong type for socket, 131
42 - The protocol is not available, 131
43 - The protocol is not supported, 131
44 - The socket type is not supported, 131
45 - The operation is not supported on the socket, 131
46 - The protocol family is not supported, 131
47 - The address family is not supported, 131
48 - The address is already in use, 131
49 - The requested address cannot be assigned, 131
50 - Socket operation on non-socket, 131
51 - The network is unreachable, 131
52 - The network dropped the connection on reset, 131
53 - Software caused the connection to abort, 131
54 - The connection was reset by the peer, 132
55 - No buffer space available, 132
56 - The socket is already connected, 132
569 - The file name is already specified, 119
57 - The socket is not connected, 132
58 - Can’t send after socket shutdown, 132
59 - Too many references: can’t splice, 132
595 - File open failed, 119
597 - SFTP client packet send failure, 119
598 - The SFTP connection is closed, 119
599 - SFTP packet read failure, 119
60 - The connection timed out, 132
600 - SFTP protocol error, 119
601 - Undefined, 120
608 - SFTP received a invalid ID in the response received during a read operation on remote directory, 120
609 - SFTP: Handle mismatch error, 120
61 - The connection was refused, 132
610 - Unexpected SSH2_FXP_ATTRS, 120
611 - Unexpected SSH_FXP_NAME, 120
612 - SSH_FXP_REALPATH request failure, 120
613 - SSH_FXP_READLINK request failure, 121
614 - unexpected SSH_FXP_NAME, 121
615 - The SFTP client received more data than expected, 121
616 - The SFTP client failed to read the data from the file descriptor, 121
617 - Excessive identity files, 121
62 - The network is down, 133
624 - The debug levels allowed for SSH protocol in openSSH is 0-9, 121
625 - Failure to read the client configuration file, 122
626 - Invalid compression level is specified in the client configuration file, 122
627 - SSH failure to setup the IO with the server, 122
628 - SSH failure to open the channel for the SSH connection with the server, 122
629 - SSH failure to setup the channel for the SSH connection with the server, 122
630 - SSH failure to verify the SSH client host key, 122
631 - SSH user authentication failure, 122
632 - The authentication method is NULL in the client software, 122
633 - Permission is denied by the server due to authentication failure, 123
633 - User login failure, 119
640 - A bad message was received during the SSH authentication, 123
641 - Missing authentication context, encountered during the SSH user authorization, 123
642 - Failure during the public key read/verification operation, 123
643 - Undefined SFTP/SSH error, 123
644 - Unexpected SSH_FXP_STATUS error, 124
645 - A bad option was specified in the SSH client

on the EAGLE 5 ISS, 124
646 - An unsupported escape character was used in the SSH client on the EAGLE 5 ISS, 124
647 - An unsupported cipher type was used in the SSH client on the EAGLE 5 ISS, 124
648 - An unsupported MAC type was used in the SSH client on the EAGLE 5 ISS, 125
649 - A bad port was used in the SSH client on the EAGLE 5 ISS, 125
65 - There is no route to the host, 133
656 - Bad forwarding was used in the SSH client on the EAGLE 5 ISS, 125
657 - Bad forwarding ports were specified in the SSH client on the EAGLE 5 ISS, 125
658 - A bad dynamic port was specified in the SSH client on the EAGLE 5 ISS, 125
659 - The host was not specified in the SSH client on the EAGLE 5 ISS, 126
660 - An invalid option or argument was specified in the SSH client on the EAGLE 5 ISS, 126
661 - The hostname was not specified in the SSH client on the EAGLE 5 ISS, 126
663 - The SSH client was unable to load the cipher type on the EAGLE 5 ISS, 126
664 - Asynchronous IO is not supported on IPSM, SSH client error, 126
665 - Compression is already enabled in the SSH client on the EAGLE 5 ISS, 126
666 - Unknown cipher number on the SSH client on the EAGLE 5 ISS, 126
667 - The SSH client key length is invalid, 126
668 - No key is available on the SSH client on the EAGLE 5 ISS, 127
669 - The secure connection was closed by the remote server, 127
67 - The host is down, 133
670 - Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network, 127
671 - An unexpected packet type was received from the SFTP/SSHD server, 127
672 - A bad packet length was received from the SSHD/SFTP server, 127
673 - A cryptographic attack was detected by the SSH client, 127
674 - The SSH/SFTP client on the EAGLE 5 ISS failed to read from the remote side, 128
675 - Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 ISS, 128
676 - Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 ISS, 128
677 - Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 ISS, 128
678 - SSH/SFTP tried to close a connection that is already closed, 128
679 - The SSH/SFTP client on the EAGLE 5 ISS failed to write to the remote side, 129
680 - SSH/SFTP tried to set the packet size twice, 129
681 - A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 ISS, 129
682 - The connection timed out when SSH tried to connect to SSHD, 130
683 - The SSH connection was refused by the remote server, 130
684 - The SSHD server is unreachable, 130
685 - The network has reset, 130
686 - The SSH/SFTP connection has been aborted, 130
687 - The SFTP/SSH connection has been reset by the peer, 130
688 - Failed to allocate network buffers, 130
689 - The SSH/SFTP socket is already connected, 130
690 - The SSH/SFTP socket is not connected, 130
691 - The network channel is down, 130
692 - The SSHD/SFTP server connection host is down, 130
693 - SFTP client channel read failure, 130
694 - SFTP client channel write failure, 130
695 - SFTP client channel open failure, 130

A

A bad dynamic port was specified in the SSH client on the EAGLE 5 ISS - Error code 658, 125
A bad message was received during the SSH authentication - Error code 640, 123
A bad option was specified in the SSH client on the EAGLE 5 ISS - Error code 645, 124
A bad packet length was received from the SSHD/SFTP server - Error code 672, 127

A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 ISS - Error code 681, 129
A bad port was used in the SSH client on the EAGLE 5 ISS - Error code 649, 125
A cryptographic attack was detected by the SSH client - Error code 673, 127
A destination address is required - Error code 40, 131
About FTRA window, 20, 112
Activating Controlled Features procedure, 5
Activating the Eagle OA&M IP Security Enhancements Controlled Feature procedure, 5, 25, 29, 42, 118
Add button, 2, 24, 26, 30, 64
  Retrieve Tables, 59
Adding
  Command to the Selected Commands Box, 64
  Multiple Commands to the Selected Commands Box, 66
  Range of Commands to the Selected Commands Box, 65
  STP Configuration Record, 26, 51
Adding an STP Configuration Record FTRA 2.0, 26, 27, 28, 29, 30
alw-card command, 46
An invalid option or argument was specified in the SSH client on the EAGLE 5 ISS - Error code 660, 126
An unexpected packet type was received from the SFTP/SSHD server - Error code 671, 127
An unsupported cipher type was used in the SSH client on the EAGLE 5 ISS - Error code 647, 124
An unsupported escape character was used in the SSH client on the EAGLE 5 ISS - Error code 646, 124
An unsupported MAC type was used in the SSH client on the EAGLE 5 ISS - Error code 648, 125
Application, FTRA
  exiting, 6, 21
  starting, 6
  using, 6
Asynchronous IO is not supported on IPSM, SSH client error - Error code 664, 126

