# Tekelec Signaling Products FTP-Based Table Retrieve Application (FTRA) User Guide

## Table of Chapters




**910-0008 Rev A, March 2005**

# Tekelec Signaling Products

# FTP-Based Table Retrieve Application (FTRA) User Guide

910-0008 Revision A
March 2005

TEKELEC

**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.

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.

**Trademarks**
The Tekelec logo and Eagle are registered trademarks of Tekelec, Inc.

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.

Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States of America and/or other countries.

**Ordering Information**
Additional copies of this document can be ordered from Tekelec Network Signaling Group, 5200 Paramount Parkway, Morrisville, North Carolina, 27560.

# Table of Contents

# List of Figures

# List of Tables

# List of Acronyms

| | |
|---|---|
| CD | Compact Disc |
| CDE | Common Desktop Environment |
| CSV | Comma Separated Value |
| DOS | Disk Operating System |
| FTP | File Transfer Protocol |
| FTRA | FTP-Based Table Retrieve Application |
| GPSM | General Purpose Service Module |
| IP | Internet Protocol |
| IPSM | IP Services Module |
| JRE | Java™ 2 Runtime Environment |
| LAN | Local Area Network |
| MB | Megabyte |
| PC | Personal Computer |
| RAM | Random Access Memory |
| ROM | Read-only Memory |
| 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 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 STP's. Database tables can be retrieved from the Eagle STP, using the Eagle STP's retrieve commands. The output of these retrieve commands is converted to CSV (comma separated value) files. Eagle STP 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 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.

- Validation of the command files before being sent to the STP.
- 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 a Windows or Unix platform is required.

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

- Operating system – Windows® 98 or later
- Processor speed – Pentium III, 750 MHz or faster
- RAM – Minimum 128 MB
- Disk space – Minimum 500 MB plus 500 MB for each configured STP
- A CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java™ 2 Runtime Environment (JRE) 1.4.0 or later.

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

- Operating system – Solaris 7 or later
- Processor speed – 500 MHz or faster
- RAM – Minimum 512 MB
- Disk space – Minimum 500 MB plus 500 MB for each configured STP
- CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java™ 2 Runtime Environment (JRE) 1.4.0 or later

To configure the Eagle 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 **`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 **`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 is running release 30.2 or greater, and you wish to use a secure connection for the FTRA to Eagle 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. 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 **`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.

**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 system currently has MCAP cards installed) in card locations 1113 or 1115, or replacing TDMs in card locations 1114 and 1116, contact Tekelec Technical Services at one of the following locations:**

- Tekelec, UK

  Phone: +44 1784 467 804.

- Tekelec, USA

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

Or you can request assistance by way of electronic mail at **`eaglets@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) – see the "Software Installation" section on page 4.

2. Start the FTRA application – see the "FTRA Initialization" section on page 11.

3. Select the current STP that the database tables will be retrieved from, or that the command files will be sent to – go to the "Selecting the Current STP" procedure on page 40.

   If you wish to use another STP, and that STP is not shown in the STP Name field of the **STP Connection Configuration** window, go to the "Adding an STP Configuration Record" procedure on page 18 and add the new STP.

4. Before database tables can be retrieved from the Eagle, or command files can be sent to the Eagle, the FTP server configuration information for that Eagle must be configured – see the "FTP Server Configuration" section on page 49.

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 – see the "Retrieve Database Tables from an STP" section on page 54.

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 – see the "Updating Database Tables in the Selected STP" section on page 77.

7. Exit the FTRA application – see the "Exit the FTRA" section on page 12.

## 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.

If the Java™ 2 Runtime Environment software has not been installed, you can install the Java™ 2 Runtime Environment software from the 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 Java™ 2 Runtime Environment 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 recreate directories or environment variables that already exist.

If problems are encountered while installing the FTRA software, contact Tekelec Technical Services. See page 3 for the contact information.

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

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

If the FTRA software is being upgraded from FTRA 1.0 to FTRA 2.x or greater, perform one of these procedures:

- "Upgrade to FTRA 2.x or Greater on Windows" on page 9
- "Upgrade to FTRA 2.x or Greater on Unix" on page 9

**Procedure – FTRA Software Installation on Windows**

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

2. Install the Java™ 2 Runtime Environment SE V1.4.0 from the CD. Right-click on the **My Computer** icon on the desktop and select **Explore**. Select the CD-ROM drive. From Windows Explorer, double-click on the **j2re-1_4_0_01_windows-i586-l** icon and follow the InstallShield Wizard instructions.

3. Create a folder that the FTRA software will be installed into (the <*base_directory*>). The folder `C:\ftra` is recommended and used in the examples for this procedure, but you may place it wherever you would prefer.

   **NOTE: The path to this directory and the name of the directory cannot contain any blank spaces.**

   To create the <*base_directory*>, select the location of the <*base_directory*> from Windows Explorer. Select **File > New > Folder** and rename the new folder with the desired folder name.

   For example, if the <*base_directory*> is to be `C:\ftra`, in Windows Explorer, select **C: Drive**. Select **File > New > Folder** and rename it `ftra`.

**4.** Extract the FTRA program files from the FTRA CD.

If you are installing FTRA 1.0, in the <*base_directory*>, create a folder named **`bin`**. From Windows Explorer, select the new <*base_directory*> (for example, **`C:\ftra`**). Select **File>New>Folder** and rename it to **`bin`**. Copy the file **`ftra_install.exe`** from the FTRA CD to the new **`\bin`** folder (for example, **`C:\ftra\bin`**). From Windows Explorer, double-click on the **`ftra_install.exe`** file. This will extract the program files into the new **`\bin`** folder created in this step.

For FTRA 2.x or greater, copy the **`ftra_install.exe`** file from the FTRA CD to the <*base_directory*>. The FTRA files can be extracted from the new directory (for example, **`C:\ftra`**). This can be done in one of two ways.

**NOTE: Extract the FTRA file from the <*base_directory*> using only the command prompt. Do not use a Windows Explorer window for the extraction.**

**a.** From the Windows command line, the **MS-DOS** prompt, enter the command **`ftra_install -d`**.

**b.** From the **Start** menu, select **Start > Run** and enter the path to the <*base_directory*> and the **`ftra_install -d`** command. For example, enter **`C:\ftra\ftra_install -d`**.

The **`ftra_install -d`** command creates all the required directories and extracts the program files.

---

**5.** Set the required system/user environment variables.

**`FTRA_HOME = C:\`**<*base_directory*> (typically, **`C:\ftra`**)

**`JRE_HOME = C:\Program Files\Java\j2re1.4.0_01`**
(typically, the folder where Java is installed)

**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.**

The method for defining environment variables differs between Windows systems.

**a. Windows 2000 operating system** – Right-click the **My Computer** icon on the desktop and select **Properties**. In the **Advanced** tab, click **Environment Variables…**
Click **New…** under User variables, and enter the variable name and value.

**b. Windows NT® operating system** – Right-click the My Computer icon on the desktop and select **Properties**. In the **Environment** tab, select any

user environment variable, enter the new variable name and value, and click **Set**.

c. **Windows 98 operating system** – Using a text editor (such as Notepad) append the following lines to the AUTOEXEC.BAT file:
```
SET FTRA_HOME="C:\<base_directory>"
SET JRE_HOME="C:\Program Files\Java\j2re1.4.0_01"
```

---

6. Create a shortcut from the **C:\<*base_directory*>\bin\ftra.bat** file to the desktop by right clicking on the **ftra.bat** icon and dragging it to the desktop.

   **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 V1.4.0 software either from the FTRA CD or download the Java™ 2 Runtime Environment, SE V1.4.0 software from Sun Microsystems' web site.

   a. To install the Java™ 2 Runtime Environment, SE V1.4.0 software from the FTRA CD, open **FileManager** and go to the CDROM drive. From **FileManager**, double-click on the `j2re-1_4_1_01-solaris-sparc.sh` file and follow the installation instructions in the "Java™ 2 Runtime Environment Installation" procedure on page 8.

   b. To install the Java™ 2 Runtime Environment (JRE) 1.4.0 from Sun Microsystem's web site, enter this 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*> to install the FTRA software into. The preferred location to install the FTRA software into is `<HOME_DIRECTORY>/ftra`, but you may place it wherever you would prefer. Open **FileManager** and go to the preferred 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:

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

   **setenv JRE_HOME '**<*jre_install_directory*>**'**

**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_0_01-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_0_01-solsparc.sh
   ```

   This will create a directory called **j2re1_4_0_01**.

5. Make a symbolic link to this directory called **/usr/java** by entering this command.

   ```
   Shell> ln -s j2re1_4_0_01 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 this command, **rm java**.

**Procedure – Upgrade to FTRA 2.x or Greater 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 step 3 on page 5.

3. Extract the FTRA program files from the FTRA CD using only the command prompt. Do not use a Windows Explorer window for the extraction. 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 **`yes`** for the upgrade to continue. When the **`ftra_install -d`** command has finished executing, the FTRA software has been installed.

4. Start the FTRA software. See the "FTRA Initialization" section on page 11 for more information on starting the FTRA software. The existing STP Connection Configuration data will automatically be converted during the FTRA system initialization.

**Procedure – Upgrade to FTRA 2.x or Greater 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 step 3 on page 7.

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`**. This will create the sub-directories and extract the program files into the existing directory containing the FTRA software.

   **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 software has been installed.

---

4. Start the FTRA software. See the "FTRA Initialization" section on page 11 for more information on starting the FTRA software. The existing 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 1. The **Initializing** window opens and displays the message "Initializing, please wait……" until the initialization process has been completed.

**Figure 1.** 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:<br>• The Retrieve Tables Log<br>• The Update Tables Log<br>• The System Log. |
| Help | Selects the **About FTRA** window. |

## Exit the FTRA

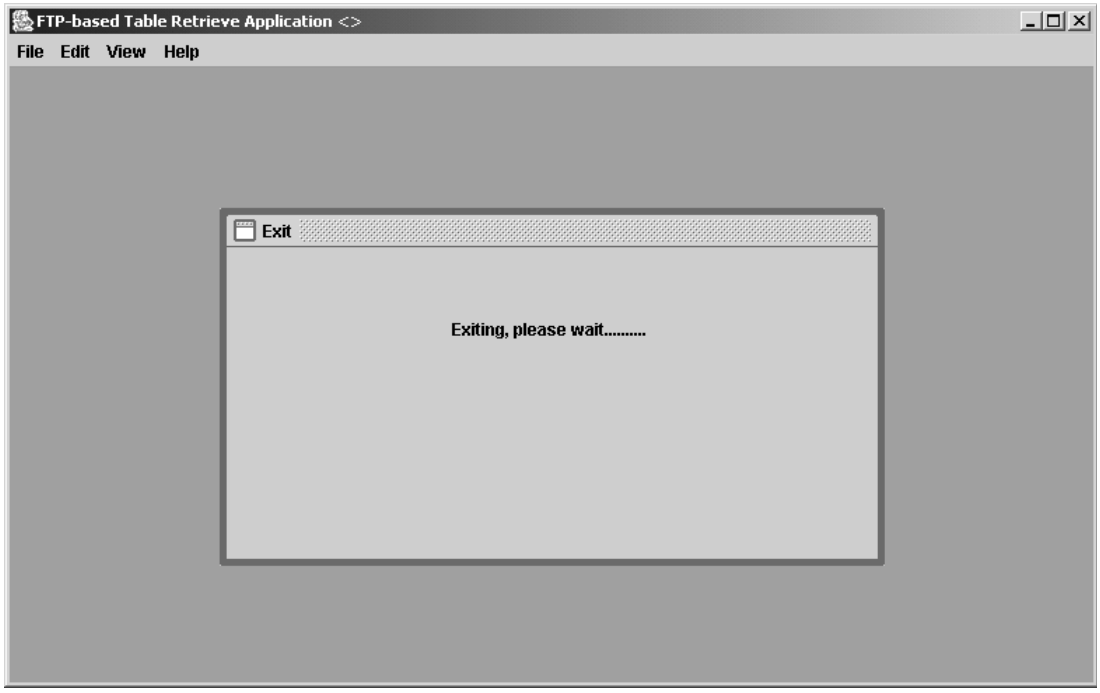
To close the **FTP-Based Table Retrieve Application** window and exit the FTRA, either select **File > Exit** from the **File** menu, see Figure 2, or click the close window button in the upper right hand corner of the window.

**Figure 2.** File Menu in the FTP-Based Table Retrieve Application Window


The **Exit?** confirmation window (see Figure 3) opens with "You are about to exit. Continue?" Click **OK** to exit and close the application. The **Exit** window (see Figure 4 on page 13) is displayed until the Exit process is completed. To cancel the exit and resume using the application, click **Cancel**.

**Figure 3.** Exit Confirmation Window

**Figure 4.** 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 5.

**Figure 5.** Edit Menu


The **STP Connection Configuration Menu** window, see Figure 6 (FTRA 1.0) or Figure 7 on page 15 (FTRA 2.0 or greater), can be used also to delete and modify an STP configuration record.

**Figure 6.** STP Connection Configuration Menu Window (FTRA 1.0)

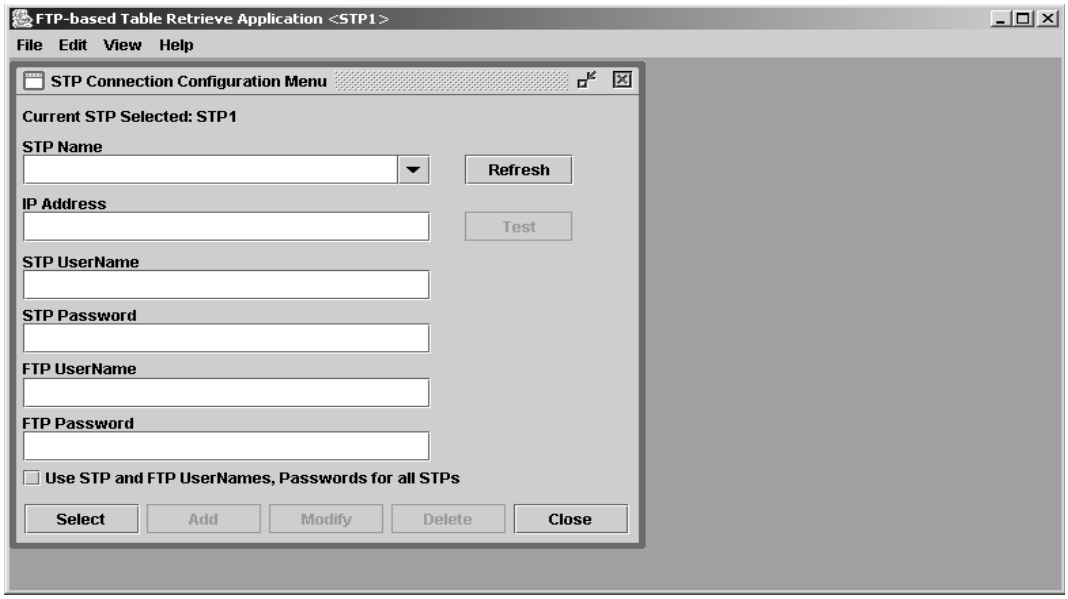


**Figure 7.** STP Connection Configuration Menu Window (FTRA 2.0 or greater)

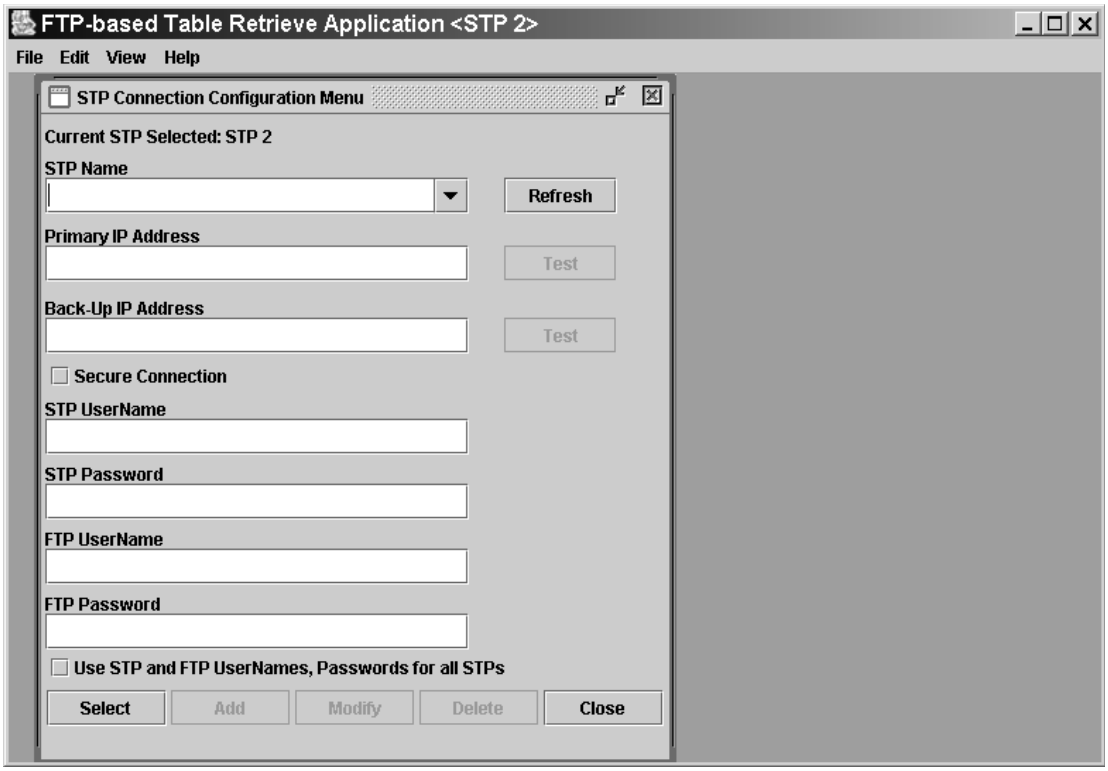



Table 2 on page 15 shows the description of the fields, buttons, and boxes in the **STP Connection Configuration Menu** window.

**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.<br>This field also provides a drop down list for selecting stored STP configuration records. |
| IP Address (FTRA 1.0 only) | The IP address of the associated STP (used for telnet sessions). The IP address is the IP address of an IPSM in the associated Eagle. |
| Primary IP Address (FTRA 2.0 or greater) | 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. |

**Table 2.** STP Connection Configuration Menu Description

| Item | Description |
|---|---|
| Backup IP Address (FTRA 2.0 or greater) | 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. |
| 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 through an available telnet terminal at the specified IP address.<br>For FTRA 1.0, the STP Connection Configuration Menu window has only one **Test** button.<br>For FTRA 2.0 or greater, 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. |
| Close | Closes the **STP Connection Configuration Menu** window. |

**Table 2.** STP Connection Configuration Menu Description

| Item | Description |
|---|---|
| **Boxes** | |
| Secure Connection (FTRA 2.0 or greater) | Enables the FTRA to use a secure IP connection to the STP.<br>To use a secure connection for the FTRA to Eagle communication, make sure the Eagle 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. 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.<br>**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.**<br>If this box is checked, the public key fingerprint for the Eagle STP specified in this window must be installed onto the FTRA for the FTRA and the specified Eagle STP 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 Host Key Provisioning" procedure on page 43. |
| 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 5 on page 14. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 14. 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). See Figure 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater). 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 8. 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 23.**

   **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 36 to change an existing STP configuration record.**

**Figure 8.** Invalid STP Name Error Message

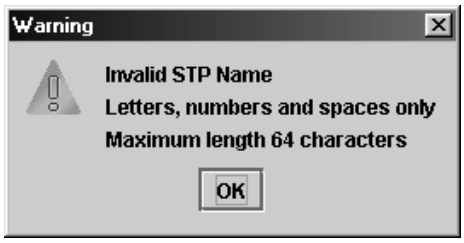


**Figure 9.** Adding an STP Configuration Record (FTRA 1.0)

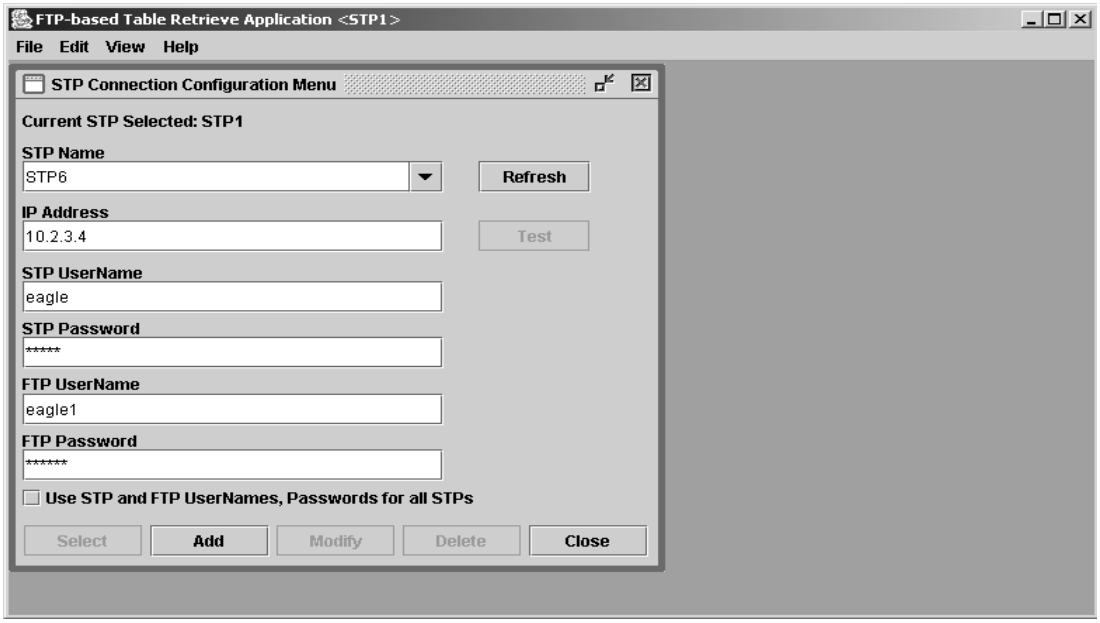
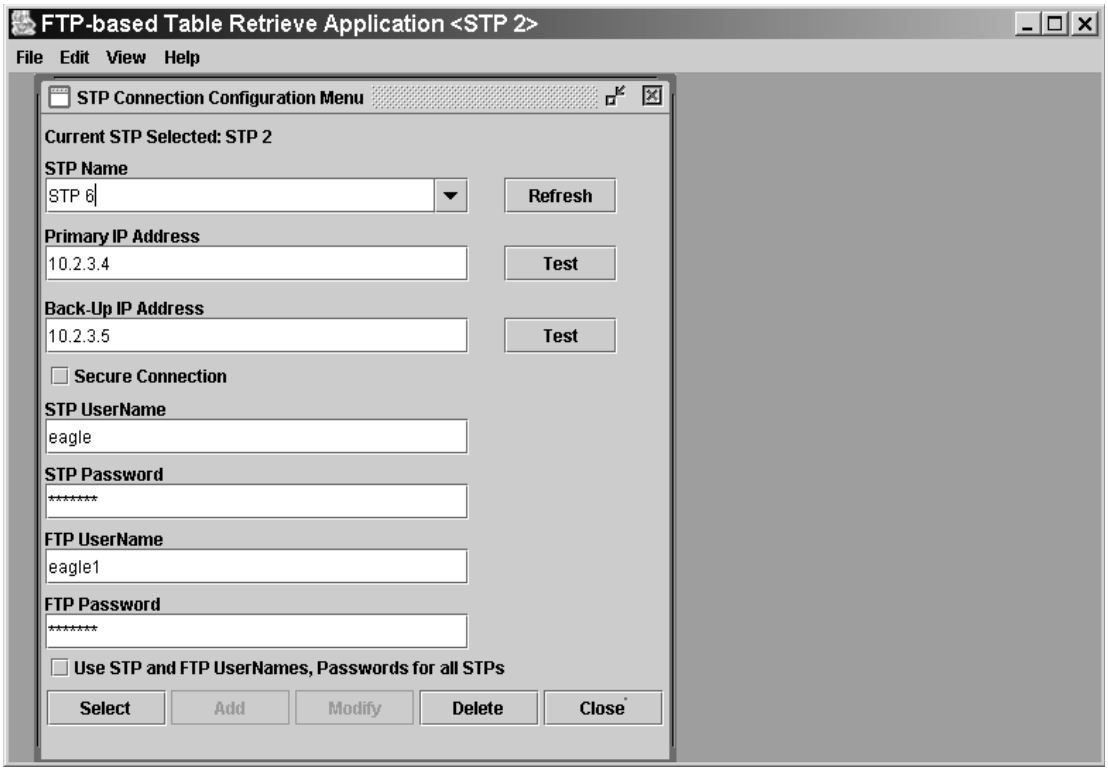



**Figure 10.** Adding an STP Configuration Record (FTRA 2.0 or greater)



3. Enter the IP address of the STP in the **IP Address** field (FTRA 1.0). If the FTRA is running version 2.0 or greater, enter the IP address you wish to use to connect to the STP in the **Primary IP Address** field, and a backup IP address in the **Backup IP Address** field. See Figure 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater).