B

Backup IP Address - FTRA 2.0, 27, 28
Backup IP Address - FTRA 2.0 or greater, 24
Backup IP Address Field - FTRA 2.0 or greater, 24, 27, 28
Bad forwarding ports were specified in the SSH client on the EAGLE 5 ISS - Error code 657, 125
Bad forwarding was used in the SSH client on the EAGLE 5 ISS - Error code 656, 125
Box
  Command List, 57, 59, 61, 66
  Secure Connection - FTRA 2.0 or greater, 25, 29, 42, 46, 51, 52
  Selected Commands, 57, 59, 64, 66, 68
    Adding a Command, 64
    Adding a Range of Commands, 65
    Adding Multiple Commands, 66
    Command Removed, 67
    Command Selected to be Removed, 67
  Stop on error
    Update Tables, 91
  Stop on error, Update Tables window, 88, 91, 100, 101, 102
  Use STP and FTP UserNames, Passwords for all STPs, 25, 26, 40, 41
Broken pipe - Error code 32, 133
Browse button
  FTP Server Configuration Menu, 53, 54
  Update Tables, 88, 89
Button
  Add, 2, 24, 26, 30, 59, 64
  Browse
    FTP Server Configuration Menu, 53, 54
    Update Tables window, 88, 89
  Cancel, 38
    Print window
      Retrieve Tables Log, 76
      System Log, 109
      Update Tables Log, 104
    Save window
      Retrieve Tables Log, 77
      System Log, 111
      Update Tables Log, 106
    Select Starting Directory window, 55
    Select window, 89, 90
  Close, 25, 32, 33, 53

Retrieve Tables, 59
Update Tables, 88
Commit, Update Validation Complete window, 93, 94
Delete, 24, 32, 33, 43
Edit, Update Validation Complete window, 93, 94, 95, 96
Load, 59, 68, 79
Modify, 24, 40, 41
Refresh, 24, 31, 32, 33, 42
Remove, 59, 66
Reset, 59, 66
Retrieve, 57, 59, 68, 69
Retrieve from Local Database, 57, 59, 68
Retrieve from STP, 57, 59, 69
Save
Retrieve Tables Log, 77
System Log, 111
Update Tables Log, 105
Select, 24, 32, 33
Select Starting Directory window, 55
Select window, 89, 90
Set, 55
FTP Server Configuration Menu, 53
Stop, Update Validation Complete window, 93
Store, 59, 68, 79
Test, 24, 32, 33, 35
Validate, 88, 92
Update Tables window, 87

C

Can’t send after socket shutdown - Error code 58, 132
Cancel button, 38
Print window
Retrieve Tables Log, 76
System Log, 109
Update Tables Log window, 104
Save window
Retrieve Tables Log, 77
System Log, 111
Update Tables Log, 106
Select Starting Directory window, 55
Select window, 89, 90
Card
GPSM-II, 5
IPSM, 5
MCAP, 5
TDM, 5
CD-ROM drive, 7
chg-ftp-serv EAGLE 5 ISS command, 53
chg-trm command, 49
chg-trm:trm=:all=no EAGLE 5 ISS command, 69
chmod command, 53, 54
Clearing the display
Connectivity Test Log, 36, 37
Retrieve Tables Log, 74
System Log, 107, 108
Update Tables Log, 102, 103
Close button
FTP Connection Configuration Menu, 53
Retrieve Tables window, 59
STP Connection Configuration Menu, 25, 32, 33
Update Tables, 88
Closing
Connectivity Test Log window, 36, 40
Retrieve Tables Log window, 74, 78
System Log window, 107, 111
Update Tables Log window, 102, 106
Command
EAGLE 5 ISS
alw-card, 46
chg-ftp-serv, 53
chg-trm, 49
chg-trm:trm=:all=no, 69
ent-ftp-serv, 53
init-card, 46, 49, 50
pass:loc=xxxx
cmd="netstat -p tcp", 136
cmd="ping yy.yy.yy.yy", 135
rst-card, 46
rtrv, 59, 79, 85
rtrv-card, 5
rtrv-ctrl-feat, 5, 25, 29, 42, 118
rtrv-feat, 57
rtrv-ftp-serv, 131
rtrv-gta, 57, 62, 69
rtrv-gtt, 57, 62, 69
rtrv-gttsel, 57, 62, 69
rtrv-gttset, 57, 62, 69
rtrv-ip-lnk, 49, 50
rtrv-secu-dflt, 28

rtrv-stp, 72, 73
rtrv-trm, 48, 49, 69
rtrv-tt, 57, 62, 69
FTRA
ftra -c, 79, 85
Selecting, 61
Command Complete
Connectivity Test window, 36
Retrieve Tables window, 57, 70, 71
Update Tables window, 93, 94, 97
Command File
Editing, 3, 95
Editor window, 93, 95, 96, 97
File Menu, 97
File Menu, 97
Invalid Command, 96
Field, Update Tables window, 89, 90, 92
Selected, Update Tables window
Stop on error box checked, 91
Sending to the Selected STP, 94
Command files, sending to the EAGLE 5 ISS, 6
Command In progress, Cannot Close Window message, 96
Command Line Interface, 2, 59, 67, 68, 79
Automatic Start, 85
Manual Start, 79
UNIX, 81
Windows, 80
Command List
Box, 57, 59, 61, 66
Field
Retrieve Tables window, 59
Update Tables window, 88
Side, 66
command prompt
DOS, 79
shell, 79
Command Removed from the Selected Commands Box, 67
Command Selected to be Removed in the Selected Commands Box, 67
Commands
EAGLE 5 ISS, 2, 87, 88
EGTT
rtrv-gta, 57, 62, 69
rtrv-gttsel, 57, 62, 69
rtrv-gttset, 57, 62, 69
GTT
rtrv-gtt, 57, 62, 69
rtrv-tt, 57, 62, 69
Menu, 20
Menu window, 59, 68, 88
Selecting a Range, 62
Selecting Multiple, 63
Commit button, Update Validation Complete window, 93, 94
Compression is already enabled in the SSH client on the EAGLE 5 ISS - Error code 665, 126
Configuration record, STP, 23, 24, 26, 31, 32, 33, 34, 35, 40, 41, 42, 43, 44, 45, 46, 51
FTRA 2.0, 33, 34
Configuration record, STP - FTRA 2.0
Adding, 26, 27, 28, 29, 30
Configuring the EAGLE 5 ISS, 5
Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network - Error code 670, 127
Connectivity Test - I procedure, 134
Connectivity Test - II procedure, 135
Connectivity Test Log, 35, 36, 37, 38, 39
Clearing the Display, 36, 37
closing, 36, 40
File Menu, 36
Print window, 37, 38
Printing, 36, 37
Save window, 39
saved file confirmation window, 39, 40
saving to a file, 36, 39
window, 35, 36, 37, 39, 40, 47, 50, 51
errors, 36
no errors, 35
Connectivity Test Log window
File Menu, 36, 37
copyright information, 112
Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 ISS - Error code 675, 128
Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 ISS - Error code 676, 128
Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 ISS - Error code 677, 128
cron, 79, 85