**CAUTION: If the backup IP address is not entered for FTRAs running 2.0 or greater, 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 format of the IP address (FTRA 1.0), or the primary and backup IP addresses (FTRA 2.0 or greater) is not entered correctly, the **Invalid IP Address** warning window is displayed. See Figure 11. If the **Invalid IP Address** window appears, click **OK**, and reenter the IP address in the **IP Address** field (FTRA 1.0) or the primary or backup IP addresses (FTRA 2.0 or greater) in the **Primary IP Address** or **Backup IP Address** fields in the correct format.

**Figure 11.** 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 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater). If the format of the STP user name is not correct, the **Invalid STP User Name** warning window is displayed. See Figure 12. If the **Invalid STP User Name** window appears, click **OK**, and re-enter the STP user name in the **STP UserName** field.

**Figure 12.** 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 system administrator for telnet sessions. See Figure 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater). If the format of the STP password is not correct, the **Invalid STP Password** warning window is displayed. See Figure 13. 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 passwords. The passwords are validated by the Eagle when the FTRA attempts a connection to the Eagle. The requirements for the format of Eagle passwords is shown in the output of the Eagle's `rtrv-secu-dflt` command.**

   **Figure 13.** Invalid STP Password Error Message


6. Enter the FTP user name assigned by the FTP server administrator in the **FTP UserName** field. See Figure 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater). 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 14. 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 43 on page 50), must allow FTPs to the IP address specified in the FTP Server Configuration Menu window.**

   **Figure 14.** Invalid FTP User Name Error Message

7. Enter the FTP password assigned by the FTP server administrator in the **FTP Password** field. See Figure 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater). If the format of the STP user name is not correct, the **Invalid FTP Password** warning window is displayed. See Figure 15. If the **Invalid FTP Password** window appears, click **OK**, and re-enter the FTP password in the **FTP Password** field.

   **Figure 15.** Invalid FTP Password Error Message


---

**NOTE: If you are running FTRA 1.0, or running FTRA 2.0 or greater 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 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. 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 9 on page 19 (FTRA 1.0) or Figure 10 on page 19 (FTRA 2.0 or greater). The newly entered STP Name and associated data is added to the STP Connection Configuration database, and the **STP Added** window (Figure 16) is displayed. Click **OK** to continue.

   **Figure 16.** STP Added Window


---

10. Verify the addition of the new STP name. See the "Displaying an Existing STP Configuration Record" procedure on page 23.

---

## 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 17 (FTRA 1.0) or Figure 18 on page 24 (FTRA 2.0 or greater).

**Figure 17.** Selecting an STP Name from the STP Name Drop Down List (FTRA 1.0)

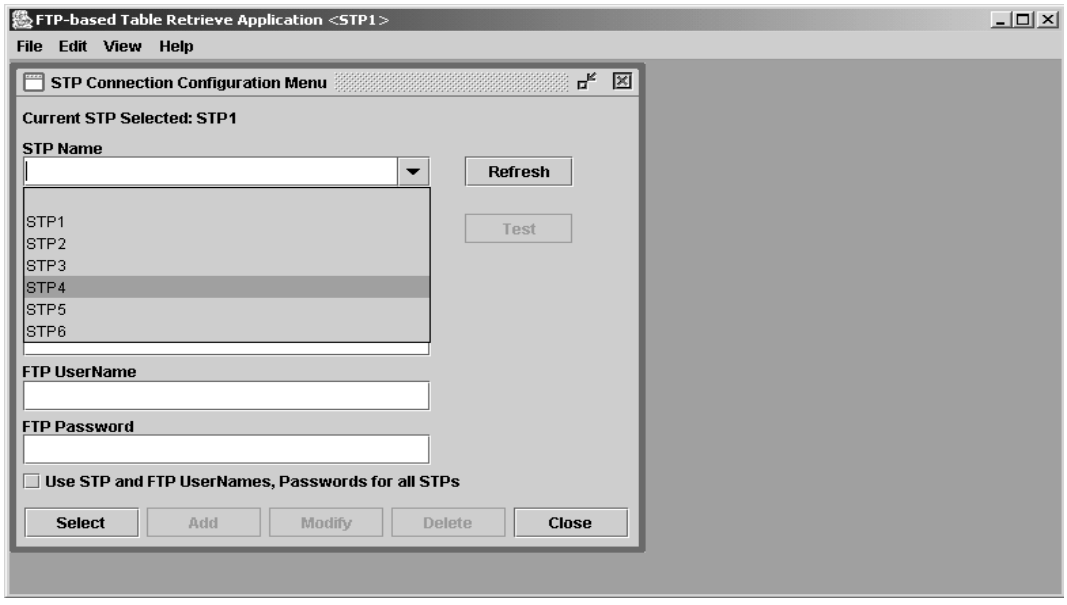
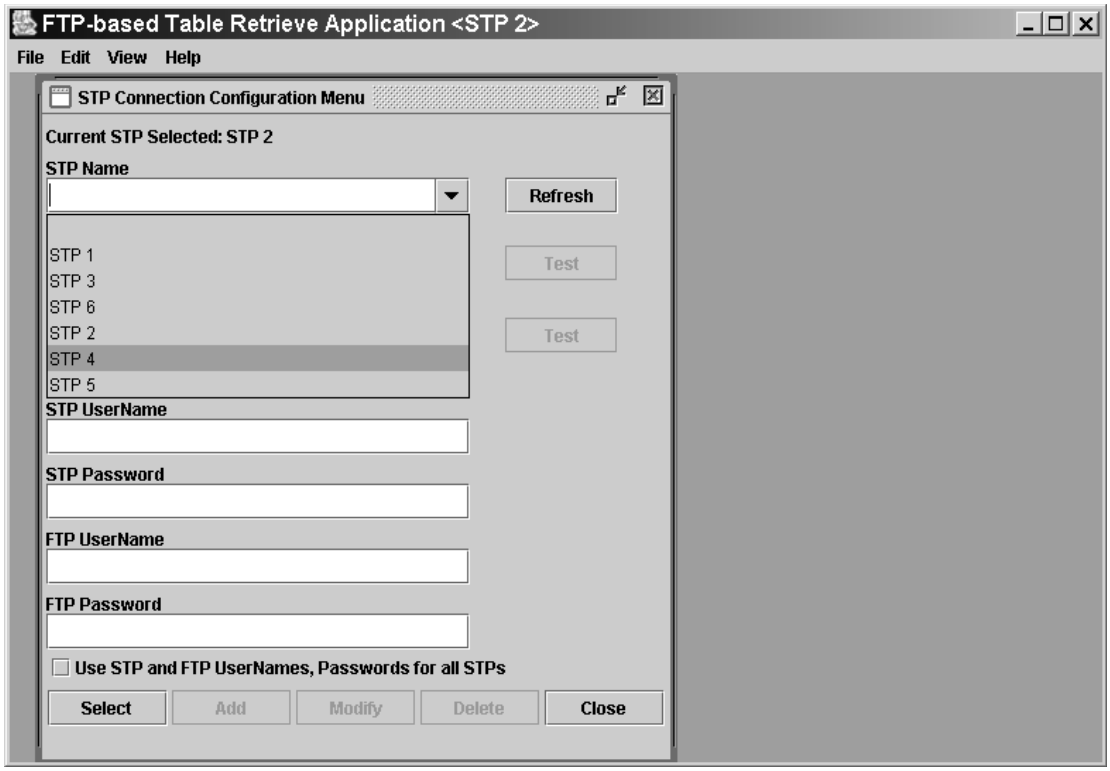


**Figure 18.** Selecting an STP Name from the STP Name Drop Down List (FTRA 2.0 or greater)



2. When the STP name is selected in step 1, the STP configuration record for the specified STP is displayed. See Figure 19 (FTRA 1.0) or Figure 20 on page 26 (FTRA 2.0 or greater). The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

**Figure 19.** STP Name Selected from the STP Name Drop Down List (FTRA 1.0)

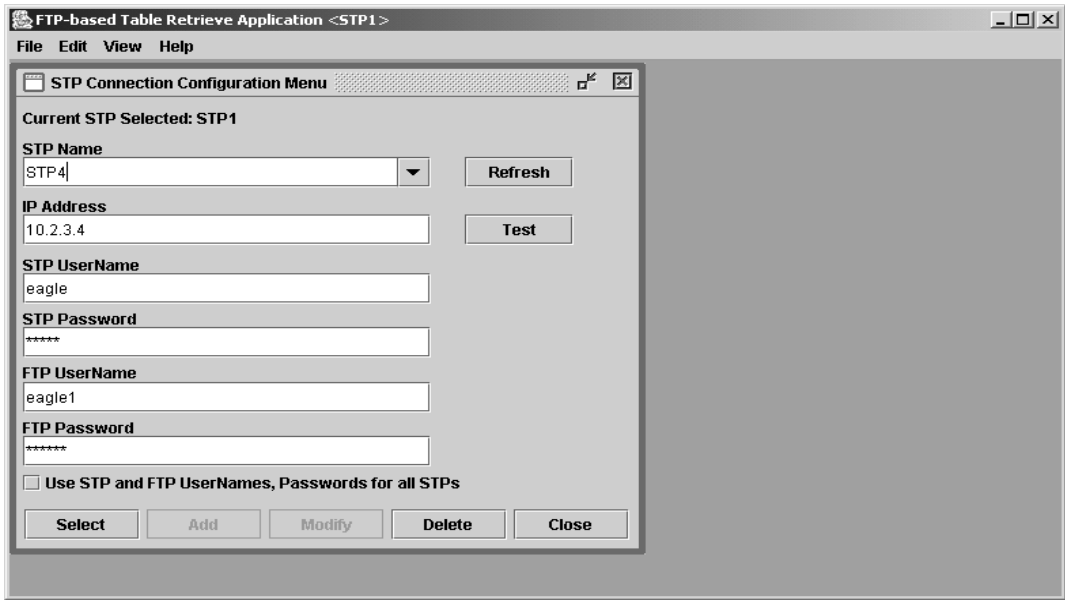
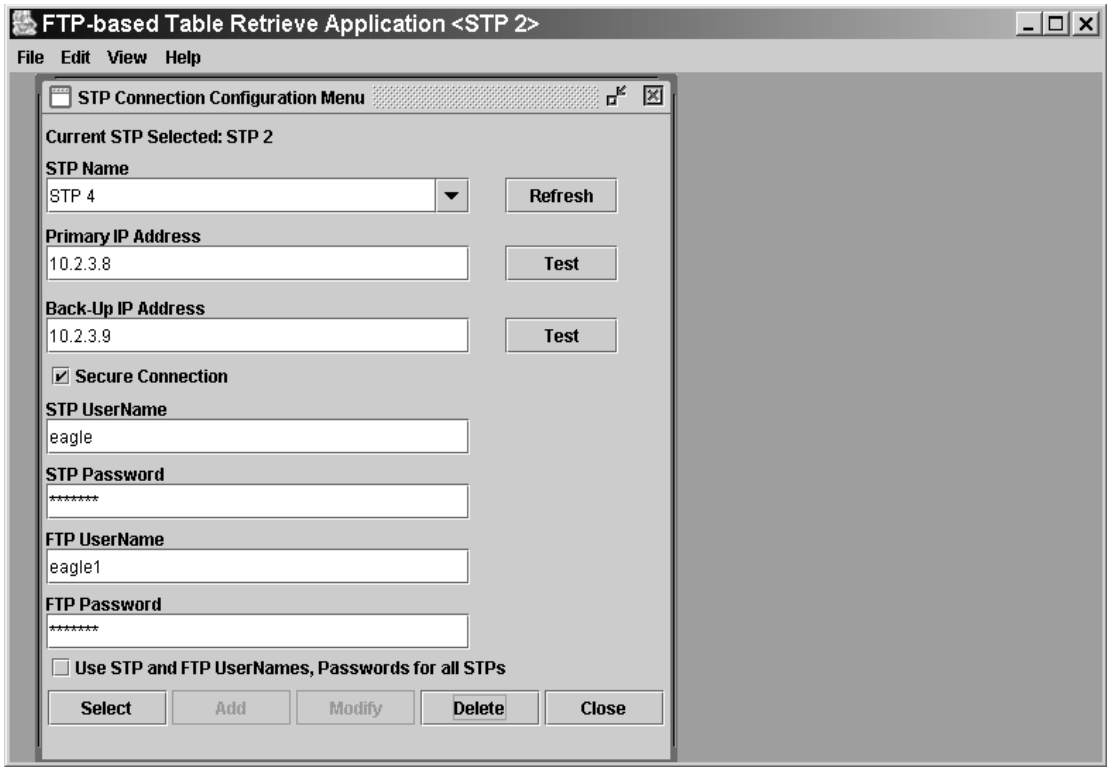


**Figure 20.** STP Name Selected from the STP Name Drop Down List (FTRA 2.0 or greater)



### 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 21 (FTRA 1.0) or Figure 22 on page 28 (FTRA 2.0 or greater). The **Refresh**, **Test**, **Select**, **Delete**, and **Close** buttons are enabled.

**Figure 21.** Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 1.0)

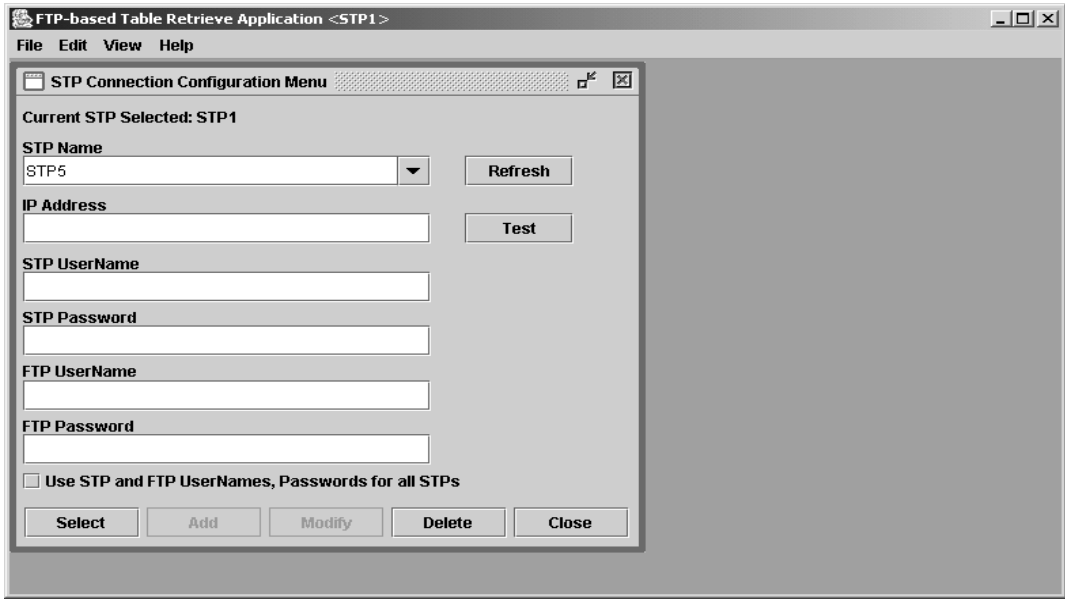
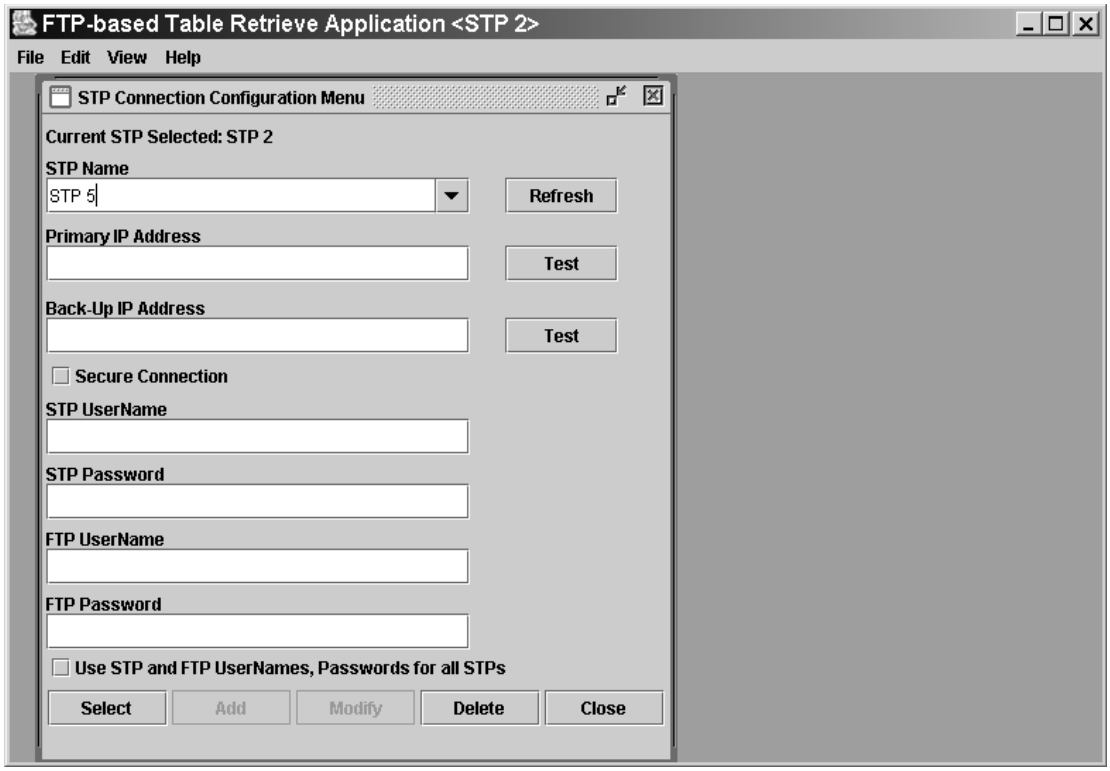


**Figure 22.** Selecting a STP Configuration Record by Typing in the STP Name Field (FTRA 2.0 or greater)



2. Click the **Refresh** button. The STP configuration record for the specified STP is displayed. See Figure 23 (FTRA 1.0) or Figure 24 on page 30 (FTRA 2.0 or greater).

**Figure 23.** STP Configuration Record (FTRA 1.0)

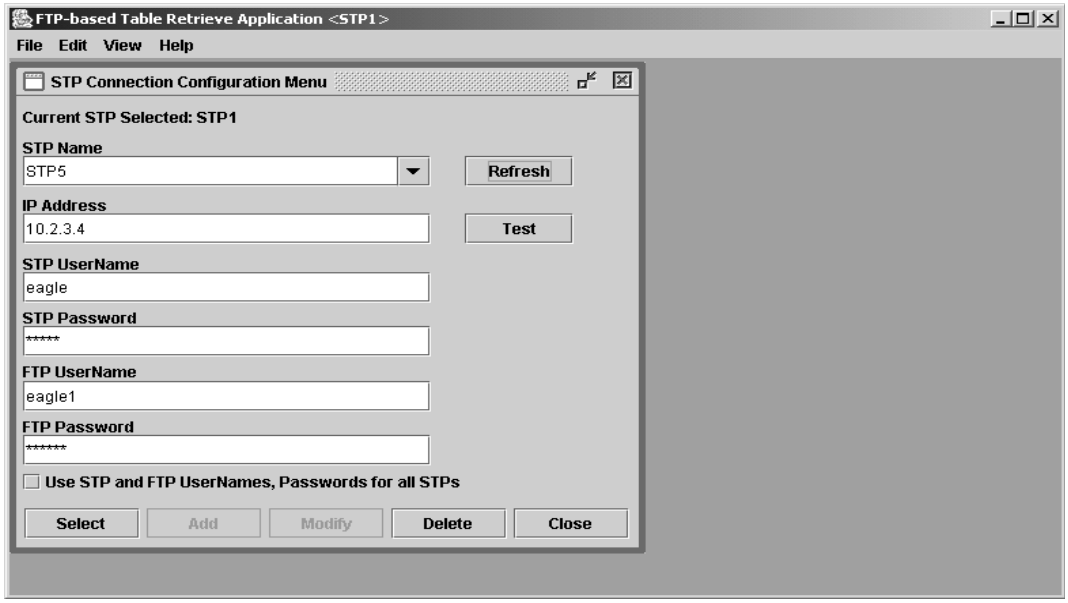
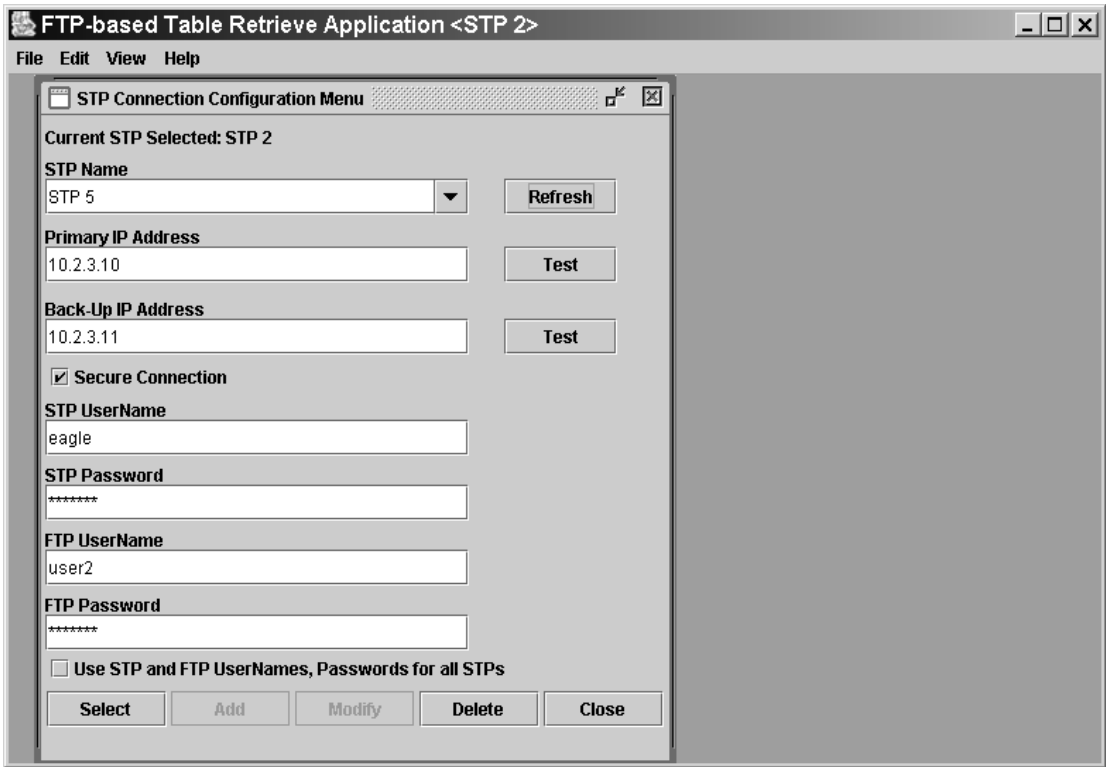


**Figure 24.** STP Configuration Record (FTRA 2.0 or greater)




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 25.

**Figure 25.** 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 5 on page 14. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 14.

2. Display the STP configuration record being modified. Go to the "Displaying an Existing STP Configuration Record" procedure on page 23.

3. Click the **Test** button. The **Connectivity Test Log** window opens. See Figure 26 and Figure 27 on page 32. 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 26.** Connectivity Test Log Window with No Errors

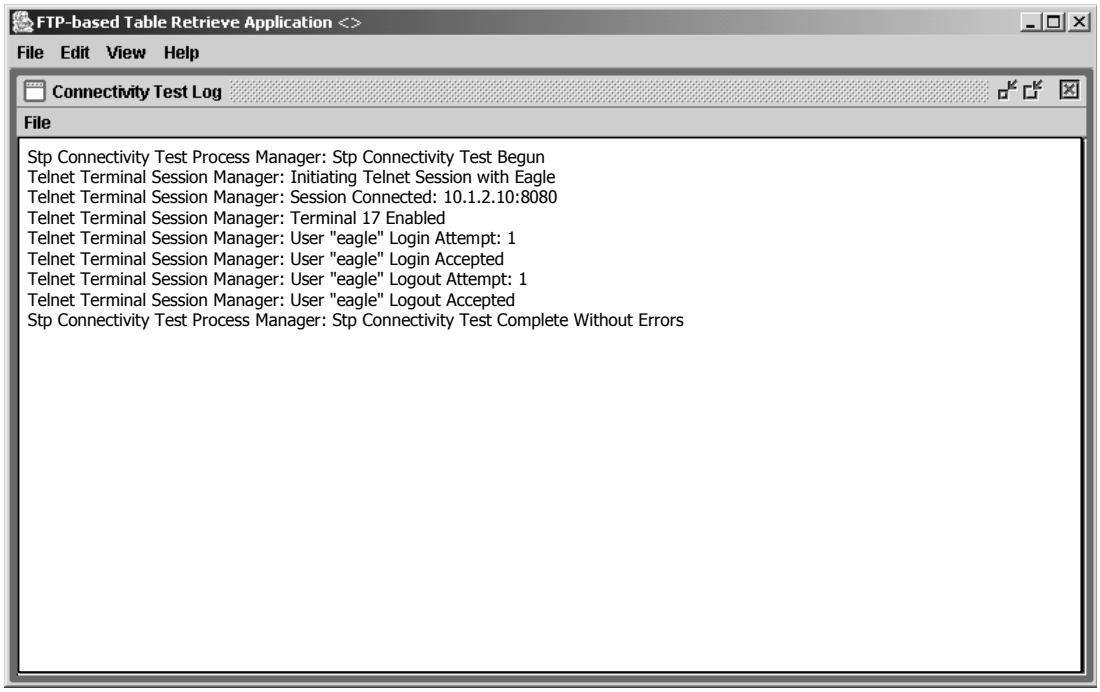
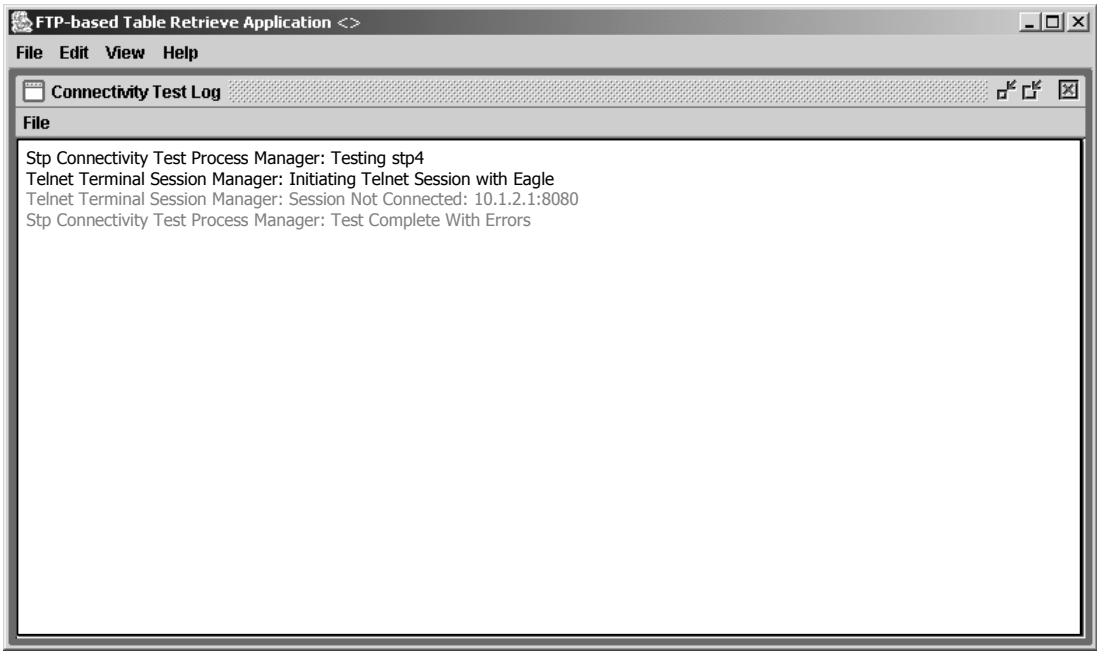
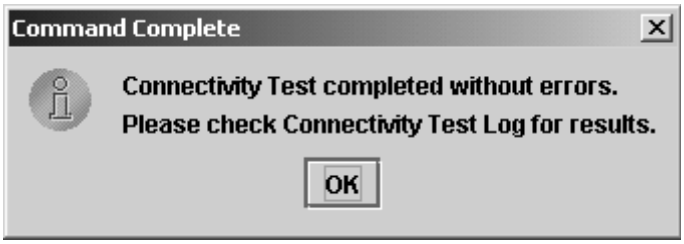


**Figure 27.** Connectivity Test Log Window with Errors




4. When the test is complete, the **Command Complete** window opens. See Figure 28. Click **OK** to continue.

**Figure 28.** Command Complete Connectivity Test Window

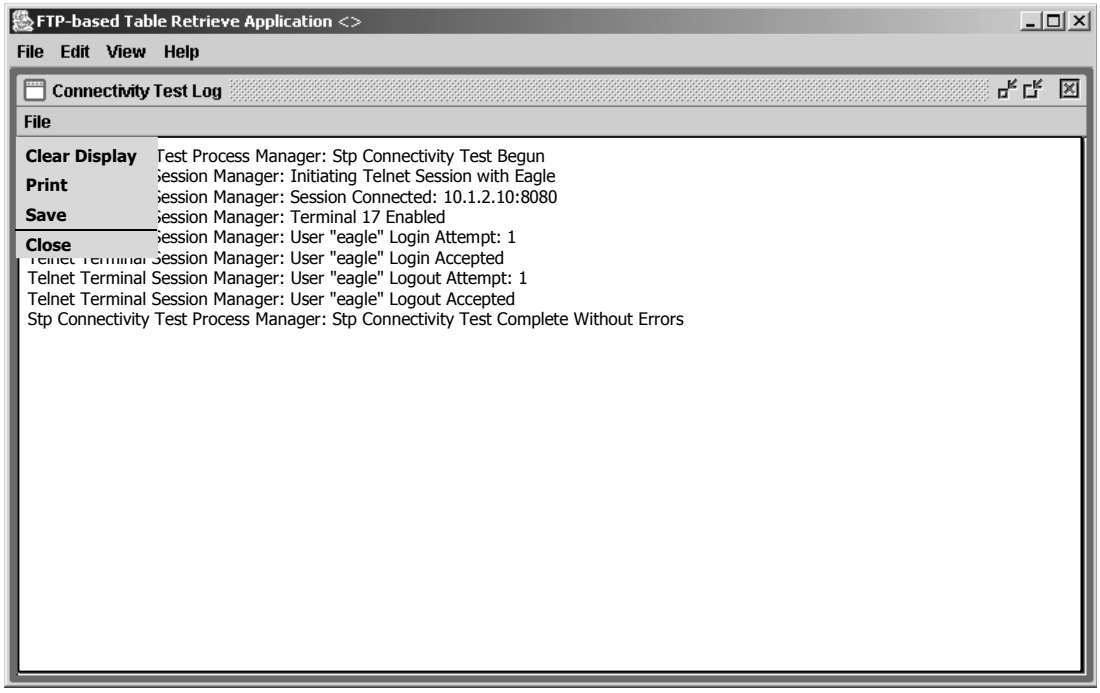



### Connectivity Test Log File Menu

The **File** menu in the **Connectivity Test Log** window, shown in Figure 29 on page 33, 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 29.** 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

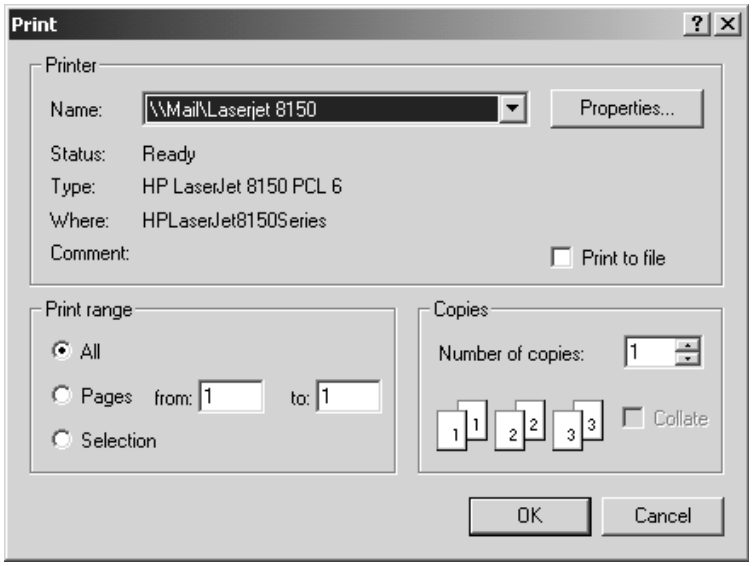
1. Select **File > Clear Display** in the **Connectivity Test Log** window. See Figure 29. The Connectivity Test Log display clears.

## Printing the Connectivity Test Log

### Procedure

1. Select **File > Print** in the **Connectivity Test Log** window. See Figure 29 on page 33. The **Print** window opens. See Figure 30.

   **Figure 30.** 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.

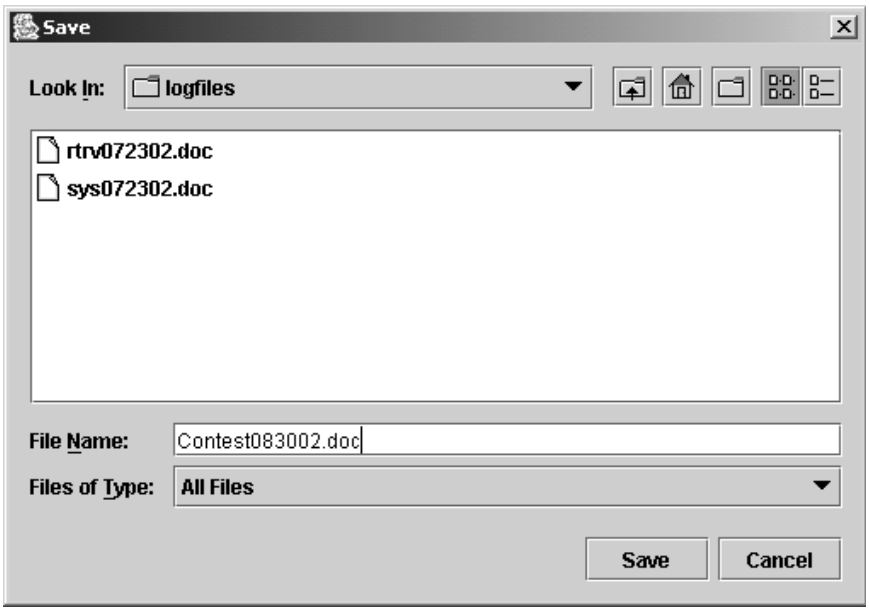
4. If you decide not to print the Connectivity Test Log, click the **Cancel** button in the **Print** window.

### Saving the Connectivity Test Log to a File

**Procedure**

1. Select **File > Save** in the **Connectivity Test Log** window. See Figure 29 on page 33. The **Save** window opens. See Figure 31.

   **Figure 31.** Save Window



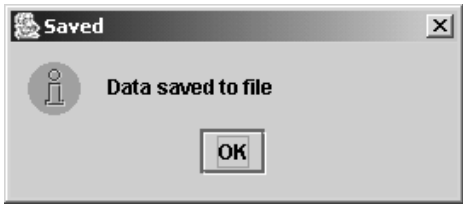

2. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

   **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 32.

   **Figure 32.** 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 29 on page 33. 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 5 on page 14. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 14.

2. Display the STP configuration record being modified. Go to the "Displaying an Existing STP Configuration Record" procedure on page 23.

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 11 on page 20, Figure 12 on page 20, or Figure 13 on page 21. If the FTP user name and FTP password are not entered, an error message is displayed. See Figure 14 on page 21 or Figure 15 on page 22

4. To apply the changes, click the **Modify** button. See Figure 33 on page 37 (FTRA 1.0) or Figure 34 on page 38 (FTRA 2.0 or greater). 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 35 on page 39). Click **OK** in the **STP Data Modified** window to continue.

**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.**

**Figure 33.** Modifying STP Configuration Record Parameters (FTRA 1.0)

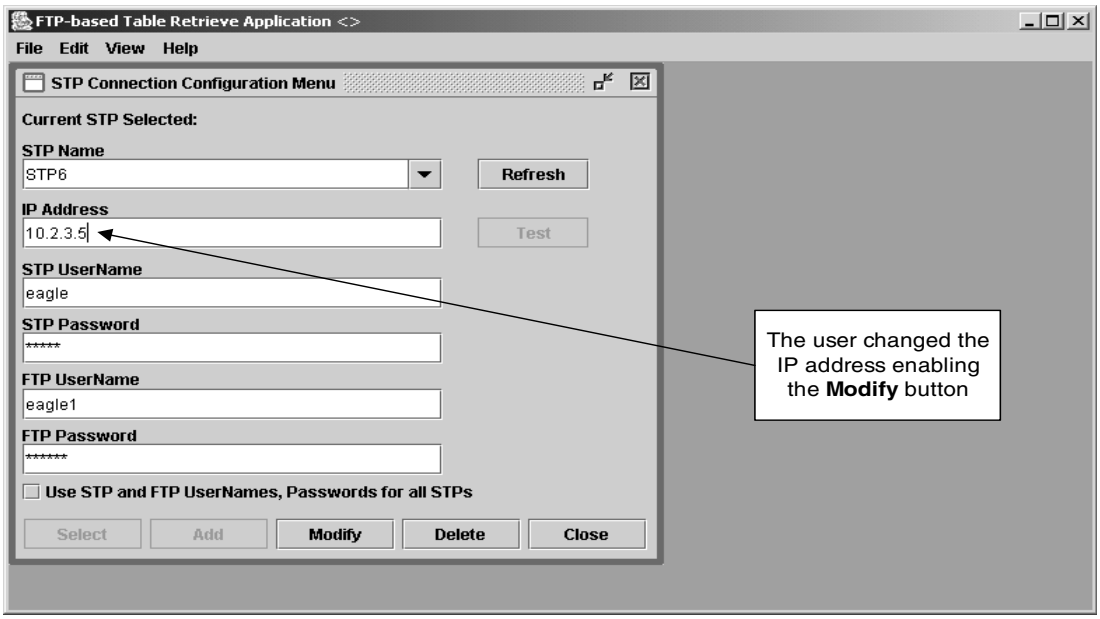


**Figure 34.** Modifying STP Configuration Record Parameters (FTRA 2.0 or greater)

**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. 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*.**

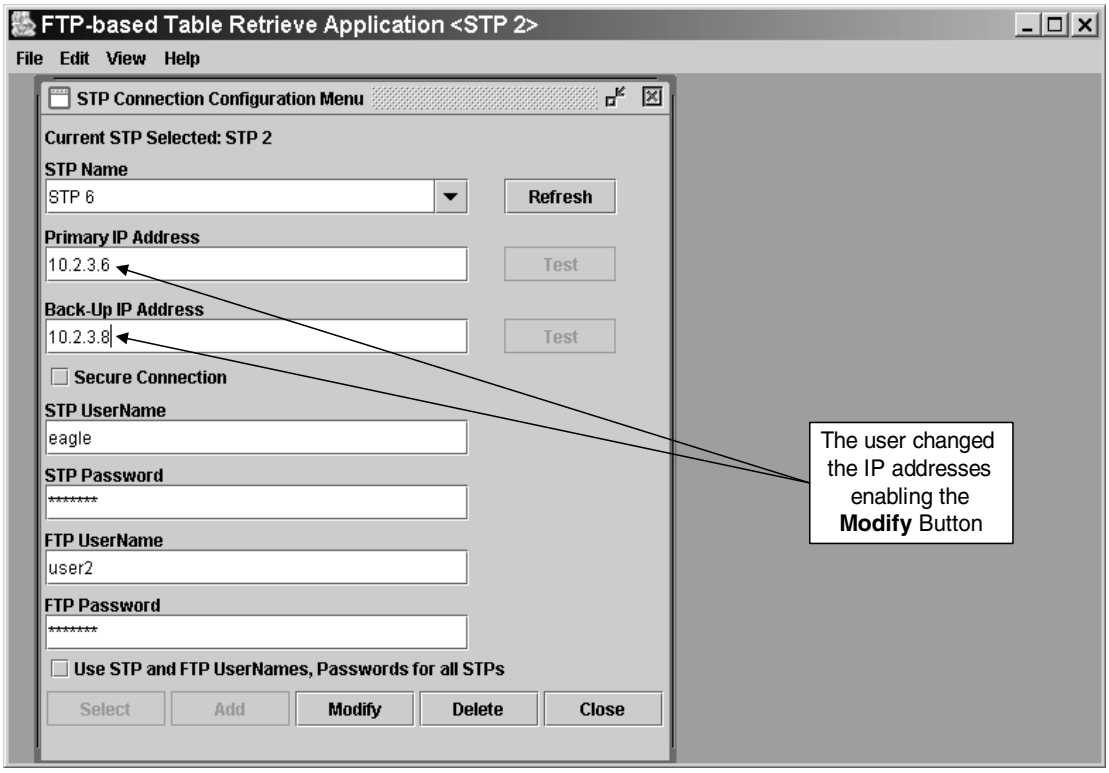
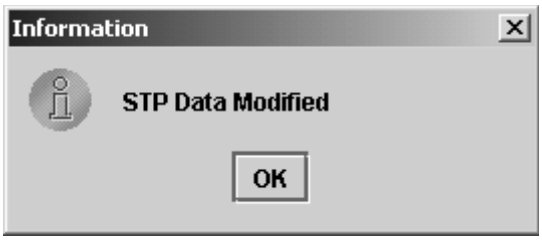
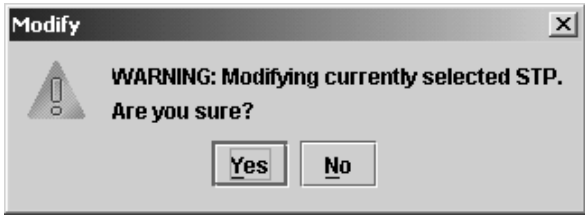


**Figure 35.** STP Data Modified Window




**NOTE: If the STP configuration record being changed is shown in the Current STP Selected: field, a Modify Warning window is displayed. See Figure 36 on page 39.**

**Figure 36.** 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 23.

## Deleting an STP Configuration Record

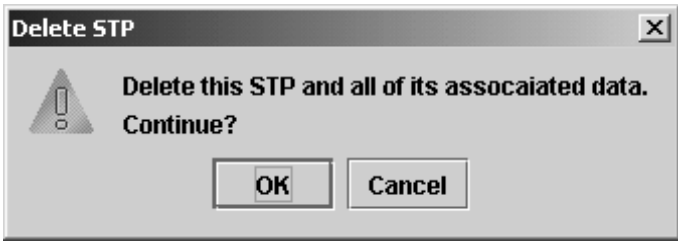
**Procedure**

1. Select **Edit > STP Connection Configuration** from the **FTP-Based Table Retrieve Application** window. See Figure 5 on page 14. The **STP Connection Configuration Menu** window opens. See Figure 6 on page 14.

2. Display the STP configuration record being deleted. Go to the "Displaying an Existing STP Configuration Record" procedure on page 23. 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 37.

**Figure 37.** 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 23.

## Selecting the Current STP

Before retrieving database tables from an Eagle STP, or sending commands to an Eagle STP, 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.