CSV file format, 2, 57, 59, 68, 79, 85
Current STP
Selected, 44
FTRA 2.0, 45
Selected: field, 42
Selecting, 6, 43
Customer Care Center, 5, 49, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133

D

Database Administration Manual - System Management, 5, 25, 29, 42, 118
Database tables, retrieving from the EAGLE 5 ISS, 6
Database, STP Connection Configuration, 23, 24, 25, 26, 30, 43
Delete button, 24, 32, 33, 43
Delete STP Data window, 43
Deleting an STP Configuration Record, 43
Description
Retrieve Tables window, 59
Update Tables window, 88
Display
Clearing
Connectivity Test Log, 36, 37
Retrieve Tables Log, 74
System Log, 107, 108
Update Tables Log, 102, 103
Displaying an Existing STP Configuration Record, 31
DOS command prompt, 79
Drop down list
STP Name, 24, 31
FTRA 2.0, 31, 32
DSA Key Fingerprint, 49, 50
Duplicate packets, 137

E

EAGLE 5 ISS
Telnet terminals, 24, 49, 69
UIM - Unsolicited Information Message, 49, 50, 69
EAGLE 5 ISS Card
GPSM-II, 5
IPSM, 5
MCAP, 5
TDM, 5
EAGLE 5 ISS chg-ftp-serv command, 53
EAGLE 5 ISS chg-trm:trm=:all=no command, 69
EAGLE 5 ISS command
alw-card, 46
chg-ftp-serv, 53
chg-trm, 49
chg-trm:trm=:all=no, 69
ent-ftp-serv, 53
init-card, 46, 49, 50
pass:loc=xxxx
cmd="netstat -p tcp", 136
cmd="ping yy.yy.yy.yy", 135
rst-card, 46
rtrv, 59, 79, 85
rtrv-card, 5
rtrv-ctrl-feat, 5, 25, 29, 42, 118
rtrv-feat, 57
rtrv-ftp-serv, 131
rtrv-gta, 57, 62, 69
rtrv-gtt, 57, 62, 69
rtrv-gttsel, 57, 62, 69
rtrv-gttset, 57, 62, 69
rtrv-ip-lnk, 49, 50
rtrv-secu-dflt, 28
rtrv-stp, 72, 73
rtrv-trm, 48, 49, 69
rtrv-tt, 57, 62, 69
EAGLE 5 ISS command files
sending, 6
EAGLE 5 ISS commands, 2, 87, 88
EAGLE 5 ISS configuration, 5
EAGLE 5 ISS database tables
retrieving, 6
EAGLE 5 ISS EGTT commands
rtrv-gta, 57, 62, 69
rtrv-gttsel, 57, 62, 69
rtrv-gttset, 57, 62, 69
EAGLE 5 ISS ent-ftp-serv command, 53
EAGLE 5 ISS Feature
EGTT, 57
FTP Retrieve and Replace, 5
GTT, 57
IP User Interface, 5
EAGLE 5 ISS feature
Eagle OA&M IP Security

Enhancements, 5, 25, 29, 42, 118
EAGLE 5 ISS GTT commands
rtrv-gtt, 57, 62, 69
rtrv-tt, 57, 62, 69
EAGLE 5 ISS Manual, Database Administration Manual - System Management, 5, 25, 29, 42, 118
EAGLE 5 ISS pass:loc=xxxx
cmd="netstat -p tcp" command, 136
cmd="ping yy.yy.yy.yy" command, 135
EAGLE 5 ISS procedure
Activating Controlled Features, 5
Activating the Eagle OA&M IP Security Enhancements Controlled Feature, 5, 25, 29, 42, 118
EAGLE 5 ISS Public Host Key Fingerprint, 46, 47, 49, 51
EAGLE 5 ISS Public Key Fingerprint, 25, 49, 50
EAGLE 5 ISS release 30.2 or greater, 5, 25, 29
EAGLE 5 ISS rtrv-card command, 5
EAGLE 5 ISS rtrv-ctrl-feat command, 5, 25, 29, 42, 118
EAGLE 5 ISS rtrv-feat command, 57
EAGLE 5 ISS rtrv-ftp-serv command, 131
EAGLE 5 ISS rtrv-gta command, 57, 62, 69
EAGLE 5 ISS rtrv-gtt command, 57, 62, 69
EAGLE 5 ISS rtrv-gttsel command, 57, 62, 69
EAGLE 5 ISS rtrv-gttset command, 57, 62, 69
EAGLE 5 ISS rtrv-secu-dflt command, 28
EAGLE 5 ISS rtrv-stp command, 72, 73
EAGLE 5 ISS rtrv-trm command, 69
EAGLE 5 ISS rtrv-tt command, 57, 62, 69
Eagle OA&M IP Security Enhancements feature, 5, 25, 29, 42, 118
Edit button, Update Validation Complete window, 93, 94, 95, 96
Edit menu
FTP-Based Table Retrieve Application, 23, 88
Editing a Command File, 95
EGTT commands
EAGLE 5 ISS
rtrv-gta, 57, 62, 69
rtrv-gttsel, 57, 62, 69
rtrv-gttset, 57, 62, 69
EGTT Feature, 57
Entering an STP Name, 33
ent-ftp-serv EAGLE 5 ISS command, 53
Environment variable
FTRA_HOME, 2
JRE_HOME, 2
Error code
30 - Read-only file system, 133
32 - Broken pipe, 133
35 - Unsupported value, 133
40 - A destination address is required, 131
41 - Protocol wrong type for socket, 131
42 - The protocol is not available, 131
43 - The protocol is not supported, 131
44 - The socket type is not supported, 131
45 - The operation is not supported on the socket, 131
46 - The protocol family is not supported, 131
47 - The address family is not supported, 131
48 - The address is already in use, 131
49 - The requested address cannot be assigned, 131
50 - Socket operation on non-socket, 131
51 - The network is unreachable, 131
52 - The network dropped the connection on reset, 131
53 - Software caused the connection to abort, 131
54 - The connection was reset by the peer, 132
55 - No buffer space available, 132
56 - The socket is already connected, 132
57 - The socket is not connected, 132
58 - Can’t send after socket shutdown, 132
59 - Too many references: can’t splice, 132
595 - File open failed, 119
596 - The file name is already specified, 119
597 - SFTP client packet send failure, 119
598 - The SFTP connection is closed, 119
599 - SFTP packet read failure, 119
60 - The connection timed out, 132
600 - SFTP protocol error, 119
601 - Undefined, 120
608 - SFTP received a invalid ID in the response received during a read operation on remote directory, 120
609 - SFTP: Handle mismatch error, 120