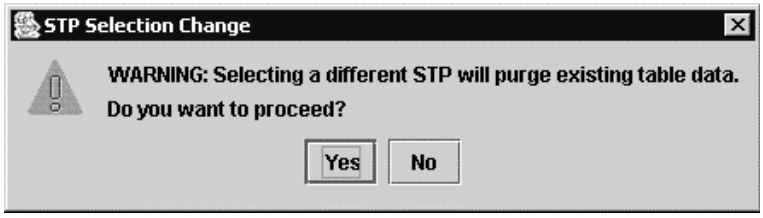
**Procedure**

1. Display an existing STP configuration record. Go to the "Displaying an Existing STP Configuration Record" procedure on page 23.

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 38.

   **Figure 38.** 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 39 (FTRA 1.0) or Figure 40 on page 42 (FTRA 2.0 or greater).

   **Figure 39.** Current STP Selected (FTRA 1.0)

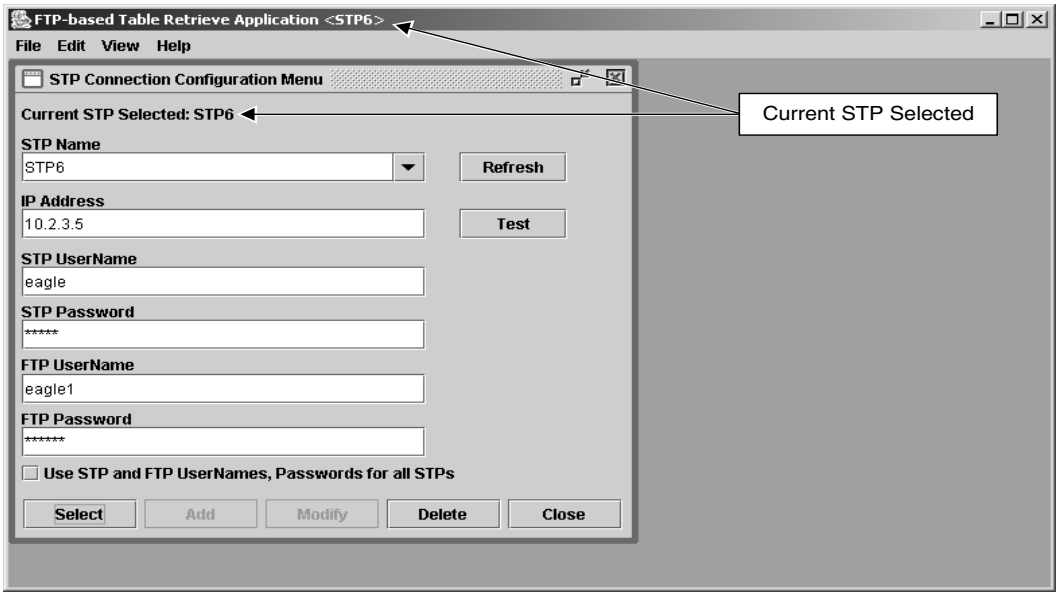
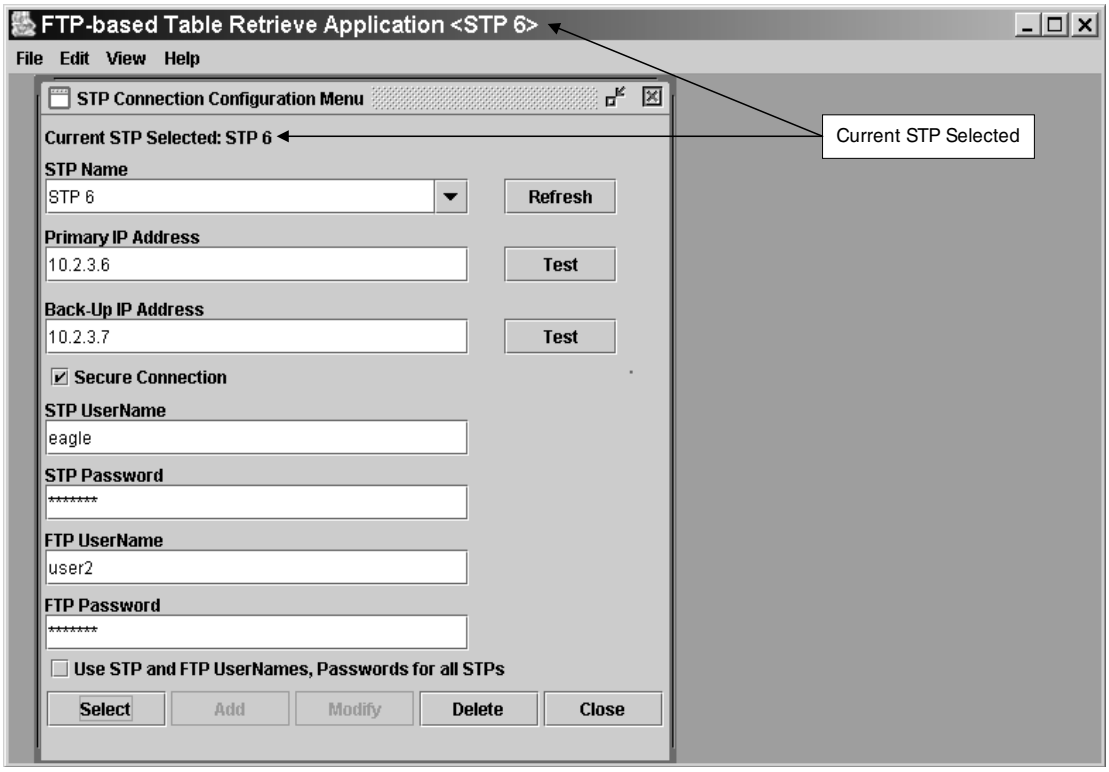


**Figure 40.** Current STP Selected (FTRA 2.0 or greater)




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 Host Key Provisioning

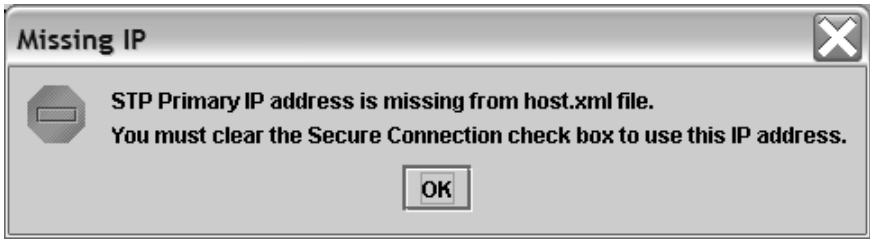
An Eagle using secure connections has a unique host key for each IPSM in the Eagle. This key is used by the FTRA (FTRA 2.0 or greater) to positively identify or authenticate each IPSM's telnet server on the Eagle. The FTRA will not connect to an unauthenticated server. The FTRA authenticates the server by matching it's pre-installed host key with the key received from the Eagle when the connection between the Eagle and the FTRA is made.

This procedure installs the public host key fingerprint, generated when the IPSM is installed into the Eagle, reinitialized 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 that the FTRA will connect to, but only for Eagles using secure connections to connect to the FTRA. This procedure must be performed before any secure connection between the Eagle and the FTRA can be initiated.

**NOTE: Once the IPSM is installed into the Eagle, 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. Reinitializing 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 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, you will receive the following warning message (Figure 41).

**Figure 41.** IP Address Warning Message




If the warning message shown in Figure 41 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 36), or add the public host key fingerprint to the FTRA's **hosts.xml** file using the procedure on page 45.

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) strong authentication, designed to provide security between the FTRA and the Eagle. This also prevents a hostile server from tricking the FTRA into exposing any Eagle 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 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 appliction 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, 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 05-03-17 15:08:45 GMT EAGLE 32.0.0
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 05-03-17 15:08:45 GMT EAGLE 32.0.0
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 specfiying 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 05-03-17 15:08:45 GMT EAGLE 32.0.0
CHG-TRM: MASP A - COMPLTD
```

---

**NOTE: When the IPSM is installed into the Eagle, 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** comand 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 05-03-17 15:08:45 GMT EAGLE 32.0.0
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 Tekelec Technical Services before removing and reinserting the IPSM. See page 3 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 system, 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 18), 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 36). 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 31. 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 and the FTRA shown in the Connectivity Test Log match. The Connectivity Test Log shows both the key received from the Eagle host and the key contained in the **hosts.xml** file for the Eagle host. The following is an example from the Connectivity Test Log containing a host key mismatch. The key received from the Eagle 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 using the **FTP Server Configuration** menu before database tables can be retrieved from the Eagle, or command files can be sent to the Eagle.

**NOTE: If the Secure Connection box in the STP Connection Configuration Menu window (applies only in FTRA 2.0 or greater) 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 43 on page 50), 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 42.

**Figure 42.** FTP Server Configuration Menu in the FTP-Based Table Retrieve Application Window


The **FTP Server Configuration Menu** window opens. See Figure 43 on page 50 and Table 3 on page 50.

**Figure 43.** FTP Server Configuration Menu Window

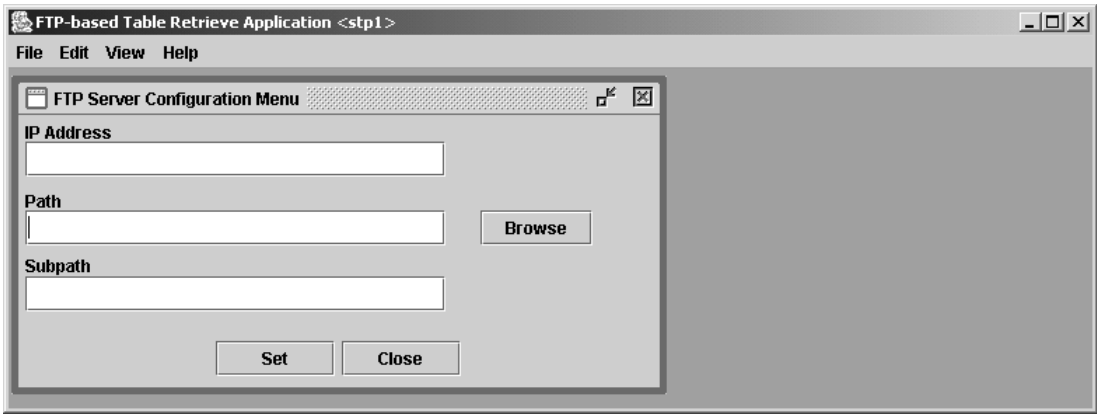



**Table 3.** FTP Server Configuration Menu Window Descriptions

| 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.<br><br>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 **`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. See Figure 43 on page 50.

   **NOTE: If the format is not entered correctly, the Invalid IP Address warning window is displayed. See Figure 44.**

   **Figure 44.** 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 45 and Table 4 on page 52.

   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.

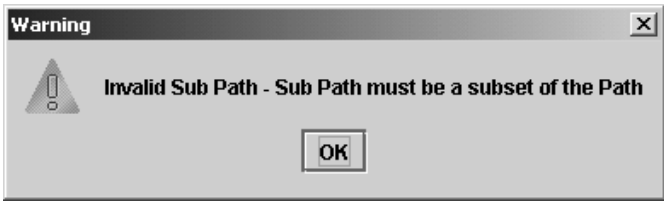
   **Figure 45.** Select Starting Directory Window

**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. |

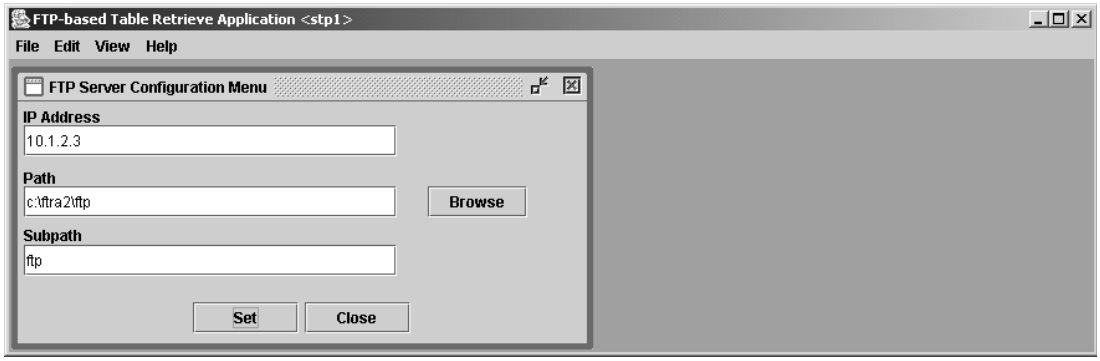
**4.** Enter the Subpath. The subpath must always be the last part of the path. The subpath is relative to the user's default directory upon FTP login. A file separator ('\' or '/') is not used to begin the subpath string. If an invalid Subpath is entered, a warning window opens. See Figure 46.

**Figure 46.** Invalid Subpath Window



5. Click the **Set** button. See Figure 47.

**Figure 47.** FTP Server Configuration Example




The **FTP Server Data Set** window opens. See Figure 48.

**Figure 48.** FTP Server Data Set Window


Click **OK** to continue.

# Retrieve Database Tables from an STP

### Retrieve Tables Window

The **Retrieve Tables** window (see Figure 50 on page 55) 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: Starting with FTRA 2.0, 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 49) that errors can be caused by attempting to retrieve and convert the GTT and EGTT database tables from the same Eagle.**

**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 49.** GTT Warning Window

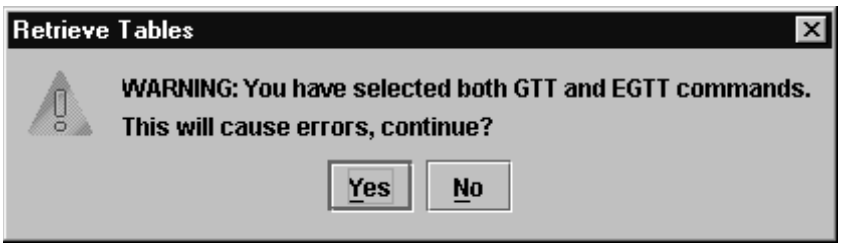


**Figure 50.** Retrieve Tables Window

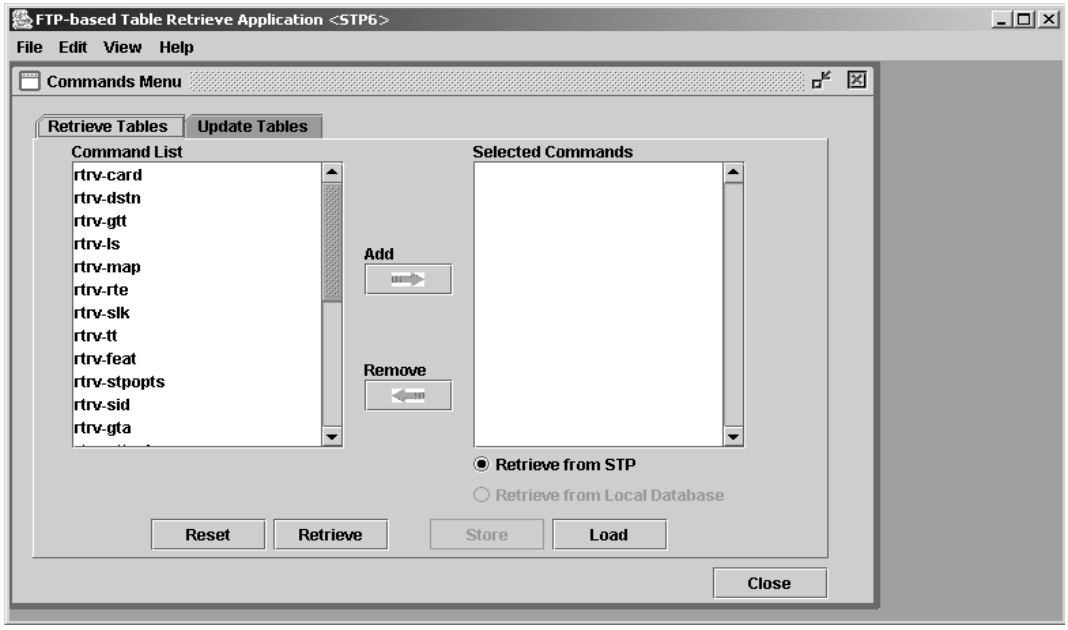



Table 5 on page 56 shows the description of the fields and buttons in the **Retrieve Tables** window.

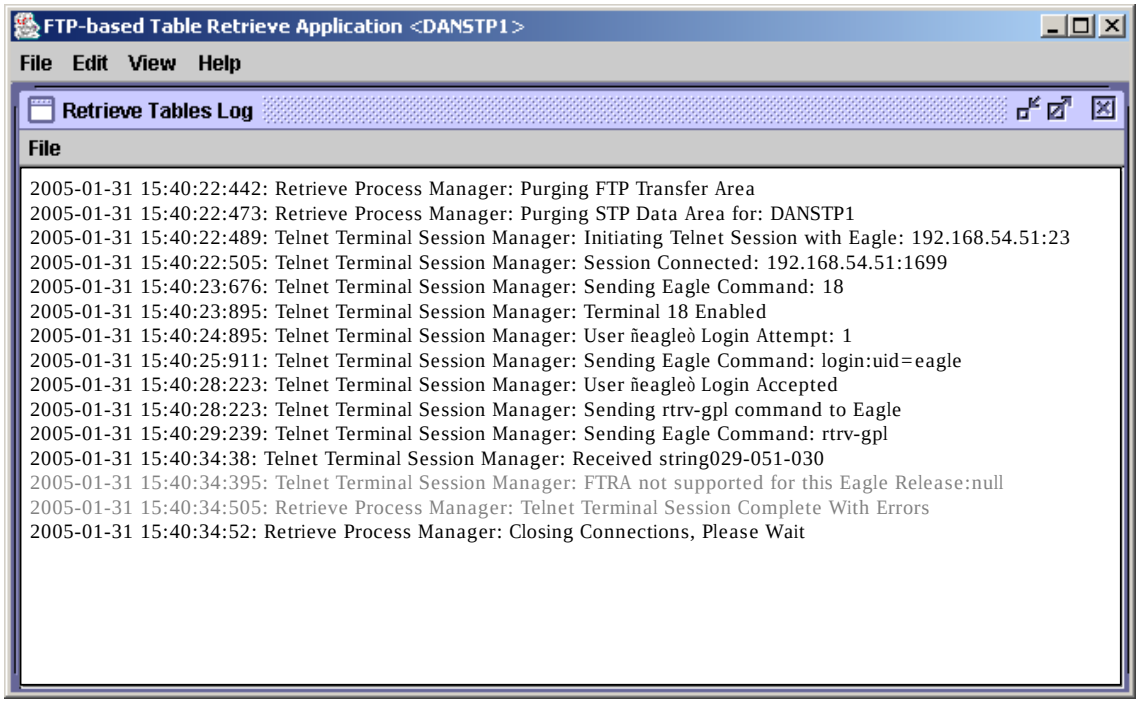
**Table 5.** Retrieve Tables Window Description

| 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.<br>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. |
| 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 releases 1.x and 2.x, the FTRA could operate only with one release of the Eagle. Starting with FTRA 3.0, the FTRA can operate with any of these Eagle releases: 29.0, 30.0, 30.2, 31.3, 31.6, 31.9, 32.0 and later. Eagle releases 32.0 and later are supported if that release supports CSV file output.

When a Retrieve Tables command is performed, FTRA 3.0 verifies that the Eagle is running one of the supported releases. If the Eagle release is not supported, an error message is displayed and the Retrieve Tables command is terminated. See Figure 51.

**Figure 51.** Retrieve Table Log - Release Not Compatible Error




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

## Procedure

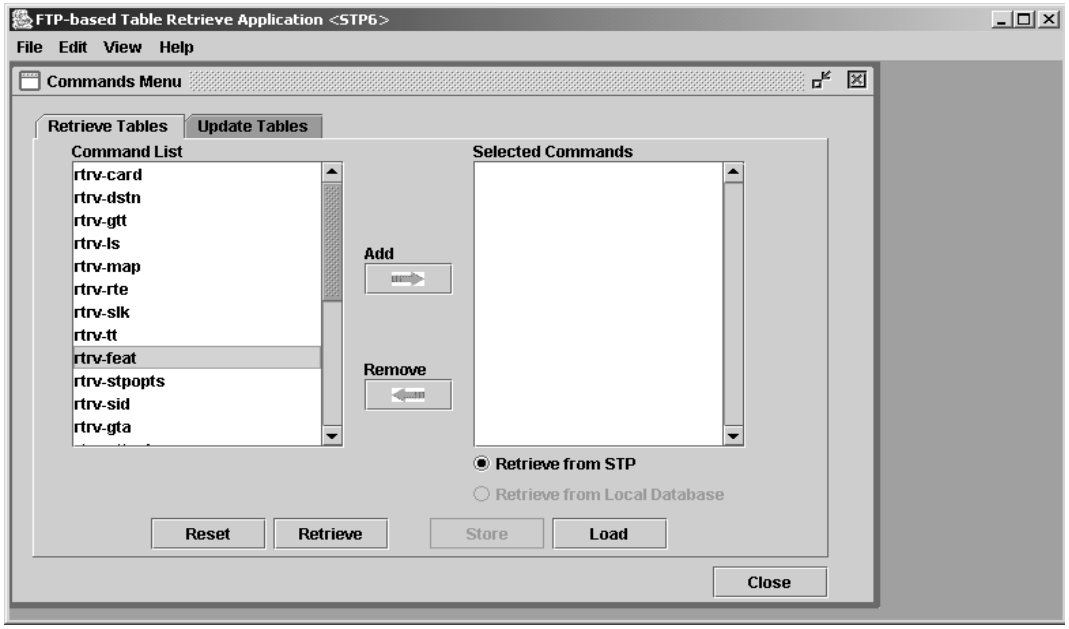
1. Select **Edit > Commands > Retrieve Tables** from the **FTP-Based Table Retrieve Application** window. See Figure 52. The **Retrieve Tables** window opens. See Figure 50 on page 55.

**Figure 52.** 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:

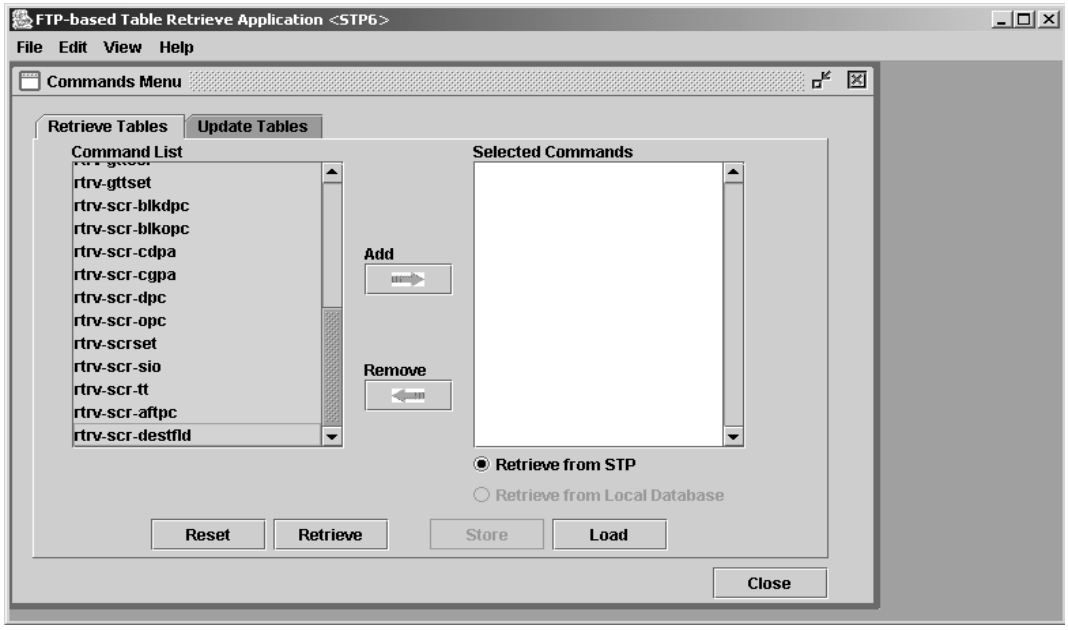