61 - The connection was refused, 132
610 - Unexpected SSH2_FXP_ATTRS, 120
611 - Unexpected SSH_FXP_NAME, 120
612 - SSH_FXP_REALPATH request failure, 120
613 - SSH_FXP_READLINK request failure, 121
614 - unexpected SSH_FXP_NAME, 121
615 - The SFTP client received more data than expected, 121
616 - The SFTP client failed to read the data from the file descriptor, 121
617 - Excessive identity files, 121
62 - The network is down, 133
624 - The debug levels allowed for SSH protocol in openSSH is 0-9, 121
625 - Failure to read the client configuration file, 122
626 - Invalid compression level is specified in the client configuration file, 122
627 - SSH failure to setup the IO with the server, 122
628 - SSH failure to open the channel for the SSH connection with the server, 122
629 - SSH failure to setup the channel for the SSH connection with the server, 122
630 - SSH failure to verify the SSH client host key, 122
631 - SSH user authentication failure, 122
632 - The authentication method is NULL in the client software, 122
633 - Permission is denied by the server due to authentication failure, 123
633 - User login failure, 119
640 - A bad message was received during the SSH authentication, 123
641 - Missing authentication context, encountered during the SSH user authorization, 123
642 - Failure during the public key read/verification operation, 123
643 - Undefined SFTP/SSH error, 123
644 - Unexpected SSH_FXP_STATUS error, 124
645 - A bad option was specified in the SSH client on the EAGLE 5 ISS, 124
646 - An unsupported escape character was used in the SSH client on the EAGLE 5 ISS, 124
647 - An unsupported cipher type was used in the SSH client on the EAGLE 5 ISS, 124
648 - An unsupported MAC type was used in the SSH client on the EAGLE 5 ISS, 125
649 - A bad port was used in the SSH client on the EAGLE 5 ISS, 125
65 - There is no route to the host, 133
656 - Bad forwarding was used in the SSH client on the EAGLE 5 ISS, 125
657 - Bad forwarding ports were specified in the SSH client on the EAGLE 5 ISS, 125
658 - A bad dynamic port was specified in the SSH client on the EAGLE 5 ISS, 125
659 - The host was not specified in the SSH client on the EAGLE 5 ISS, 126
660 - An invalid option or argument was specified in the SSH client on the EAGLE 5 ISS, 126
661 - The hostname was not specified in the SSH client on the EAGLE 5 ISS, 126
663 - The SSH client was unable to load the cipher type on the EAGLE 5 ISS, 126
664 - Asynchronous IO is not supported on IPSM, SSH client error, 126
665 - Compression is already enabled in the SSH client on the EAGLE 5 ISS, 126
666 - Unknown cipher number on the SSH client on the EAGLE 5 ISS, 126
667 - The SSH client key length is invalid, 126
668 - No key is available on the SSH client on the EAGLE 5 ISS, 127
669 - The secure connection was closed by the remote server, 127
67 - The host is down, 133
670 - Connection failure due to network outage or the connection was lost due to a faulty SSHD/SFTP server or network, 127
671 - An unexpected packet type was received from the SFTP/SSHD server, 127
672 - A bad packet length was received from

the SSHD/SFTP server, 127
673 - A cryptographic attack was detected by the SSH client, 127
674 - The SSH/SFTP client on the EAGLE 5 ISS failed to read from the remote side, 128
675 - Corrupted check bytes were detected on the SSH/SFTP client on the EAGLE 5 ISS, 128
676 - Corrupted MAC on input was detected by the SSH/SFTP client on the EAGLE 5 ISS, 128
677 - Corrupted pad on input was detected by the SSH/SFTP client on the EAGLE 5 ISS, 128
678 - SSH/SFTP tried to close a connection that is already closed, 128
679 - The SSH/SFTP client on the EAGLE 5 ISS failed to write to the remote side, 129
680 - SSH/SFTP tried to set the packet size twice, 129
681 - A bad packet size was detected by the SSH/SFTP client on the EAGLE 5 ISS, 129
682 - The connection timed out when SSH tried to connect to SSHD, 130
683 - The SSH connection was refused by the remote server, 130
684 - The SSHD server is unreachable, 130
685 - The network has reset, 130
686 - The SSH/SFTP connection has been aborted, 130
687 - The SFTP/SSH connection has been reset by the peer, 130
688 - Failed to allocate network buffers, 130
689 - The SSH/SFTP socket is already connected, 130
690 - The SSH/SFTP socket is not connected, 130
691 - The network channel is down, 130
692 - The SSHD/SFTP server connection host is down, 130
693 - SFTP client channel read failure, 130
694 - SFTP client channel write failure, 130
695 - SFTP client channel open failure, 130
Error Codes
FTP, 118
Generic Network, 131
SFTP, 118
SSH, 118
Error message
STP Name does not exist, 34
Errors
SFTP, 119
SFTP Client, 119
SSH Client, 121
SSH/SFTP Connection/Setup, 130
Errors - contacting the Customer Care Center, 5, 49, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133
Excessive identity files - Error code 617, 121
Exit Confirmation window, 21
Exit menu, 20
Exit window, 21, 22
Exiting the FTRA application, 6, 21

F

Failed to allocate network buffers - Error code 688, 130
Failure during the public key read/verification operation - Error code 642, 123
Failure to read the client configuration file - Error code 625, 122
Feature
Eagle OA&M IP Security Enhancements, 5, 25, 29, 42, 118
EGTT, 57
FTP Retrieve and Replace, 5
GTT, 57
IP User Interface, 5
Field
Command File, Update Tables window, 89, 90, 92
Command List
Retrieve Tables, 59
Update Tables, 88
Current STP Selected:, 42
File Name:, 55
Select Starting Directory window, 55
Select window, 90
Files of type:
Select Starting Directory window, 55

Select window, 90
FTP Password, 24, 29
FTP UserName, 24, 29
IP Address, 53
Backup - FTRA 2.0 or greater, 24, 27, 28
Primary - FTRA 2.0 or greater, 24, 27, 28
Look in:
Select Staring Directory window, 55
Select window, 90
Path, 53
Selected Commands, Retrieve Tables, 59
STP Name, 6, 24, 26, 31, 33
STP name typed
FTRA 2.0, 33
STP Password, 24, 28
STP UserName, 24, 28
Subpath, 53
file extension
.doc, 39, 77, 105, 110
.txt, 39, 77, 105, 110
File format
CSV, 2, 57, 59, 68, 79, 85
File menu
Command File Editor window, 97
Connectivity Test Log, 36, 37
FTP-Based Table Retrieve Application window, 21
Retrieve Tables Log, 74
System Log, 107, 108
Update Tables Log, 102, 103
File Name: Field
Select Starting Directory window, 55
Select window, 90
File open failed - Error code 595, 119
Files of type: Field
Select Starting Directory window, 55
Select window, 90
Fingerprint
Key
DSA, 49, 50
Public Host Key
EAGLE 5 ISS, 46, 47, 49, 51
Public Key
EAGLE 5 ISS, 25, 49, 50
flag - strict host key, 47
FTP Error Codes, 118
FTP Password Field, 24, 29
FTP Retrieve and Replace Feature, 5
FTP server, 52, 134
secure, 52
FTP Server Configuration, 2, 6, 52
Menu, 20, 52
Browse button, 53, 54
Close button, 53
IP Address, 52, 134
IP Address Field, 53
Path Field, 53
Set button, 53, 55
Subpath Field, 53
Menu window, 29, 52, 53, 118, 120, 134, 135
FTP Server Data Set window, 56
FTP Server Verification procedure, 134
FTP UserName Field, 24, 29
FTP-Based Table Retrieve Application
Edit Menu, 23, 52, 88
File Menu, 21
Help Menu, 112
View Menu, 75, 103, 108
window, 20, 21, 26, 35, 40, 43, 61, 75, 76, 88, 103, 104, 105, 108, 109, 110, 112
File menu, 21
FTRA
Command
ftra -c, 79, 85
Initialization, 20
STP IP connection
secure, 25, 29
version level, 112
FTRA 2.0
Current STP Selected, 45
FTP Server, 52
Secure FTP Server, 52
STP Configuration Record, 33, 34
Adding, 26, 27, 28, 29, 30
STP Connection Configuration
Menu window, 52
STP Connection Configuration Menu
Backup IP Address, 24
Backup IP Address Field, 27, 28
IP Address
Backup, 24, 27, 28
Primary, 24, 27
Primary IP Address, 24

Primary IP Address Field, 28
Secure Connection Box, 25, 29, 42, 46, 51, 52
STP Name drop down list, 31, 32
STP name typed, 33
FTRA 2.x or greater - software
installing
Windows, 7
FTRA application
exiting, 6, 21
starting, 6
using, 6
ftra -c command, 79, 85
ftra file, 47
FTRA icon, 20
FTRA software
installing, 6
FTRA window
GTT Warning window, 57
Retrieve Tables, 6, 57, 58, 61, 79
description, 59
GTT Warning window, 57
Update Tables, 6, 87, 88, 89, 90, 91, 96, 97, 100, 101, 102
description, 88
Select, description, 90
Update Validation Complete, 92, 93, 94
Update Validation Complete with errors, 94
ftra.bat, 47
FTRA_HOME environment variable, 2

G

Generic Network Error Codes, 131
GPSM-II, 5
GTT commands
EAGLE 5 ISS
rtrv-gtt, 57, 62, 69
rtrv-tt, 57, 62, 69
GTT Feature, 57
GTT Warning window, 57

H

Help menu
FTP-Based Table Retrieve Application, 112
hexadecimal, 49
Host Key - Secure EAGLE 5 ISS Provisioning, 46
host key checking - strict, 47
Host Key Fingerprint
Public
EAGLE 5 ISS, 46, 47, 49, 51
host key flag - strict, 47
hosts.xml, 46, 47, 49, 50, 51

I

Icon, FTRA, 20
init-card command, 46, 49, 50
Initializing the FTRA, 20
Initializing window, 20
Installing
FTRA software, 6
Windows - FTRA 2.x or greater, 7
Invalid compression level is specified in the client configuration file - Error code 626, 122
Invalid FTP Password warning window, 29
Invalid FTP User Name warning window, 29
Invalid IP Address warning window, 27, 28, 53, 54
Invalid STP Name Error Message window, 26
Invalid STP Name warning window, 26
Invalid STP Password warning window, 28
Invalid STP User Name warning window, 28
IP Address, 24, 52, 134, 135, 136
Backup - FTRA 2.0, 27, 28
Backup - FTRA 2.0 or greater, 24
IPSM, 49, 50
Primary - FTRA 2.0, 27
Primary - FTRA 2.0 or greater, 24
IP address, 24
IP Address Field, 53
Backup - FTRA 2.0 or greater, 24, 27, 28
Primary - FTRA 2.0 or greater, 24, 27, 28
IP Address warning message, 46
IP connection
FTRA and STP
secure, 25, 29
IP User Interface Feature, 5
IPSM, 5, 46, 48, 49, 50, 135, 136
IPSM IP Address, 49, 50

J

JRE_HOME environment variable, 2

K

Key Fingerprint
DSA, 49, 50
Public
EAGLE 5 ISS, 25, 49, 50

L

Load button, 59, 68, 79
Log
Connectivity Test, 35, 36, 37, 38, 39
window, File Menu, 36, 37
Retrieve Tables, 20, 57, 70, 72, 74, 75, 76
window, File Menu, 74
System, 20, 107, 108, 109, 110, 111
closing, 107, 111
window, 107, 108, 109, 110, 111
File menu, 107, 108
Update Tables, 20, 87, 88, 91, 92, 93, 94, 97, 98, 99, 100, 101, 102, 103, 104, 105
window, 92, 98, 102, 103, 104, 105, 106
Commit Command Completed, 98
File Menu, 102, 103
Look in: Field
Select Starting Directory window, 55
Select window, 90

M

MCAP, 5
Menu
Commands, 20
Connectivity Test Log
File, 36
Edit
FTP-Based Table Retrieve Application, 23, 88
Exit, 20
File
Command File Editor window, 97
Connectivity Test Log window, 36, 37
FTP-Based Table Retrieve Application window, 21
Retrieve Tables Log window, 74
System Log window, 107, 108
Update Tables Log window, 102, 103
FTP Server Configuration, 20, 52
Browse button, 53, 54
Set button, 53
FTP-Based Table Retrieve Application, 52
Help
FTP-Based Table Retrieve Application, 112
Retrieve Tables Log
File, 74
STP Connection Configuration, 20, 23
View
FTP-Based Table Retrieve Application, 75, 103, 108
Message
Command In Progress, Cannot Close Window, 96
IP Address warning, 46
Must Enter Command Script File Name, 92
Processing Validate Request, Please Wait, 92, 98
Update Tables processing completed without errors, 97
Missing authentication context, encountered during the SSH user authorization - Error code 641, 123
Modify button, 24, 40, 41
Modify Warning window, 42
Modifying an Existing STP Configuration Record, 40, 46, 51
Must Enter Command Script File Name message, 92

N

netstat -a|grep 21, 134
Network latency, 137
No buffer space available - Error code 55, 132
No key is available on the SSH client on the EAGLE 5 ISS - Error code 668, 127