   **a.** To select a single command, click on the command and it is highlighted. See Figure 53.

**Figure 53.** Selecting a Command



**b.** 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 54.

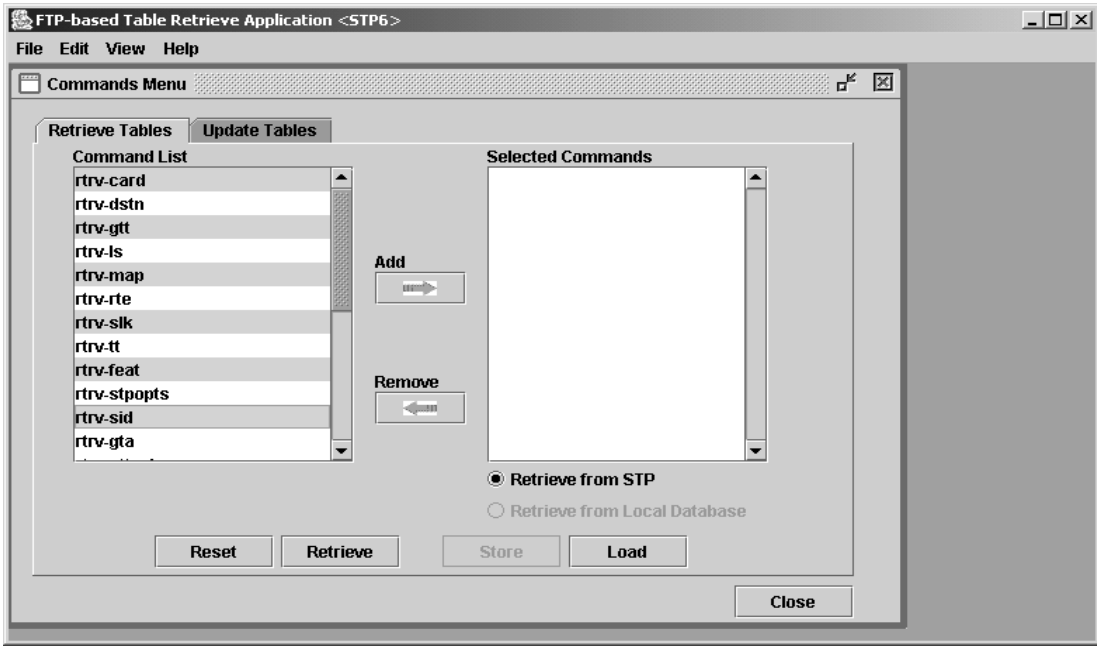
**Figure 54.** Selecting a Range of Commands




**c.** 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 55 on page 60.

**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 54.**

**Figure 55.** 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 56, Figure 57 on page 61, and Figure 58 on page 61.

**Figure 56.** Adding a Command to the Selected Commands Box

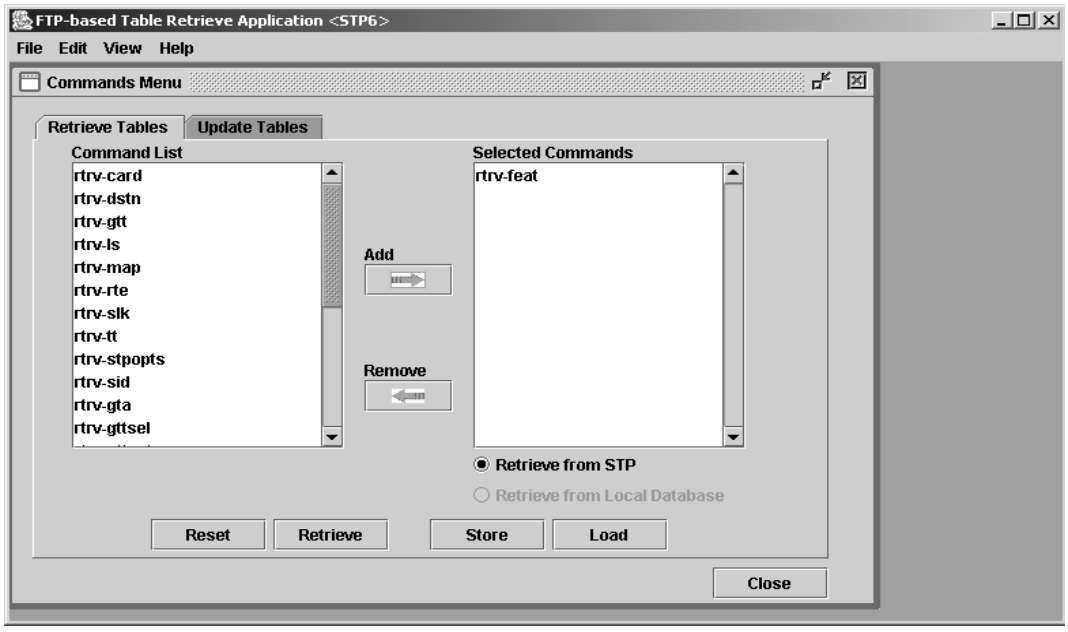


**Figure 57.** Adding a Range of Commands to the Selected Commands Box

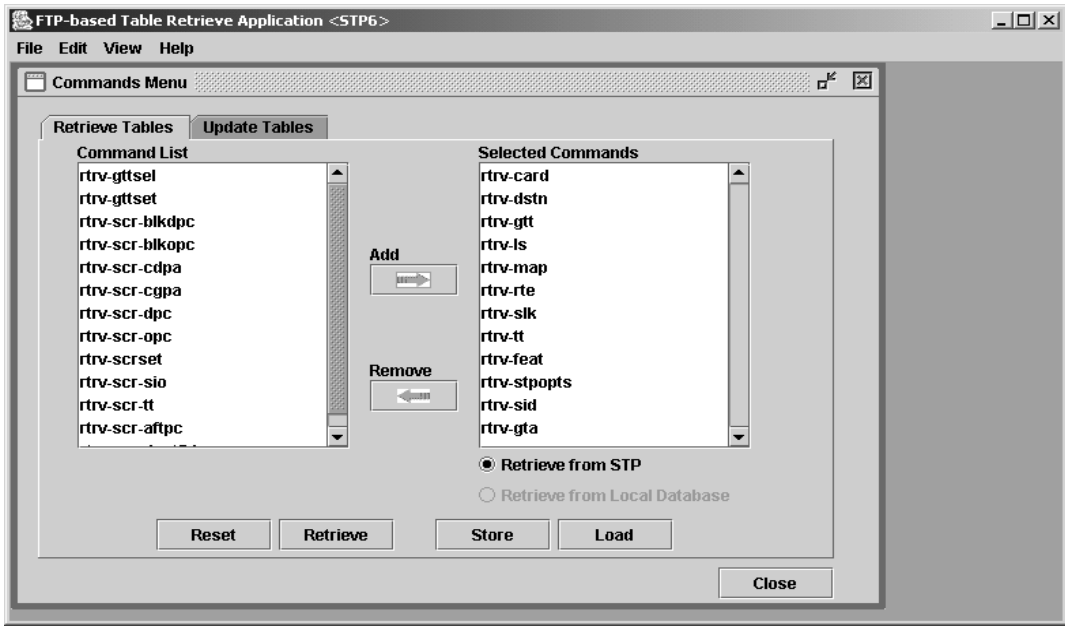
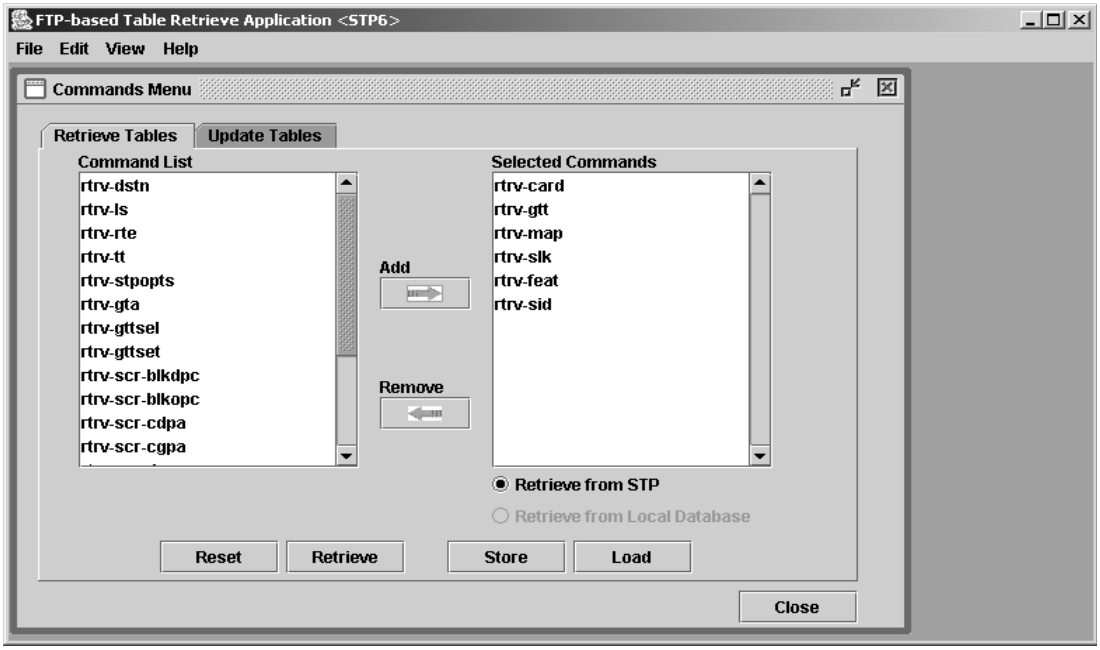



**Figure 58.** Adding Multiple Commands to Selected Commands Box

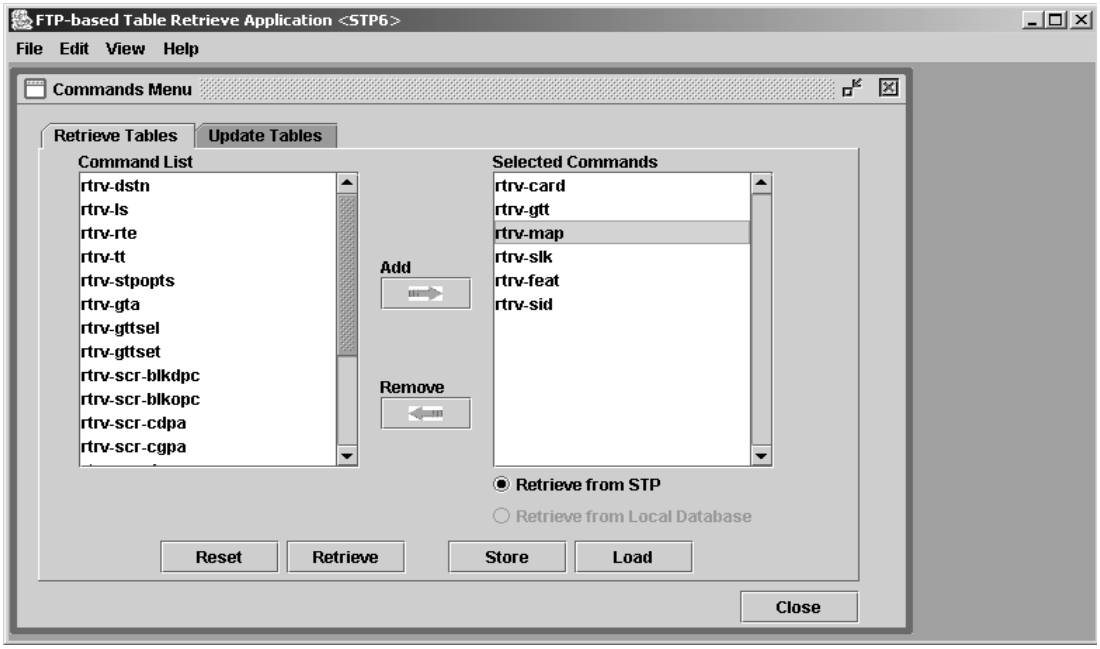


**NOTE: If no commands are being moved from the Selected Commands box to the Command List box, skip step 4 and go to step 5.**

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 59.

**Figure 59.** Command Selected to be Removed in the Selected Commands Box

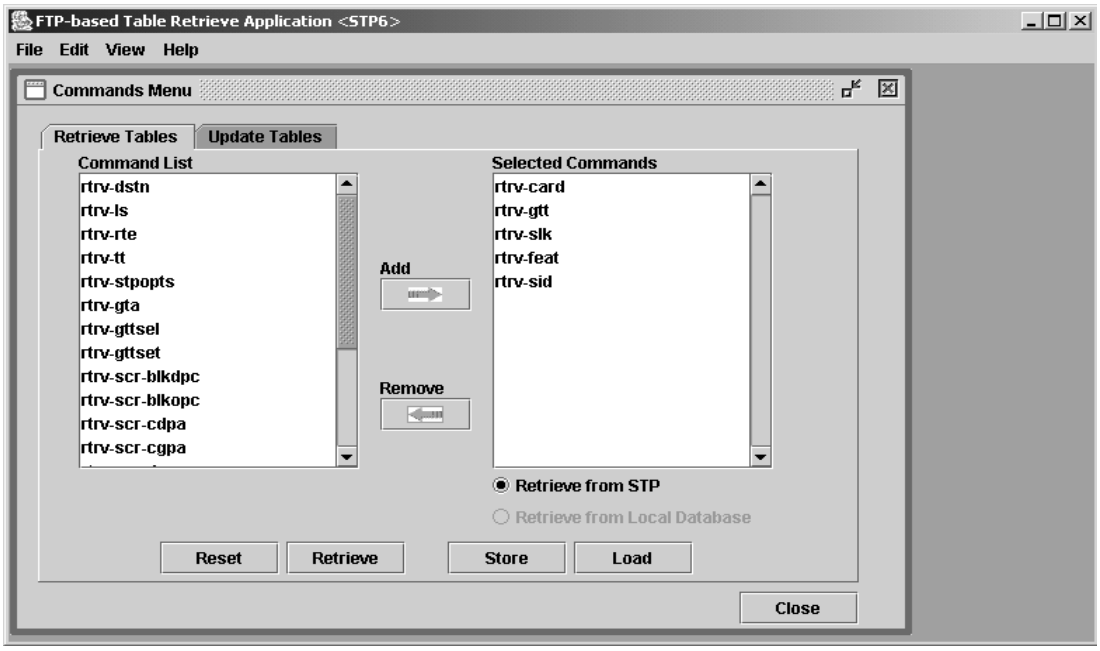



   b. To select a range of multiple commands to be removed, click on the first command and while holding down the Shift key, click on the last command to be removed. Click the **Remove** button. All highlighted commands are moved to the **Command List** box.

   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 60 on page 63.

**NOTE: When a command is removed it is placed at the bottom of the Command List box.**

**Figure 60.** Command Removed from the Selected Commands Box




**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.

---

**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 61.

**Figure 61.** 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 56 on page 60, Figure 57 on page 61, or Figure 58 on page 61.

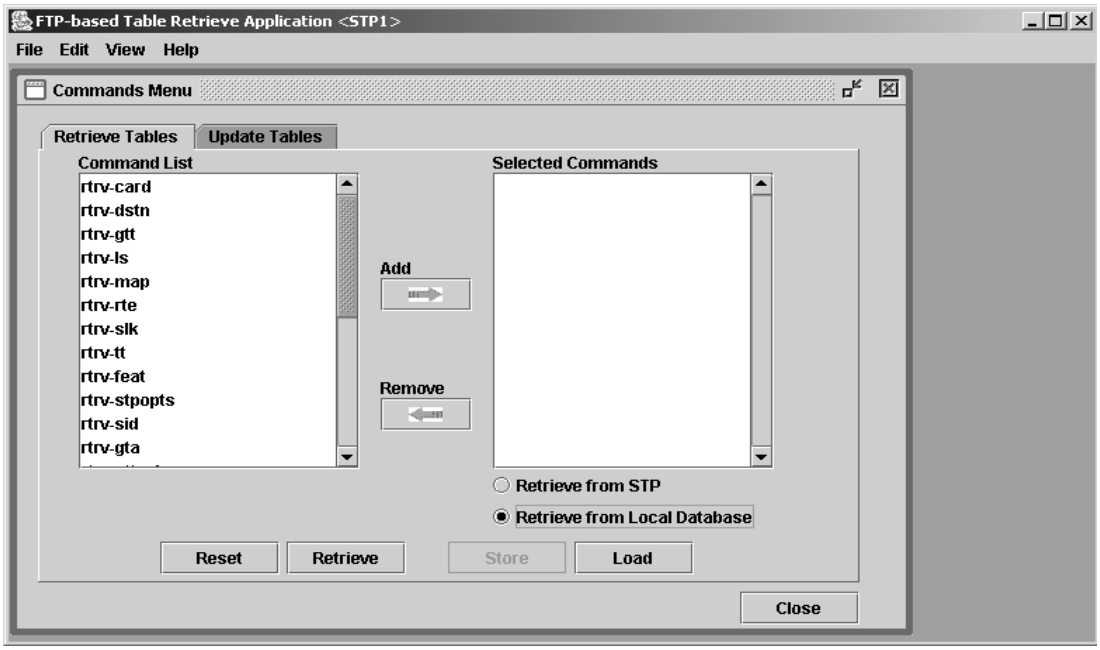
To use the Command Line Interface, go to the "Command Line Interface" section on page 73.

---

**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 62. Click the **Retrieve** button.

**Figure 62.** Retrieving Database Tables from the Local Database




---

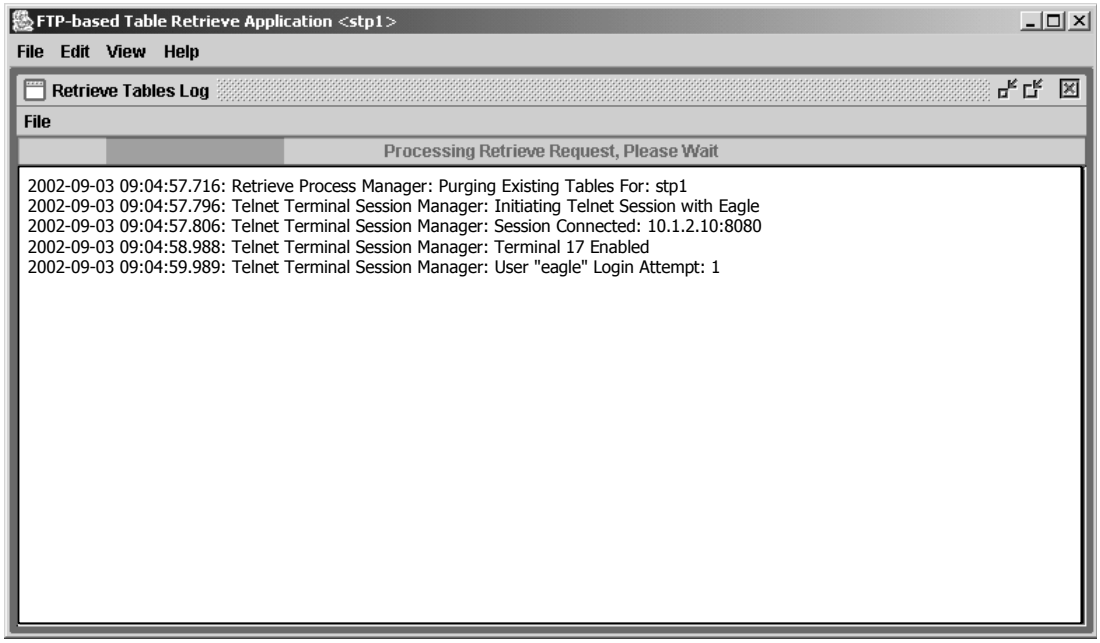
**NOTE: If step 6 was performed, skip step 7. This procedure is finished.**

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 63) and displays the message "Processing Retrieve Request, Please Wait" until the retrieve process completes.

   **NOTE: The telnet terminals on the Eagle to which FTRA will be connecting should have their terminal settings set to `all=no` (use the Eagle command `chg-trm:trm=<telnet terminal>:all=no` to make this setting; use the Eagle command `rtrv-trm` to verify the Eagle 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 54.**

   **Figure 63.** 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 64 on page 66.

**Figure 64.** 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 65.

**Figure 65.** Command Complete Window With Errors


The **Retrieve Table Log** window opens. See Figure 66 on page 67 and Figure 67 on page 68. 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 63 on page 65).

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 66 and Figure 67 on page 68.

**Figure 66.** Retrieve Tables Log Window without Errors

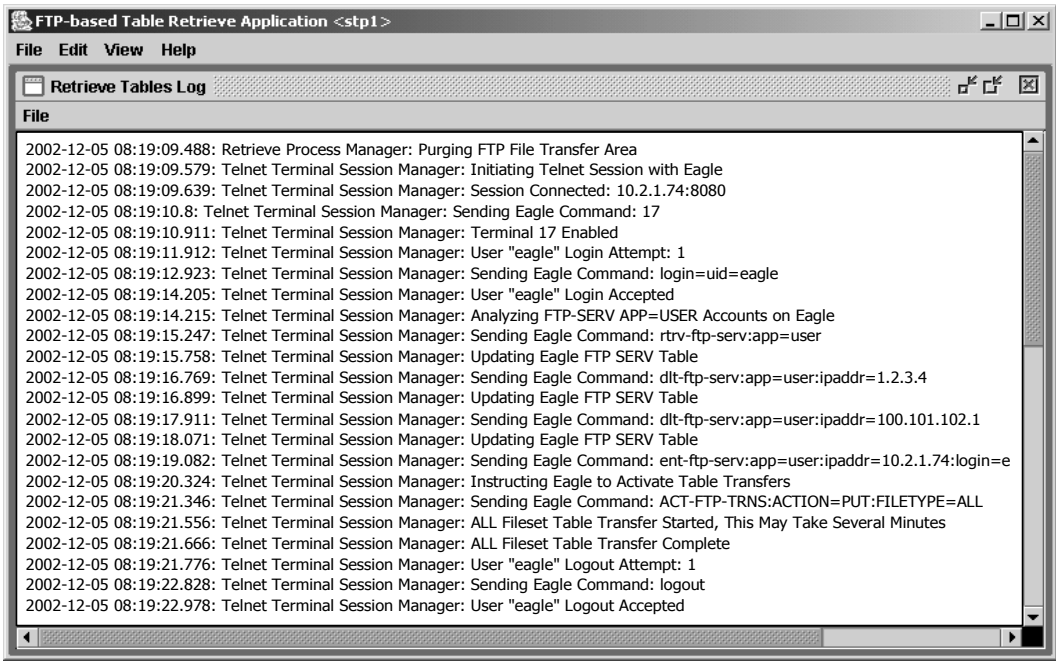
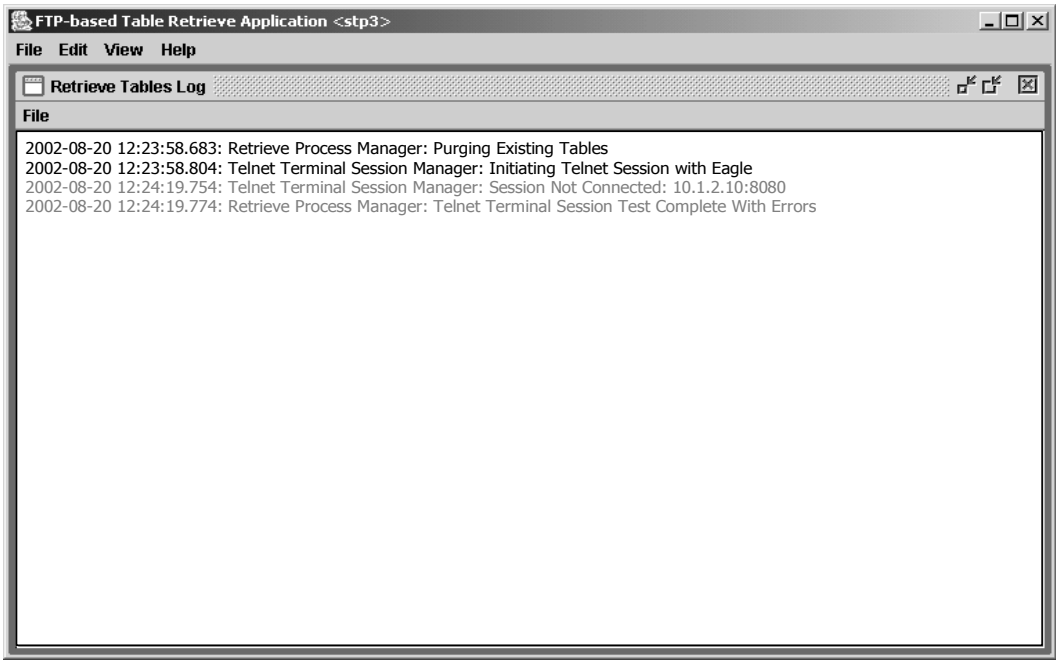


**Figure 67.** Retrieve Table Log with Errors

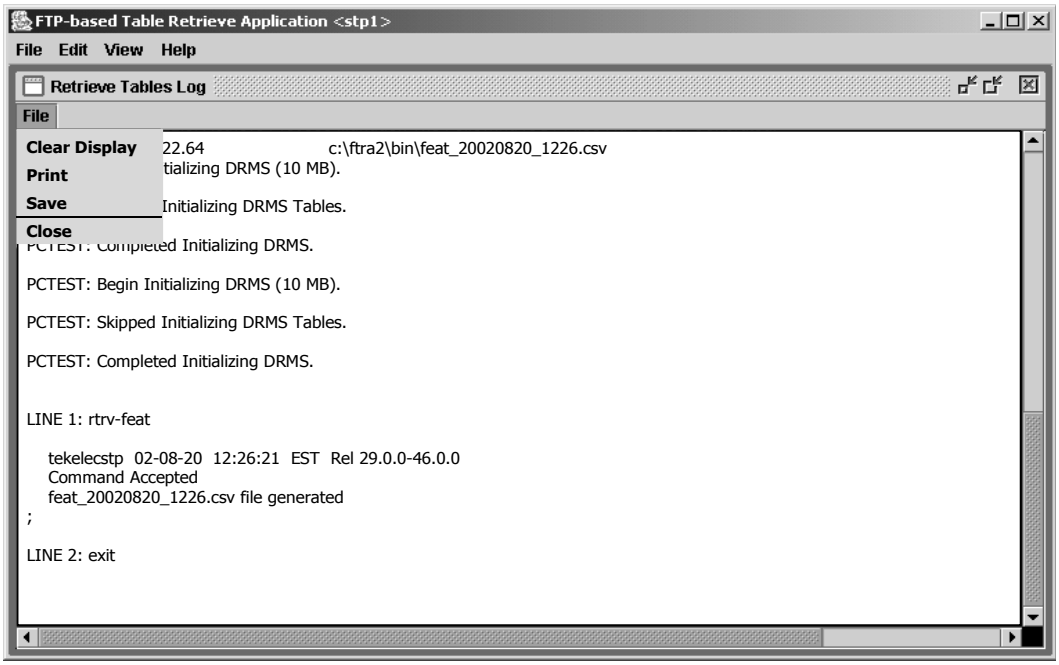



### Retrieve Tables Log File Menu

The **File** menu in the **Retrieve Tables Log** window, shown in Figure 68 on page 69, 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 68.** 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 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 **Retrieve Tables Log** window. See Figure 68.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 69. The **Retrieve Tables Log** window opens.

**Figure 69.** 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

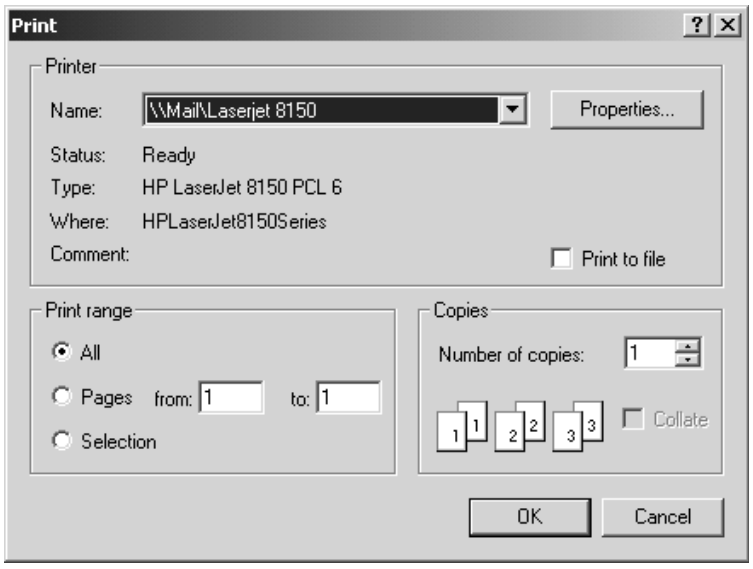
**NOTE: Perform either step 1 or steps 2 and 3.**

1. Select **File > Print** in the **Retrieve Tables Log** window. See Figure 68 on page 69.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 69 on page 69. The Retrieve Tables Log opens.

3. Select **File > Print** in the **Retrieve Tables Log** window. The **Print** window opens. See Figure 70.

**Figure 70.** 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

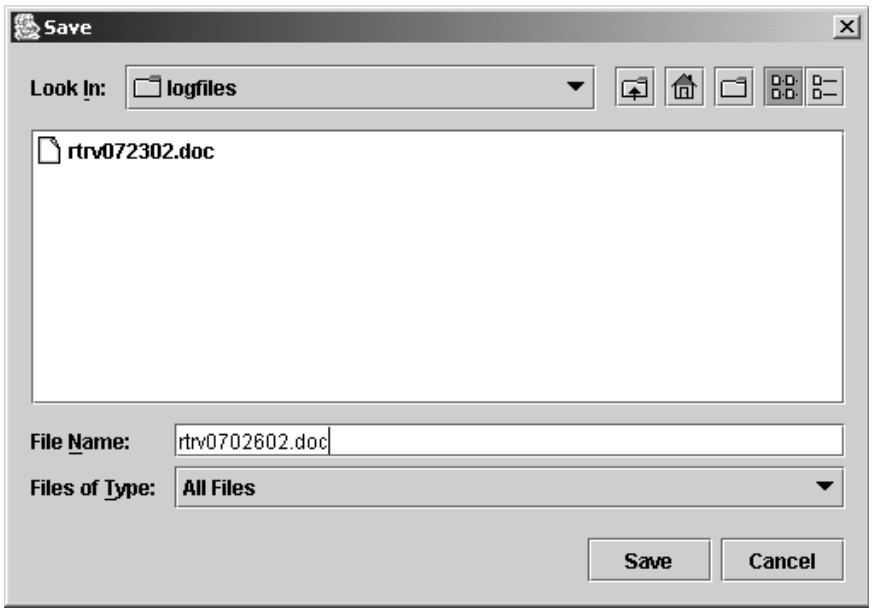
**NOTE: Perform either step 1 or steps 2 and 3.**

1. Select **File > Save** in the **Retrieve Tables Log** window. See Figure 68 on page 69.

2. Select **View > Retrieve Tables Log** from the **View** menu in the **FTP-based Table Retrieve Application** window. See Figure 69 on page 69. The **Retrieve Tables Log** window opens.

3. Select **File > Save** in the **Retrieve Tables Log** window. The **Save** window opens. See Figure 71.

**Figure 71.** Save Window



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

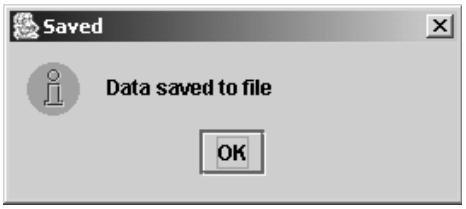
   **NOTE: The .doc file type is recommended, although the user can use Microsoft Word to open the file, even if it was saved as a .txt file.**

---

   **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 72.

   **Figure 72.** 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 68 on page 69. 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 STP'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 54.

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`** command at the DOS command prompt (in Windows) or at a shell command prompt (in UNIX).