O

openSSH 3.0.2p1, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 134

P

Packet drop, 137
pass:loc=xxxx
  cmd="netstat -p tcp" EAGLE 5 ISS command, 136
  cmd="ping yy.yy.yy.yy" EAGLE 5 ISS command, 135
Path Field, 53
path parameter, 53
Permission is denied by the server due to authentication failure - Error code 633, 123
ping -s zz.zz.zz.zz command, 135
Primary IP Address - FTRA 2.0, 27
Primary IP Address - FTRA 2.0 or greater, 24
Primary IP Address Field - FTRA 2.0 or greater, 24, 27, 28
Print window
  Cancel button
    Update Tables Log, 104
  Connectivity Test Log, 37, 38
  Retrieve Tables Log, 76
  System Log, 109
  Update Tables Log, 104
Printing
  Connectivity Test Log, 36, 37
  Retrieve Tables Log, 74, 75
  System Log, 107, 109
  Update Tables Log, 102, 104
Problems - contacting the Customer Care Center, 5, 49, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133
Procedure
  Activating Controlled Features, 5
  Activating the Eagle OA&M IP Security Enhancements Controlled Feature, 5, 25, 29, 42, 118
  Connectivity Test - I, 134
  Connectivity Test - II, 135
  FTP Server Verification, 134
  SFTP Server Verification, 134
  SSHD Server Verification, 134
Processing Retrieve Request
  Update Tables Log window, 92
Processing Validate Request, Please Wait message, 92, 98
Protocol Troubleshooting, 137
Protocol wrong type for socket - Error code 41, 131
Provisioning the Secure EAGLE 5 ISS Host Key, 46
ps, 134
ps -ef|grep sshd, 118
ps -f|grep sshd, 134
Public Host Key Fingerprint
  EAGLE 5 ISS, 46, 47, 49, 51
Public Key Fingerprint
  EAGLE 5 ISS, 25, 49, 50

R

Read-only file system - Error code 30, 133
Record, STP configuration, 23
Refresh button, 24, 31, 32, 33, 42
release 30.2 or greater - EAGLE 5 ISS, 5, 25, 29
Release Not Compatible Error - Retrieve Tables Log window, 60
Remove button, 59, 66
Reset button, 59, 66
Retrieve button, 57, 59, 68, 69
Retrieve Database Tables from an STP, 57
Retrieve from Local Database button, 57, 59, 68
Retrieve from STP button, 57, 59, 69
Retrieve Tables
  Command List Box, 57, 59, 61, 66
  Selected Commands Box, 57, 59, 64, 66, 68
Retrieve Tables Log, 20, 57, 70, 72, 74, 75, 76
  Clearing the Display, 74
  closing, 74, 78
  File Menu, 74
  Print window, 76
  Printing, 74, 75
  Save window, 76, 77
  saved file confirmation window, 77
  saving to a file, 74, 76
Retrieve Tables Log window, 69, 71, 72, 74, 75, 76, 78
  File Menu, 74
  Processing Retrieve Request, 70
  Release Not Compatible Error, 60
  with Errors, 73
  with the RTRV-STP Command, 73
  without Errors, 72
Retrieve Tables window, 6, 57, 58, 61, 79
  Add button, 59, 64

Close button, 59
description, 59
GTT Warning window, 57
Load button, 59, 68, 79
Remove button, 59, 66
Reset button, 59, 66
Retrieve button, 57, 59, 68, 69
Retrieve from Local Database button, 57, 59, 68
Retrieve from STP button, 57, 59, 69
Store button, 59, 68, 79
Retrieving EAGLE 5 ISS database tables, 2, 6
rst-card command, 46
rtrv commands, 59, 79, 85
rtrv-card EAGLE 5 ISS command, 5
rtrv-ctrl-feat EAGLE 5 ISS command, 5, 25, 29, 42, 118
rtrv-feat EAGLE 5 ISS command, 57
rtrv-ftp-serv EAGLE 5 ISS command, 131
rtrv-gta EAGLE 5 ISS command, 57, 62, 69
rtrv-gtt EAGLE 5 ISS command, 57, 62, 69
rtrv-gttsel EAGLE 5 ISS command, 57, 62, 69
rtrv-gttset EAGLE 5 ISS command, 57, 62, 69
rtrv-ip-lnk command, 49, 50
rtrv-secu-dflt EAGLE 5 ISS command, 28
rtrv-stp EAGLE 5 ISS command, 72, 73
rtrv-trm command, 48, 49
rtrv-trm EAGLE 5 ISS command, 69
rtrv-tt EAGLE 5 ISS command, 57, 62, 69

S

Save button
Retrieve Tables Log
Save window, 77
System Log Save window, 111
Update Tables Log Save window, 105
Save window
Cancel button
System Log, 111
Update Tables Log, 106
Connectivity Test Log, 39
Retrieve Tables Log, 76, 77
System Log, 110, 111
Update Tables Log, 105, 106
Saved File Confirmation window
Connectivity Test Log, 39, 40
Retrieve Tables Log, 77
System Log, 111
Update Tables Log, 105, 106
Saving to a file
Connectivity Test Log, 36, 39
Retrieve Tables Log, 74, 76
System Log, 107, 110
Update Tables Log, 102, 105
secure connection, 5, 25, 46
Secure Connection Box - FTRA 2.0 or greater, 25, 29, 42, 46, 51, 52
Secure EAGLE 5 ISS Host Key Provisioning, 46
Secure FTP server, 52
Secure Host Key - EAGLE 5 ISS Provisioning, 46
secure IP connection between FTRA and STP, 25, 29
Security Administration, 49
Select button, 24, 32, 33
Select Starting Directory window, 55
Select window, 89, 90
Select Starting Directory window, 53, 54, 55
Cancel button, 55
Select button, 55
Select window
Cancel button, 89, 90
description, 90
Select button, 89, 90
Update Tables, 87, 88, 89, 90
Selected Commands
Box, 57, 59, 64, 66, 68
Adding a Command, 64
Adding a Range of Commands, 65
Adding Multiple Commands, 66
Command Selected Removed, 67
Command Selected to be Removed, 67
Field, Retrieve Tables window, 59
Selected STP, 2, 6, 44, 57, 59, 67, 68, 69, 87, 88, 93, 94, 95, 97
Sending a Command File, 94
Selecting
Command, 61
Current STP, 6, 43
Multiple Commands, 63
Range of Commands, 62
Sending a Command File to the Selected STP, 94
Sending EAGLE 5 ISS command files, 6