The user can automate this retrieve process through the use of external scheduling software such as Task Scheduler (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 12.

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`** command (see Figure 73 on page 74 or Figure 74 on page 74). The stored **`rtrv`** commands are sent to all provisioned STPs. The data tables are retrieved and converted to the CSV file format.

**Figure 73.** FTRA Windows Command Line Interface

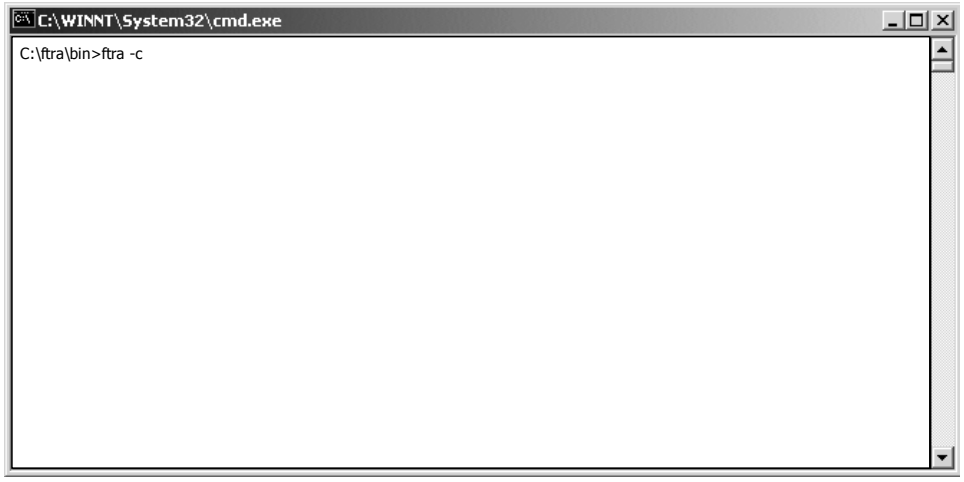



**Figure 74.** FTRA UNIX Command Line Interface

### Procedure – Command Line Interface Automatic Start

1. Enter the **`ftra -c`** command, the path to the **`bin`** directory of the FTRA <*install_directory*>, the start time of the external scheduling software such as Task Scheduler (in Windows, see Figure 75) and "cron" (in Unix, see Figure 76 on page 76).

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

   **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 77 on page 76.**

**Figure 75.** FTRA Windows Task Scheduler

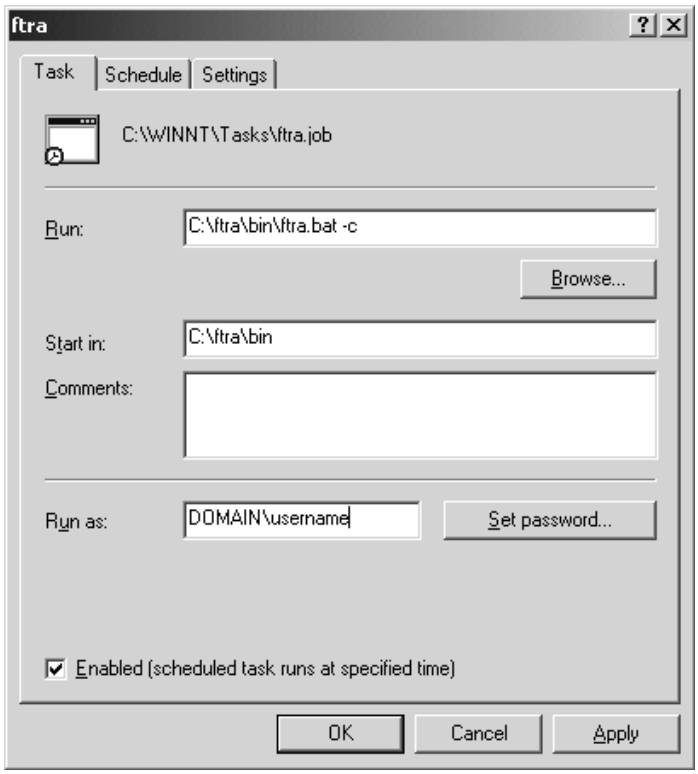


**Figure 76.** UNIX **cron** Job Scheduled using **crontab**

**NOTE: The last line shows that the FTRA is scheduled to run at 3:00 AM Monday through Friday.**

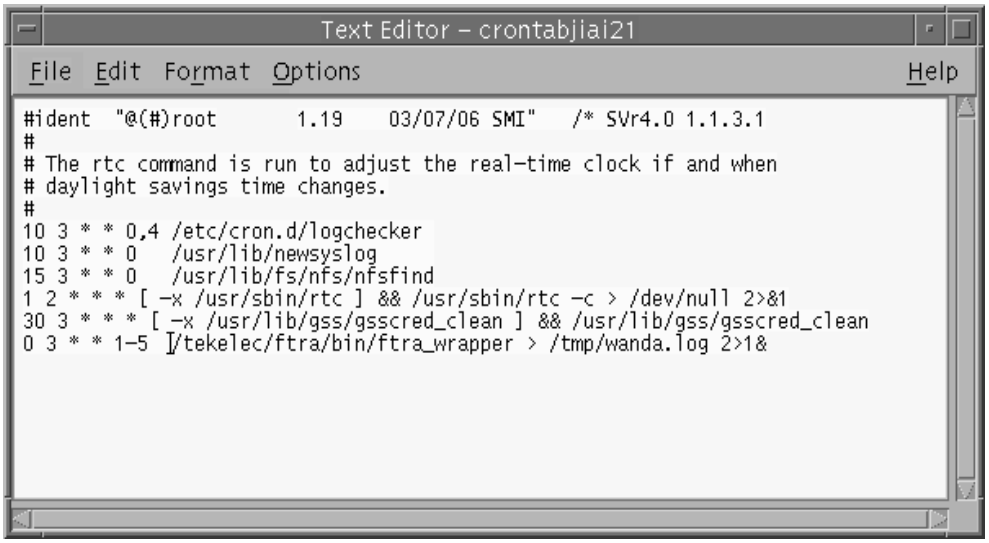
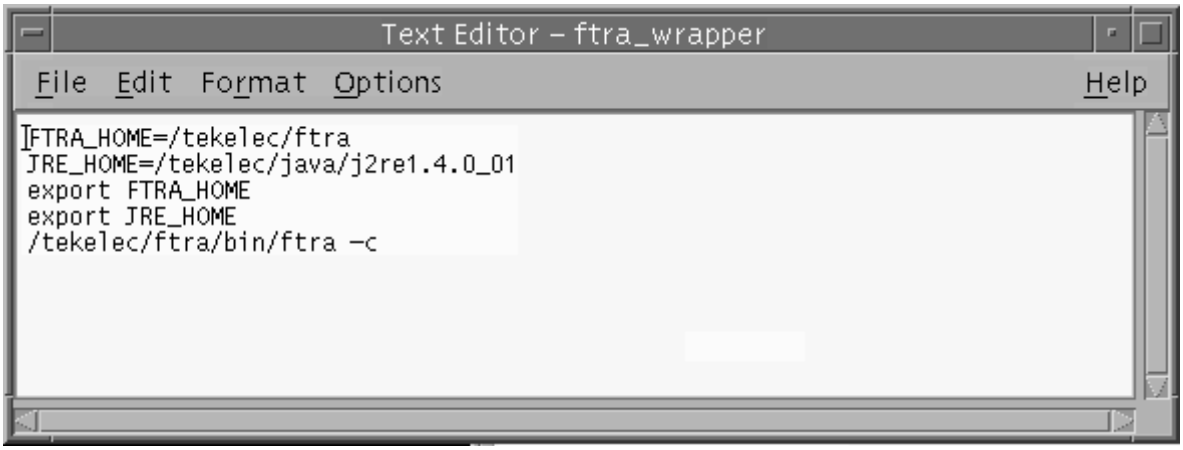



**Figure 77.** CRON FTRA Wrapper Script



## Updating Database Tables in the Selected STP

The **Update Tables** window (see Figure 78) is used to send Eagle STP 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 78.** Update Tables Window

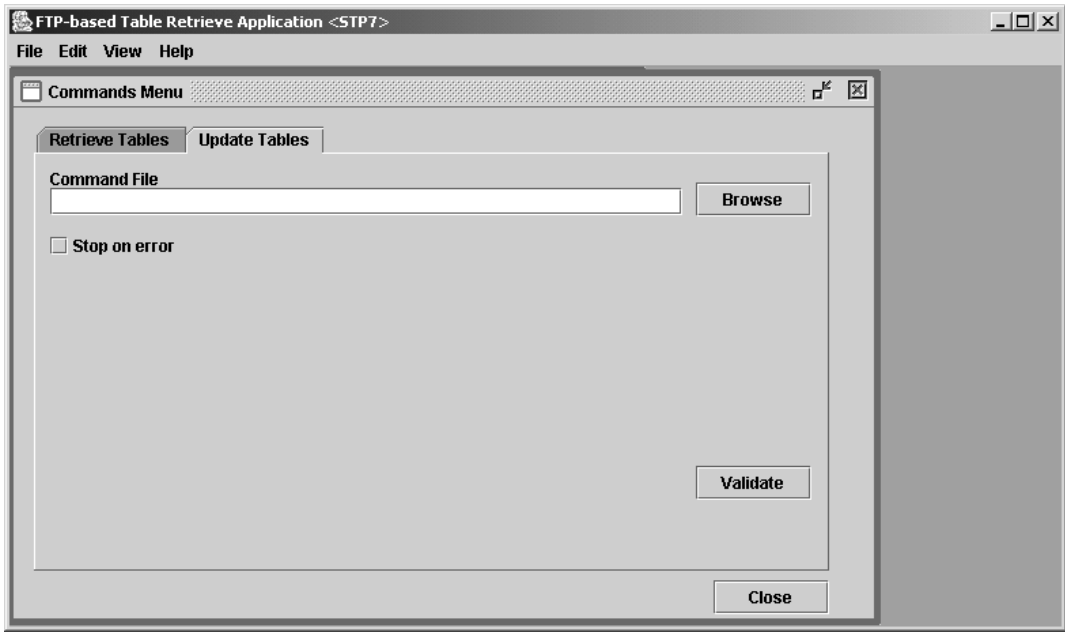


Table 6 shows the description of the fields and buttons in the **Update Tables** window.

**Table 6.** 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 STP 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 STP commands using the offline database. |
| Close | Closes the **Commands Menu** window. |

### Validating a Command File

**Procedure**

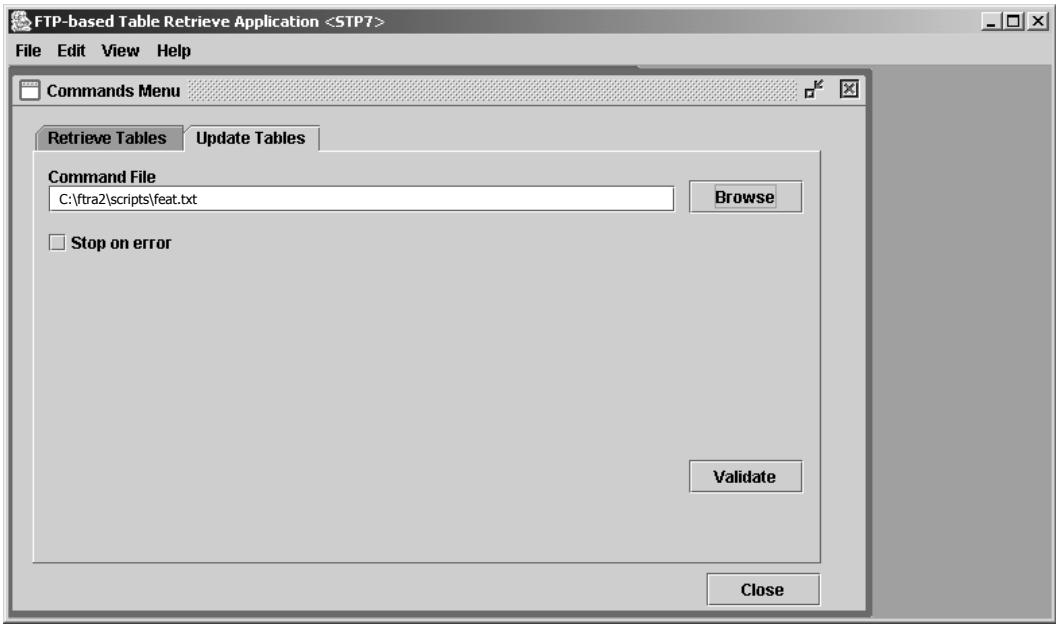
1. Select **Edit > Commands > Update Tables** in the **FTP-based Table Retrieve Application** window. See Figure 79. The **Update Tables** window opens. See Figure 78 on page 77.

**Figure 79.** 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 80.

   **Figure 80.** Update Tables with a Command File Selected




   b. Click the **Browse** button. The **Select** window is opened. See Figure 81 on page 80. 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 7 on page 80 shows the description of the buttons in the **Select** window.

**Figure 81.** Select Window

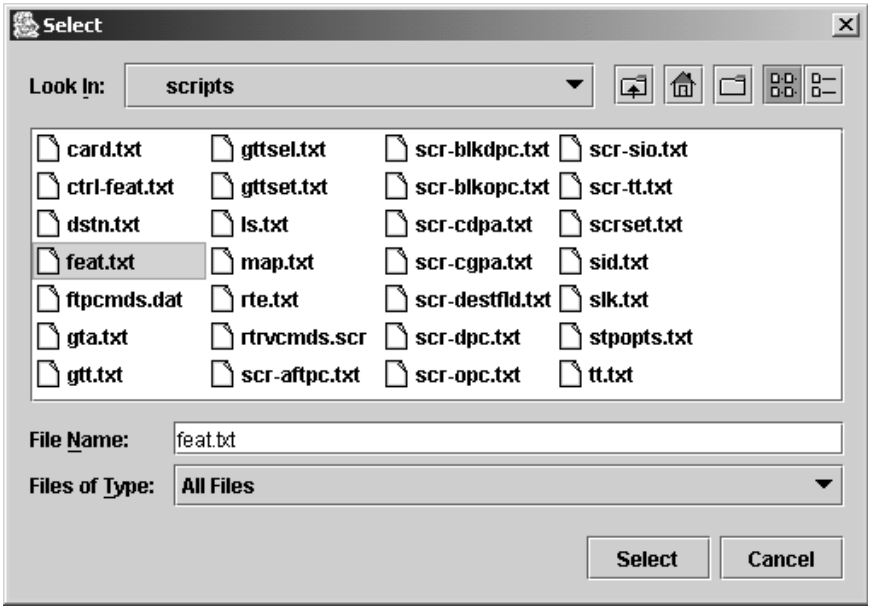
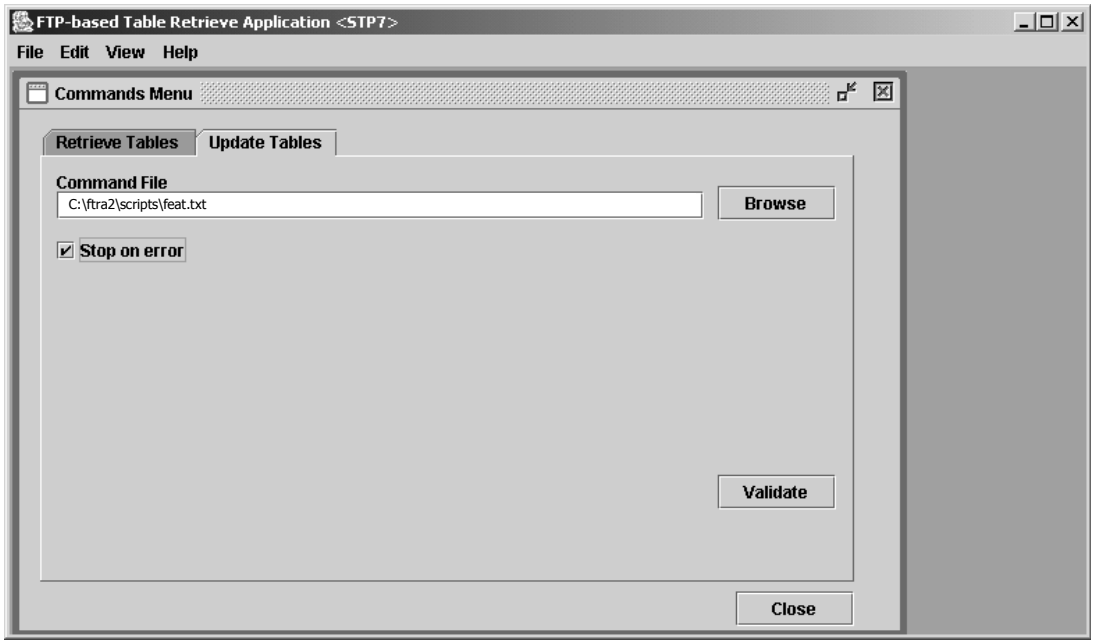



**Table 7.** Select Window Descriptions

| 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. |

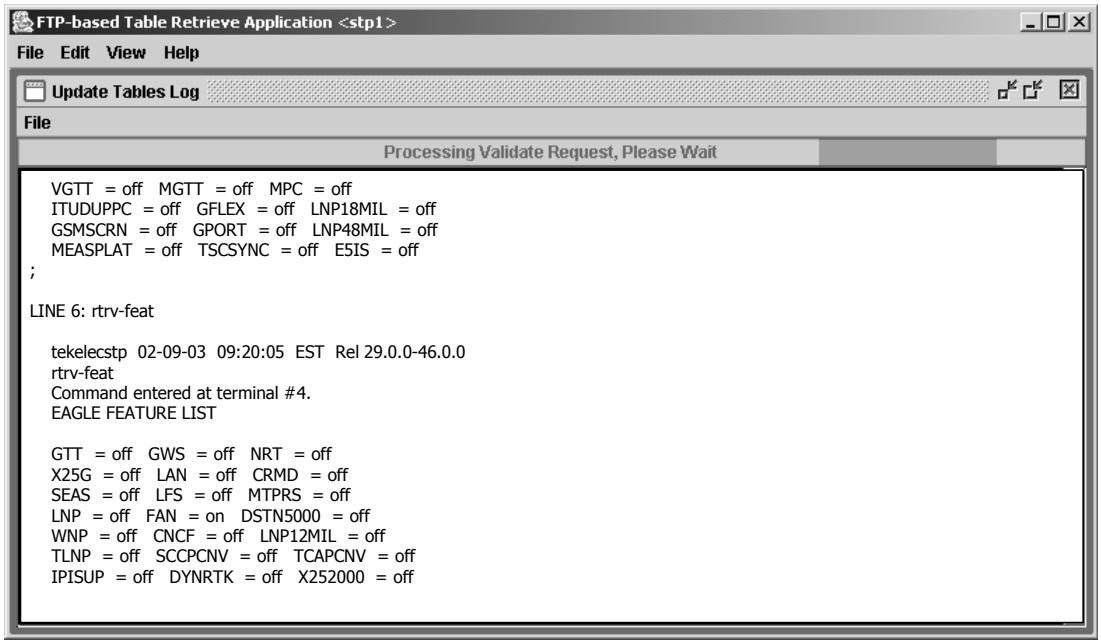
3. If you wish to have the command validation stop if any errors are found, check the **Stop on error** box in the **Update Tables** window. See Figure 82. If you wish to have the command validation processed regardless of any errors, uncheck the **Stop on error** box. The error results are displayed in the Update Tables Log.

**Figure 82.** 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 83.

**Figure 83.** Update Tables Log Window - Processing Retrieve Request




The **Update Validation Complete** window opens. See the "Update Validation Complete Window" section on page 83.

---

5. The **Update Tables Log** window opens. It contains the events and error messages generated during the validation. See Figure 93 on page 88, Figure 94 on page 89, and Figure 95 on page 90 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 84.**

**Figure 84.** 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 85.

**Figure 85.** Update Validation Complete Window without Errors

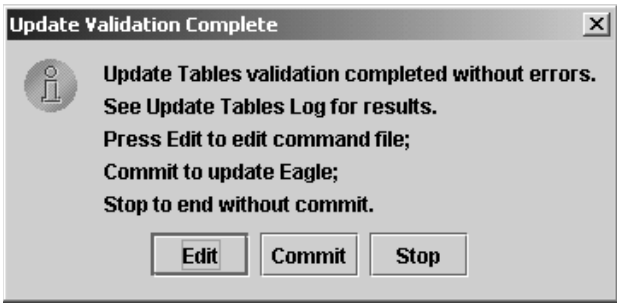



Table 8 shows the description of the buttons in the **Update Validation Complete** window.

**Table 8.** 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 85. |
| 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 84.<br>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 86. 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 85.

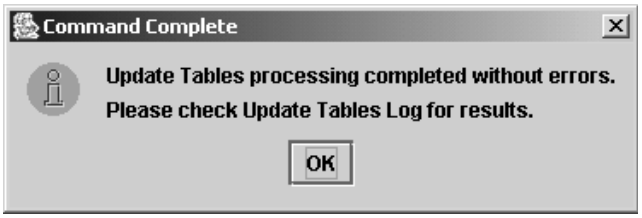
**Figure 86.** Update Validation Complete Window with Errors


### 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 85 on page 83. 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 87. Click **OK**, to continue. The Update Tables Log contains the commit processing events. See Figure 93 on page 88.

**Figure 87.** Command Complete Window



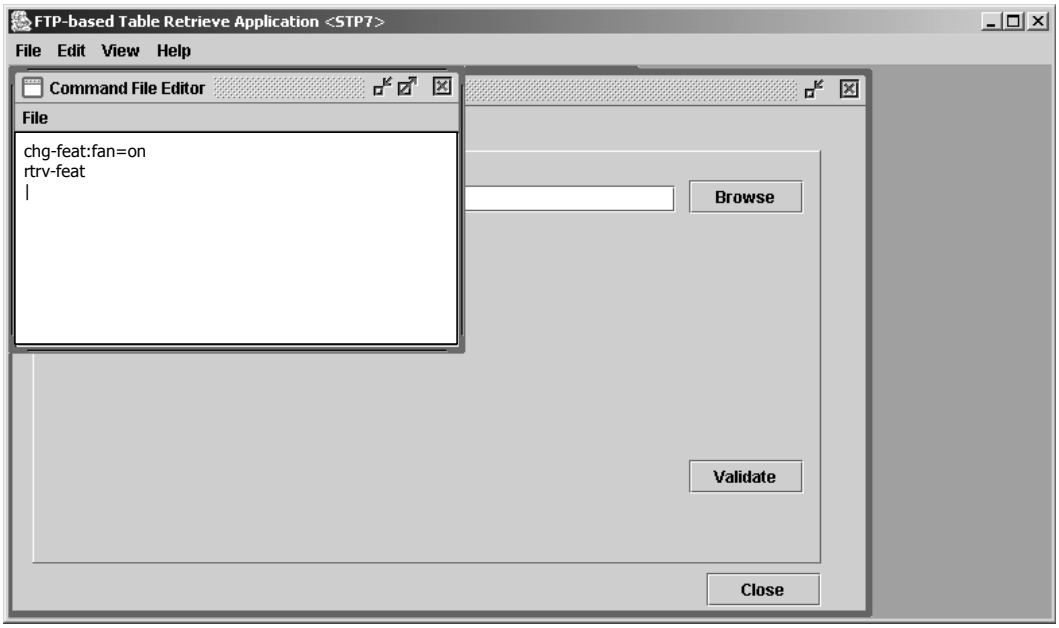
### Stop Without Sending or Editing a Command File

To stop the process without sending or editing a command file, click the **Stop** button in the **Update Validation Complete** window. See Figure 85 on page 83. 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 88.

**Figure 88.** 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.

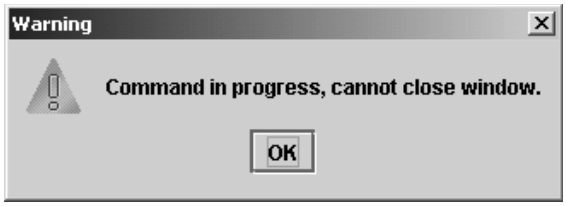
## Procedure

1. Click the **Edit** button in the **Update Validation Complete** window. See Figure 85 on page 83. The **Command File Editor** window opens. See Figure 88 on page 85.

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

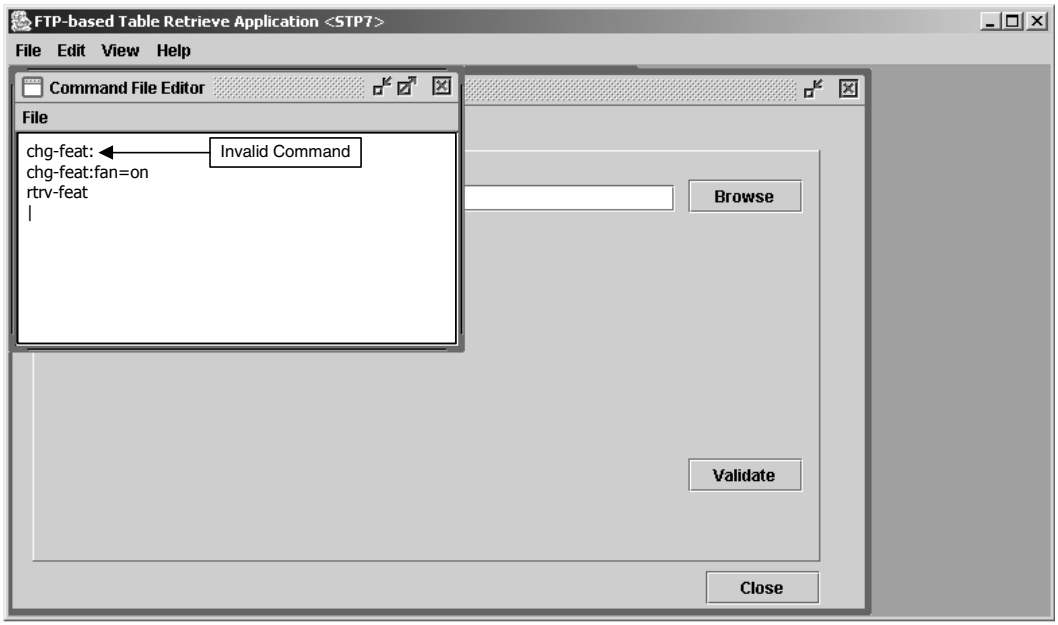
   **NOTE: If an attempt is made to close the Update Tables window while the Command File Editor window is opened, the Command In progress, Cannot Close Window warning message is displayed. See Figure 89.**

   **Figure 89.** Command In progress, Cannot Close Window



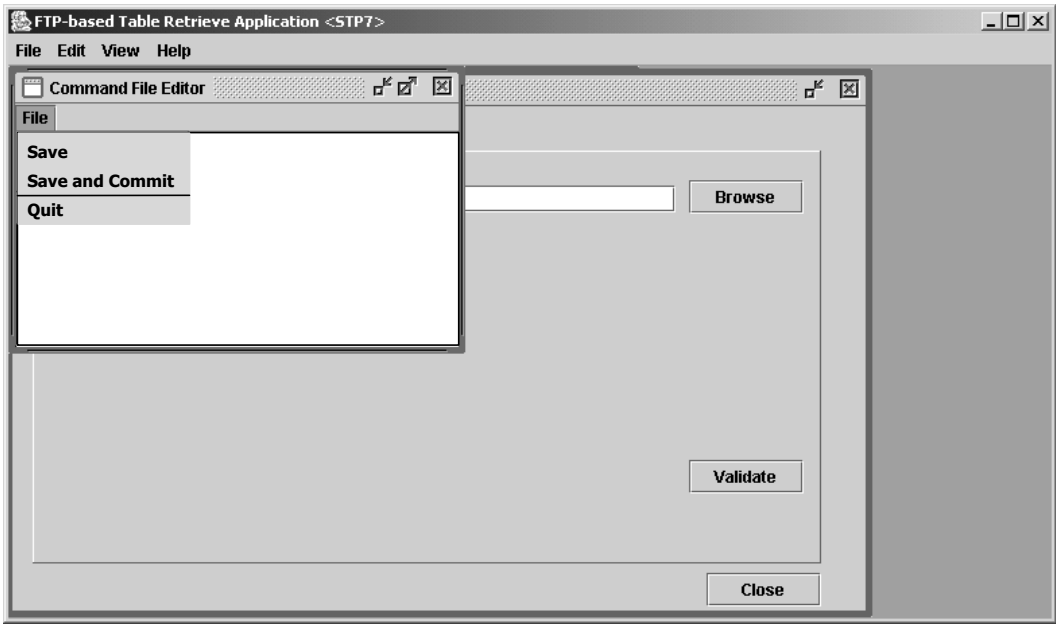