Server
FTP - FTRA 2.0, 52
FTP, Configuration, 6
Secure FTP - FTRA 2.0, 52
Set button, 55
FTP Server Configuration Menu, 53
SFTP client channel open failure - Error code 695, 130
SFTP client channel read failure - Error code 693, 130
SFTP client channel write failure - Error code 694, 130
SFTP Client Errors, 119
SFTP client packet send failure - Error code 597, 119
SFTP Connection Errors, 130
SFTP Error Codes, 118
SFTP Errors, 119
SFTP packet read failure - Error code 599, 119
SFTP protocol error - Error code 600, 119
SFTP received a invalid ID in the response received during a read operation on remote directory - Error code 608, 120
SFTP Server, 127, 130, 134
SFTP Server Verification procedure, 134
SFTP Setup Errors, 130
SFTP/SSH Error Codes, 118
SFTP: Handle mismatch error - Error code 609, 120
Shell command prompt, 79
Socket operation on non-socket - Error code 50, 131
Software
FTRA
Installing, 6
FTRA 2.x or greater
Installing
Windows, 7
Software caused the connection to abort - Error code 53, 131
SSH Client Errors, 121
SSH Connection Errors, 130
SSH Error Codes, 118
SSH failure to open the channel for the SSH connection with the server - Error code 628, 122
SSH failure to setup the channel for the SSH connection with the server - Error code 629, 122
SSH failure to setup the IO with the server - Error code 627, 122
SSH failure to verify the SSH client host key - Error code 630, 122
SSH Setup Errors, 130
SSH user authentication failure - Error code 631, 122
SSH, the Secure Shell: The Definitive Guide, 137
SSH/SFTP Error Codes, 118
SSH/SFTP tried to close a connection that is already closed - Error code 678, 128
SSH/SFTP tried to set the packet size twice - Error code 680, 129
SSH_FXP_READLINK request failure - Error code 613, 121
SSH_FXP_REALPATH request failure - Error code 612, 120
SSHD Server, 127, 130, 134
SSHD Server Verification procedure, 134
sshtools.xml, 128
Starting the FTRA application, 6
Stop button, Update Validation Complete window, 93
Stop on error box
Update Tables window, 88, 91, 100, 101, 102
Stop on error box Checked
Command File Selected
Update Tables window, 91
Stop Without Sending or Editing a Command File, 95
Store button, 59, 68, 79
STP
FTRA IP connection
secure, 25, 29
Retrieve Database Tables, 57
selecting current, 6
STP Added window, 30
STP Configuration Record, 23, 24, 26, 31, 32, 33, 34, 35, 40, 41, 42, 43, 44, 45, 46, 51
Adding, 26, 51
Deleting, 43
Displaying, 31
FTRA 2.0, 33, 34
Modifying, 40, 46, 51
testing, 35

STP Configuration Record - FTRA 2.0
Adding, 26, 27, 28, 29, 30
STP Connection Configuration, 2
Database, 23, 24, 25, 26, 30, 43
Menu, 20, 23
Menu window, 23, 24, 25, 26, 31, 33, 35, 40, 42, 43, 44, 119, 135, 136
FTRA 2.0, 52
FTRA 2.0 or greater, 23
STP Connection Configuration Menu
Add button, 2, 24, 26, 30
Close button, 25, 32, 33
Delete button, 24, 32, 33, 43
FTP Password Field, 24, 29
FTP UserName Field, 24, 29
IP Address, 135, 136
Backup - FTRA 2.0, 27, 28
Backup - FTRA 2.0 or greater, 24
Primary - FTRA 2.0, 27
Primary - FTRA 2.0 or greater, 24
IP Address Field
Backup - FTRA 2.0 or greater, 24, 27, 28
Primary - FTRA 2.0 or greater, 24, 27, 28
Modify button, 24, 40, 41
Refresh button, 24, 31, 32, 33, 42
Secure Connection Box - FTRA 2.0 or greater, 25, 29, 42, 46, 51, 52
Select button, 24, 33
STP Name drop down list, 24, 31
FTRA 2.0, 31, 32
STP Name Field, 6, 24, 26, 31, 33
STP name typed
FTRA 2.0, 33
STP Password Field, 24, 28
STP UserName Field, 24, 28
Test button, 24, 32, 33, 35
Use STP and FTP UserNames, Passwords for all STPs Box, 25, 26, 40, 41
STP Connectivity Test, 2
STP Data Modified window, 41, 42
STP Name, 24, 25, 26, 30, 31, 32, 33, 34, 40, 43, 44, 45
entering, 33
STP Name does not exist error message, 34
STP Name drop down list, 24, 31
FTRA 2.0, 31, 32
STP Name Field, 6, 24, 26, 31, 33
STP name typed
FTRA 2.0, 33
STP Password Field, 24, 28
STP Selection Change window, 24, 44, 45
STP UserName Field, 24, 28
strict host key checking, 47
strict host key flag, 47
Subpath Field, 53
Support - contacting the Customer Care Center, 5, 49, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133
System Log, 20, 107, 108, 109, 110, 111
Clearing the Display, 107, 108
closing, 107, 111
Print window, 109
Printing, 107, 109
Save window, 110, 111
saved file confirmation window, 111
saving to a file, 107, 110
System Log window, 107, 108, 109, 110, 111
Cancel button, 109
File menu, 107, 108

T

Task Scheduler
Windows, 79, 85
TCP Out of Order, 137
TCP Packet Delay, 137
TCP Packet Error, 137
TCP Packet Errors, 137
TCP Packet Loss, 137
TDM, 5
Technical Assistance - contacting the Customer Care Center, 5, 49, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133
telnet server, 46
Telnet terminals, 24, 49, 69
Terminals
EAGLE 5 ISS
Telnet, 24, 49, 69
Test button, 24, 32, 33, 35
Testing an STP Configuration Record, 35
The address family is not supported - Error code 47, 131

The address is already in use - Error code 48, 131
The authentication method is NULL in the client software - Error code 632, 122
The connection timed out - Error code 60, 132
The connection timed out when SSH tried to connect to SSHD - Error code 682, 130
The connection was refused - Error code 61, 132
The connection was reset by the peer - Error code 54, 132
The debug levels allowed for SSH protocol in openSSH is 0-9 - Error code 624, 121
The file name is already specified - Error code 596, 119
The host is down - Error code 67, 133
The host was not specified in the SSH client on the EAGLE 5 ISS - Error code 659, 126
The hostname was not specified in the SSH client on the EAGLE 5 ISS - Error code 661, 126
The network channel is down - Error code 691, 130
The network dropped the connection on reset - Error code 52, 131
The network has reset - Error code 685, 130
The network is down - Error code 62, 133
The network is unreachable - Error code 51, 131
The operation is not supported on the socket - Error code 45, 131
The protocol family is not supported - Error code 46, 131
The protocol is not available - Error code 42, 131
The protocol is not supported - Error code 43l, 131
The requested address cannot be assigned - Error code 49, 131
The secure connection was closed by the remote server - Error code 669, 127
The SFTP client failed to read the data from the file descriptor - Error code 616, 121
The SFTP client received more data than expected - Error code 615, 121
The SFTP connection is closed - Error code 598, 119
The SFTP/SSH connection has been reset by the peer - Error code 687, 130
The socket is already connected - Error code 56, 132
The socket is not connected - Error code 57, 132
The socket type is not supported - Error code 44, 131
The SSH client key length is invalid - Error code 667, 126
The SSH client was unable to load the cipher type on the EAGLE 5 ISS - Error code 663, 126
The SSH connection was refused by the remote server - Error code 683, 130
The SSH/SFTP client on the EAGLE 5 ISS failed to read from the remote side - Error code 674, 128
The SSH/SFTP client on the EAGLE 5 ISS failed to write to the remote side - Error code 679, 129
The SSH/SFTP connection has been aborted - Error code 686, 130
The SSH/SFTP socket is already connected - Error code 689, 130
The SSH/SFTP socket is not connected - Error code 690, 130
The SSHD server is unreachable - Error code 684, 130
The SSHD/SFTP server connection host is down - Error code 692, 130
There is no route to the host - Error code 65, 133
Too many references: can’t splice - Error code 59, 132
Troubleshooting Procedures, 134

U

UIM - Unsolicited Information Message EAGLE 5 ISS, 49, 50, 69
UIM 1493, 49, 50
UIM 1494, 49, 50
Undefined - Error code 601, 120
Undefined SFTP/SSH error - Error code 643, 123
Unexpected SSH_FXP_NAME - Error code 611, 120
unexpected SSH_FXP_NAME - Error code 614, 121
Unexpected SSH_FXP_STATUS error - Error

code 644, 124
Unexpected SSH2_FXP_ATTRS - Error code 610, 120
Unknown cipher number on the SSH client on the EAGLE 5 ISS - Error code 666, 126
Unsupported value - Error code 35, 133
Update Tables Log, 20, 87, 88, 91, 92, 93, 94, 97, 98, 99, 100, 101, 102, 103, 104, 105
Clearing the Display, 102, 103
closing, 102, 106
Print window, 104
Printing, 102, 104
Save window, 105, 106
saved file confirmation window, 105, 106
saving to a file, 102, 105
Update Tables Log window, 92, 98, 102, 103, 104, 105, 106
Commit Command Completed, 98
File Menu, 102
File menu, 102, 103
Processing Retrieve Request, 92
Update Tables processing completed without errors message, 97
Update Tables window, 6, 87, 88, 89, 90, 91, 96, 97, 100, 101, 102
Browse button, 88, 89
Close button, 88
Command File field, 89, 90, 92
Command File Selected
Stop on error box Checked, 91
description, 88
Select window, description, 90
Update Validation Complete Window
Update Tables
Update Validation Complete, 92, 93, 94
Update Validation Complete window, 87, 93, 95, 96
with errors Window
Update Tables
Update Validation Complete with errors, 94
Validate button, 87, 88, 92
Update Validation Complete window, 87, 92, 93, 94, 95, 96
description, 93
with errors, 94
without errors, 94
Updating Database Tables in the Selected STP, 87
Use STP and FTP UserNames, Passwords for all STPs Box, 25, 26, 40, 41
User Guide Conventions, 2
User login failure - Error code 633, 119
Using the FTRA application, 6

V

Validate button
Update Tables, 88, 92
Update Tables window, 87
Validating command files, 3
Variable
environment
FTRA_HOME, 2
JRE_HOME, 2
Version level, 112
View menu
FTP-Based Table Retrieve Application, 75, 103, 108
Viewing log files, 3

W

Window
About FTRA, 20, 112
Command Complete Connectivity Test, 36
Command File Editor, 93, 95, 96, 97
File Menu, 97
Invalid Command, 96
Command File Editor window
File Menu, 97
Commands Menu, 59, 68, 88
Connectivity Test Log, 35, 36, 37, 39, 40, 47, 50, 51
closing, 36, 40
File Menu, 36, 37
Print, 37, 38
Save, 39
Saved file confirmation, 39, 40
with errors, 36
with no errors, 35
Exit, 21, 22
Exit Confirmation, 21
FTP Server Configuration Menu, 29, 52, 53, 118, 120, 134, 135

FTP Server Data Set, 56
FTP-Based Table Retrieve Application, 20, 21, 26, 35, 40, 43, 61, 75, 76, 88, 103, 104, 105, 108, 109, 110, 112
GTT Warning, 57
Initializing, 20
Invalid FTP Password warning, 29
Invalid FTP User Name warning, 29
Invalid IP Address warning, 27, 28, 53, 54
Invalid STP Name Error Message, 26
Invalid STP Name warning, 26
Invalid STP Password warning, 28
Invalid STP User Name warning, 28
Modify Warning, 42
Print
  Retrieve Tables Log, 76
  Update Tables Log, 104
Retrieve Tables, 6, 57, 58, 61, 79
  Add button, 59, 64
  Close button, 59
  Command Complete, 57, 70, 71
  Command List Field, 59
  description, 59
  GTT Warning, 57
  Load button, 59, 68, 79
  Remove button, 59, 66
  Reset button, 59, 66
  Retrieve button, 57, 59, 68, 69
  Retrieve from Local Database button, 57, 59, 68
  Retrieve from STP button, 57, 59, 69
  Selected Commands Field, 59
  Store button, 59, 68, 79
Retrieve Tables Log, 69, 71, 72, 74, 75, 76, 78
  closing, 74, 78
  File Menu, 74
  Print, 76
  Processing Retrieve Request, 70
  Release Not Compatible Error, 60
  Save, 76, 77
  Saved file confirmation, 77
  with Errors, 73
  with the RTRV-STP Command, 73
  without Errors, 72
Save
  Retrieve Tables window, 77
Select
  File Name: Field, 90
  Files of type: Field, 90
  Look in: Field, 90
  Update Tables, 87, 88, 89, 90
Select Starting Directory, 53, 54, 55
  File Name: Field, 55
  Files of type: Field, 55
  Look in: Field, 55
Select, description, 90
STP Added, 30
STP Connection Configuration Menu, 23, 24, 25, 26, 31, 33, 35, 40, 42, 43, 44, 119, 135, 136
  FTRA 2.0, 52
  FTRA 2.0 or greater, 23
STP Data Deleted, 43
STP Data Modified, 41, 42
STP Selection Change, 24, 44, 45
System Log, 107, 108, 109, 110, 111
  closing, 107, 111
  File Menu, 107, 108
  Print, 109
  Print window
    Cancel button, 109
  Save, 110, 111
  Saved file confirmation, 111
Update Tables, 6, 87, 88, 89, 90, 91, 96, 97, 100, 101, 102
  Browse button, 88, 89
  Close button, 88
  Command Complete, 93, 94, 97
  Command File field, 89, 90, 92
  Command List Field, 88
  description, 88
  Select, description, 90
  Stop on error box, 88, 91, 100, 101, 102
  Update Validation Complete, 93
  Validate button, 87, 88, 92
Update Tables Log, 92, 98, 102, 103, 104, 105, 106
  closing, 102, 106
  Commit Command Completed, 98
  File Menu, 102, 103
  Print, 104
  Processing Retrieve Request, 92
  Save, 105, 106
  Saved file confirmation, 105, 106
Update Validation Complete, 87, 92, 93,

94, 95, 96
Commit button, 93, 94
description, 93
Edit button, 93, 94, 95, 96
Stop button, 93
with errors, 94
without errors, 94
Windows Explorer, 7
Windows Task Scheduler, 79, 85