2. Edit the command file. Figure 90 shows a command file with an invalid command. In this example, the invalid command is `chg-feat:`. This command should be removed from the command file, or have a correct parameter and value added to it.

   **Figure 90.** Command File Editor with Invalid Command



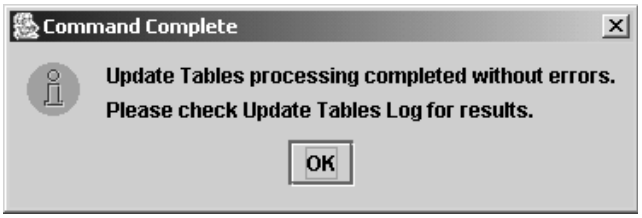
3. When the editing is complete, perform one of these steps.
   a. Select **File > Save** from the **Command File Editor** window (see Figure 91). The command file is saved and the **Command File Editor** window remains open. The command file is not sent to the selected STP. The command file can be validated again in the **Update Tables** window.

**Figure 91.** File Menu in the Command File Editor Window




   b. Select **File > Save and Commit** from the **Command File Editor** window (see Figure 91). 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 92. The command file is sent to the selected STP. The Update Tables Log contains the commit processing events. See Figure 93 on page 88

**Figure 92.** Command Complete Window




   c. Select **File > Quit** from the **Command File Editor** window (see Figure 91). 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 83 on page 82) 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 93, Figure 94 on page 89, Figure 95 on page 90, and Figure 96 on page 91 for the **Update Tables Log** window examples.

**Figure 93.** Update Tables Log Window after the Commit Command Completed

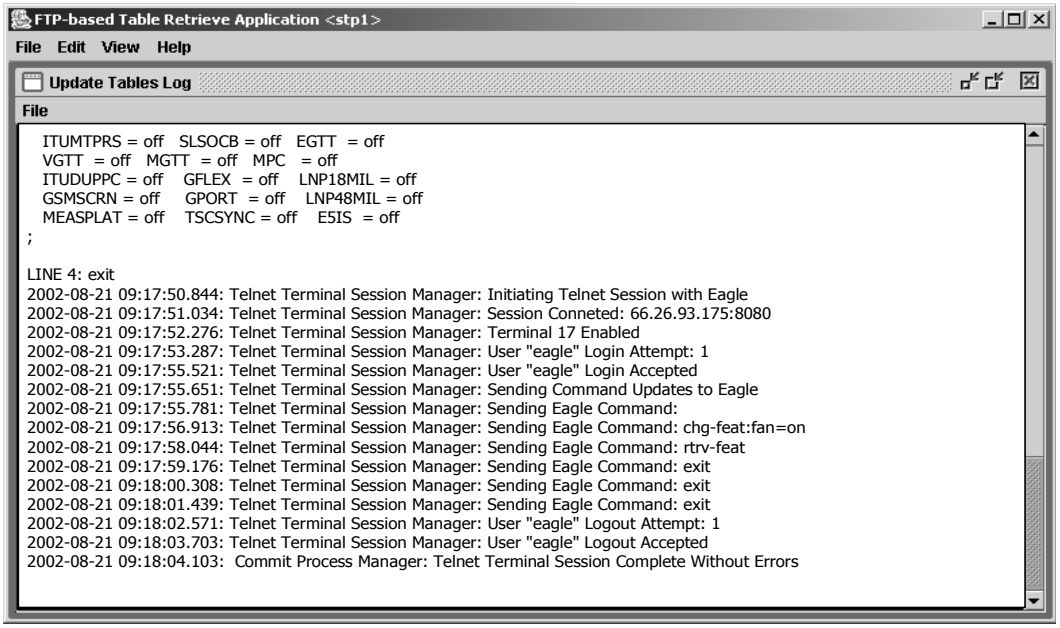


**Figure 94.** Update Tables Log

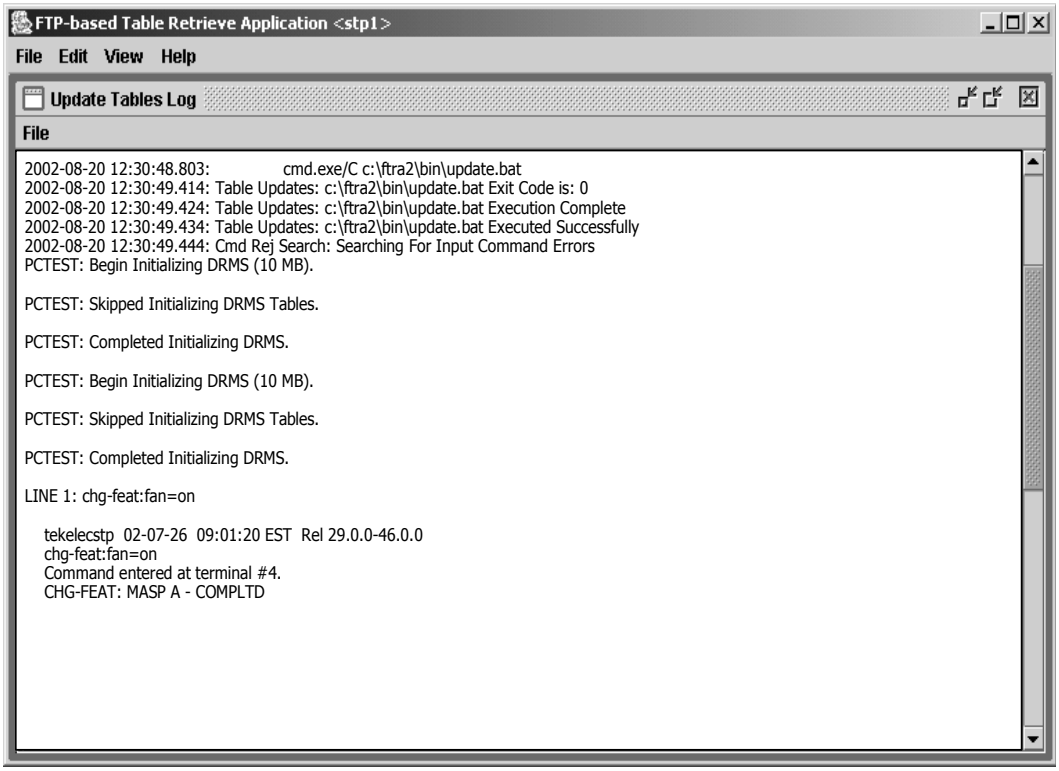


**Figure 95.** Update Tables Log with Stop on Error Box Checked in the Update Tables Window

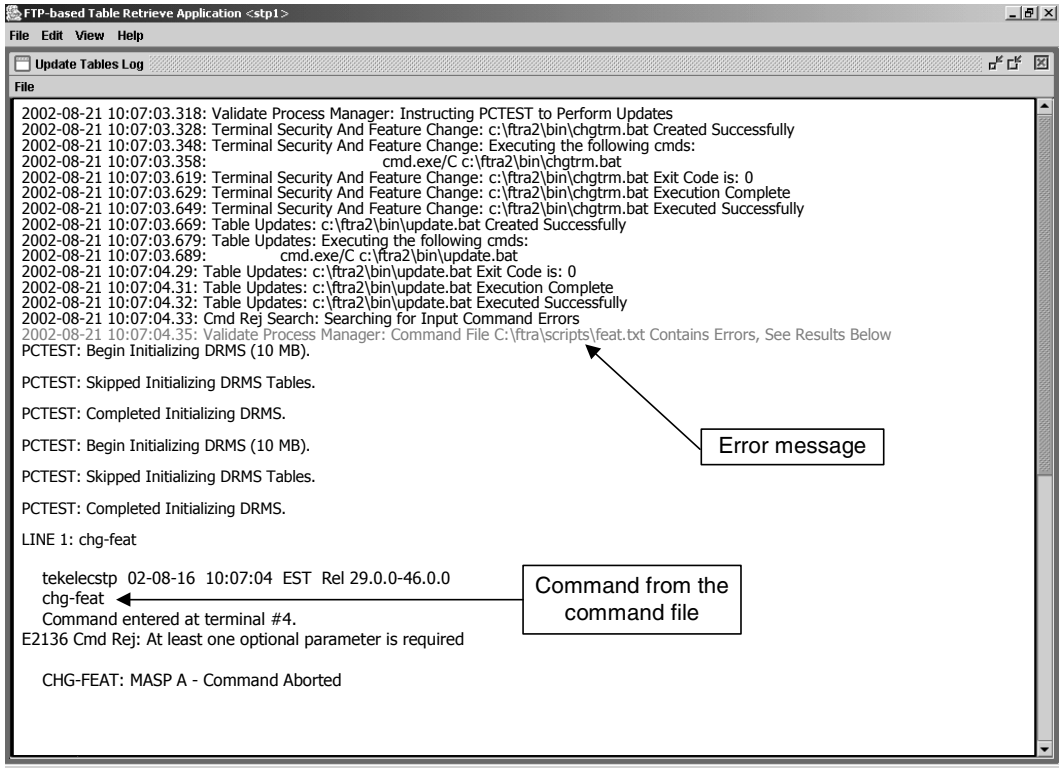


**Figure 96.** Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window

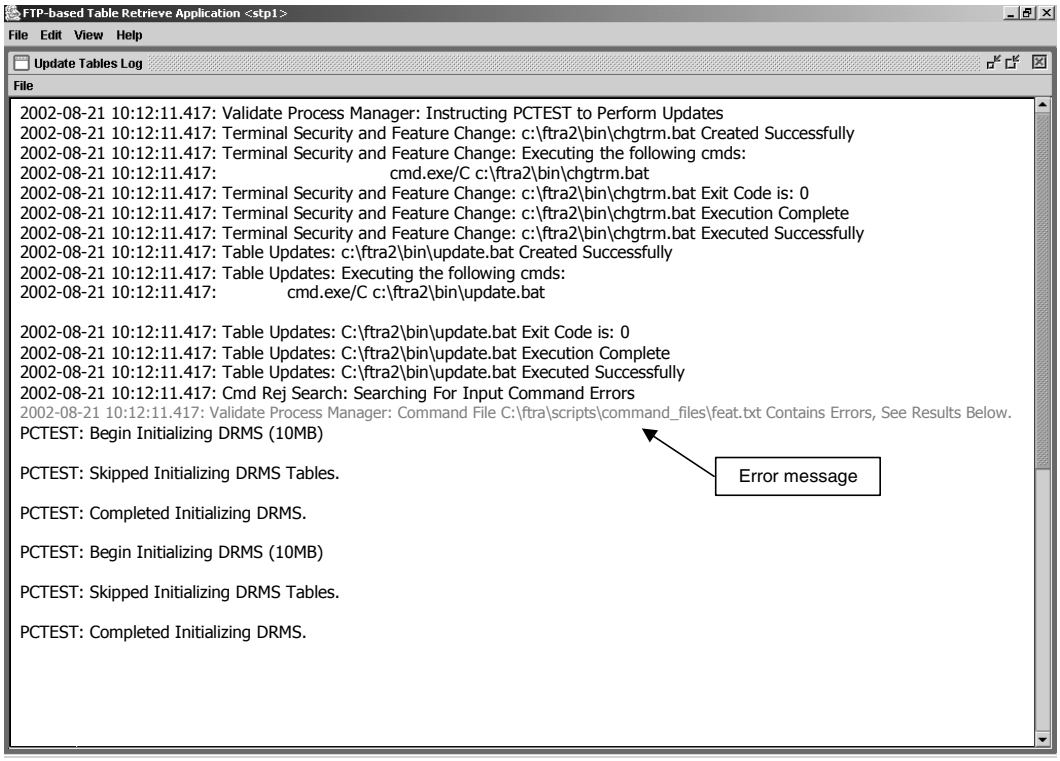
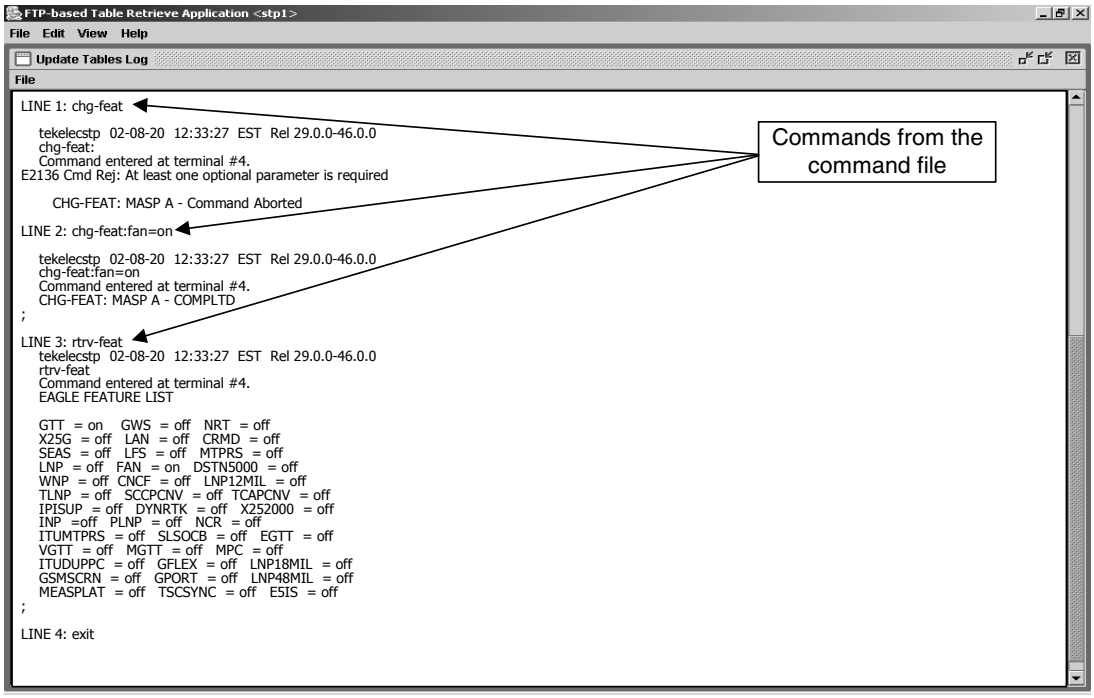



Figure 90 on page 86 shows an example of a command file that produced the error shown in Figure 96.

**Figure 96.** Update Tables Log with Stop on Error Box NOT Checked Error in the Update Tables Window (Continued)

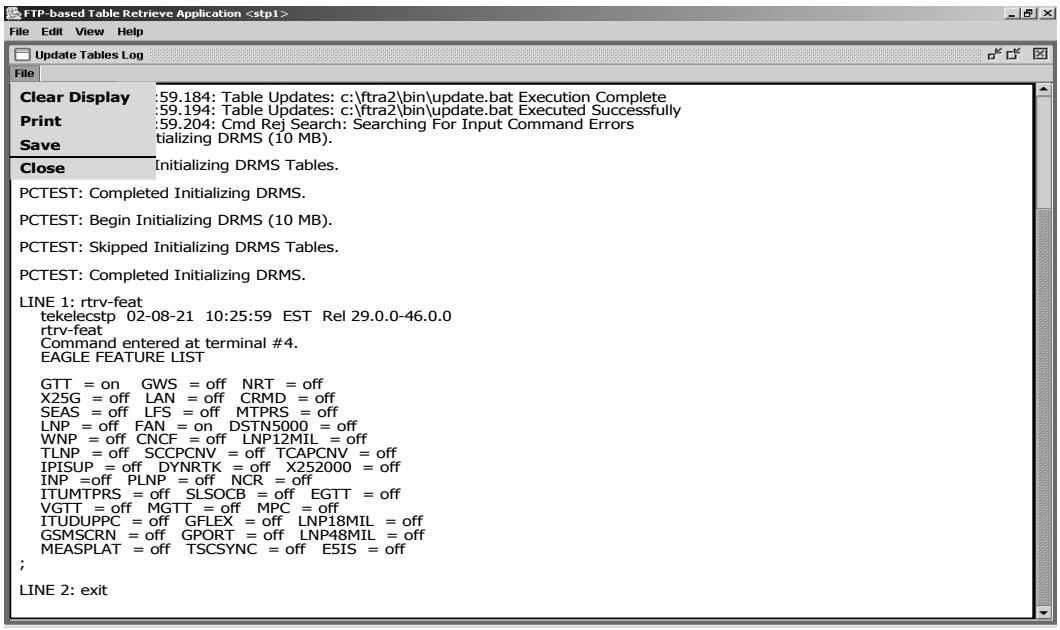



### File Menu in the Update Tables Log Window

The **File** menu in the **Update Tables Log** window, shown in Figure 97 on page 93, 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 97.** 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 97.

2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 98. The **Update Tables Log** window opens.

**Figure 98.** 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

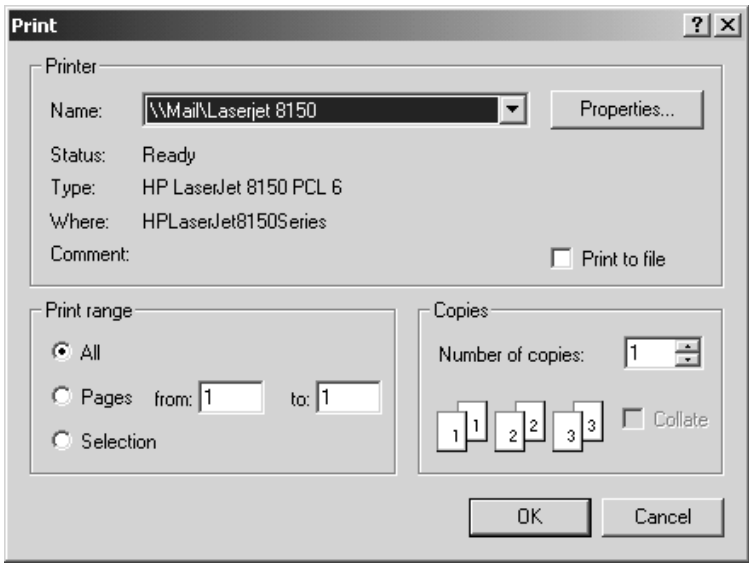
**NOTE: Perform either step 1 or steps 2 and 3.**

1. Select **File > Print** from the **Update Tables Log** window. See Figure 97 on page 93.

2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 98 on page 93. The Update Tables Log opens.

3. Select **File > Print** from the **Update Tables Log** window. The **Print** window opens. See Figure 99.

**Figure 99.** 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

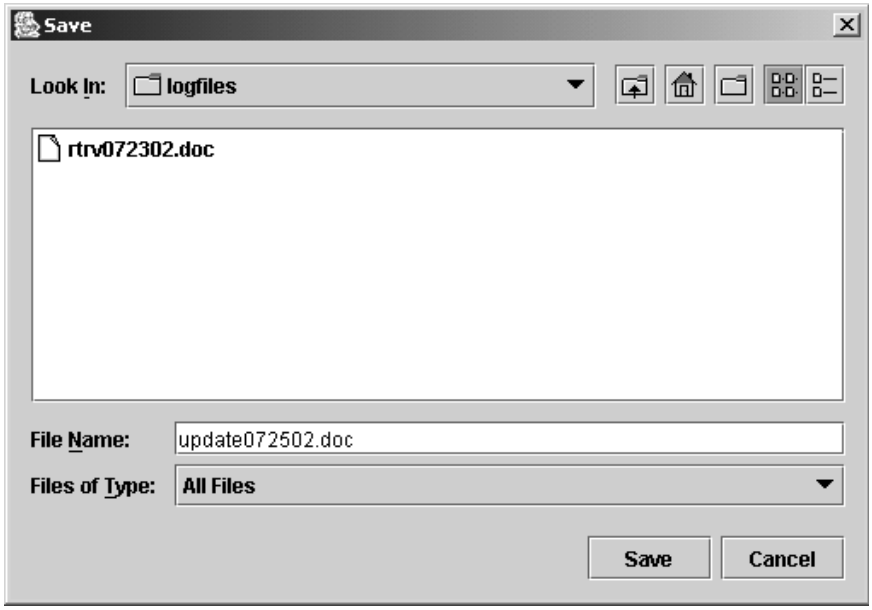
**NOTE: Perform either step 1 or steps 2 and 3.**

1. Select **File > Save** from the **Update Tables Log** window. See Figure 97 on page 93.

2. Select **View > Update Tables Log** in the **FTP-based Table Retrieve Application** window. See Figure 98 on page 93. The Update Tables Log opens.

3. Select **File > Save** in the **Update Tables Log** window. The **Save** window opens. See Figure 100.

**Figure 100.** Save Window

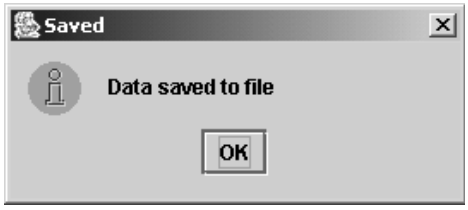


4. Select a location for the file, and enter the file name and file type (with either the .doc or .txt extensions).

   **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 101. Click **OK**, to continue.

   **Figure 101.** 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

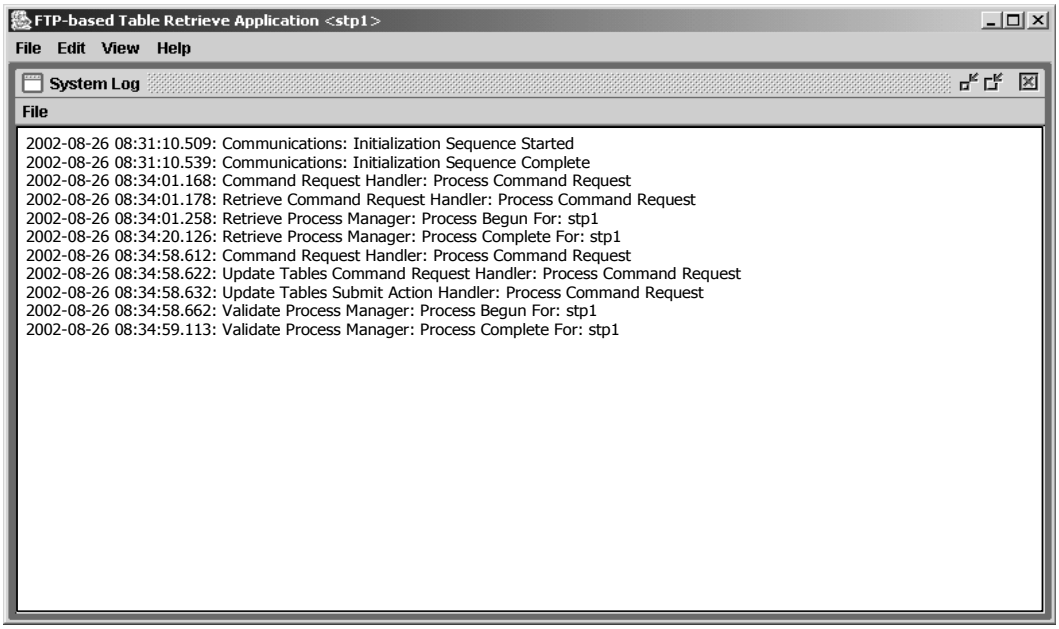
#### Procedure

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 97 on page 93. 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 102.

**Figure 102.** System Log Window

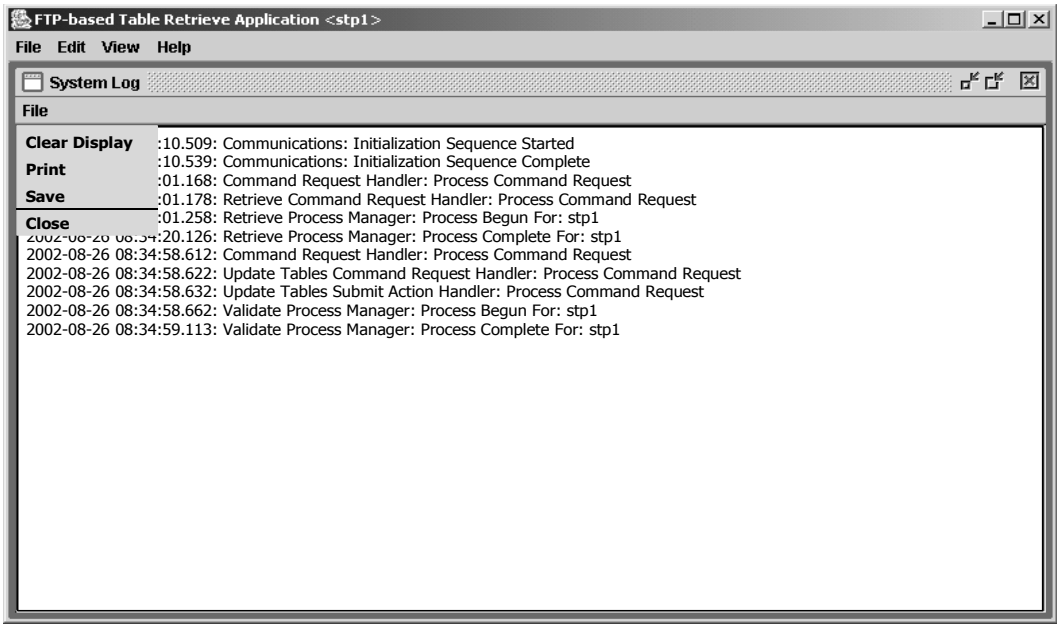



### File Menu in the System Log Window

The **File** menu in the **System Log** window, shown in Figure 103 on page 98, 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 103.** 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 104. The **System Log** window opens.

   **Figure 104.** View Menu


2. Select **File > Clear Display** in the **System Log** window. See Figure 103. The System Log display clears.

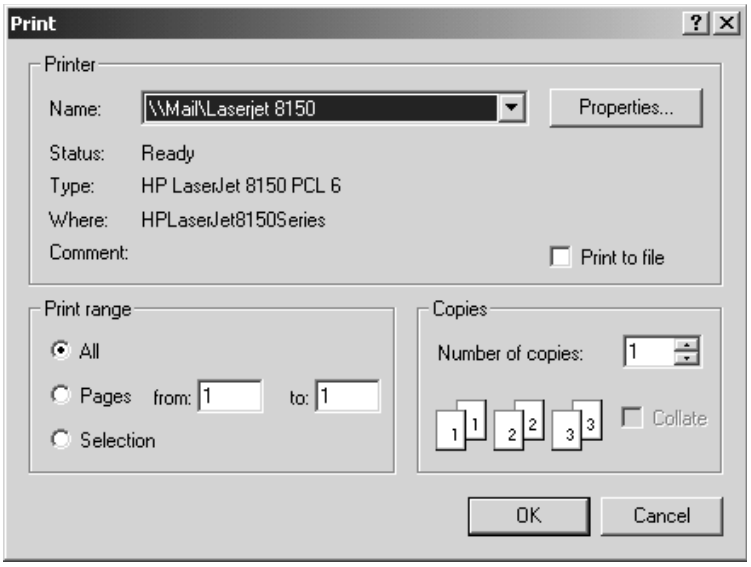
### Printing the System Log

#### Procedure

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 104 on page 98. The **System Log** window opens.

2. Select **File > Print** in the **System Log** window. The **Print** window opens. See Figure 105.

   **Figure 105.** 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.

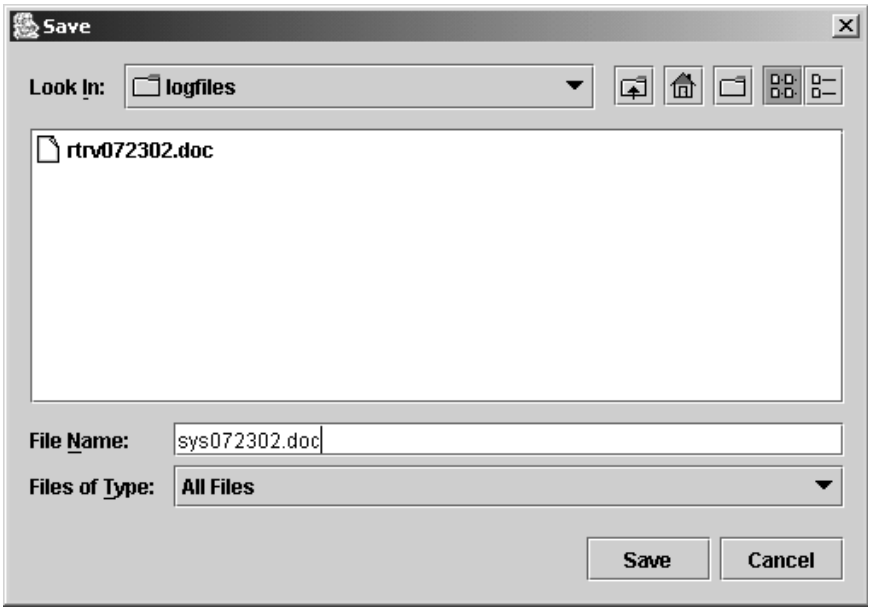
### Saving the System Log to a File

**Procedure**

1. Select **View > System Log** in the **FTP-based Table Retrieve Application** window. See Figure 104 on page 98. The System Log opens.

2. Select **File > Save** in the **System Log** window. The **Save** window opens. See Figure 106.

   **Figure 106.** 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 107. Click **OK** to continue.

**Figure 107.** 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.

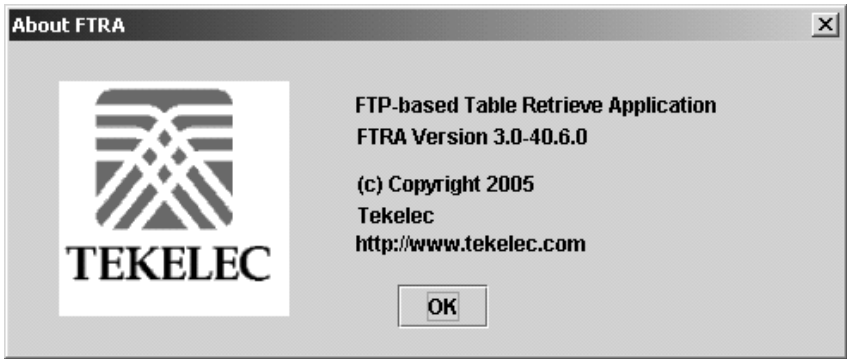
## About FTRA Window

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 108.

**Figure 108.** Help Menu


The **About FTRA** window opens. See Figure 109. Click **OK**, to continue.

**Figure 109.** Typical About FTRA Window



## SSH/SFTP Error Codes

Table 9 and Table 10 on page 116 contain a list of the error codes that can be generated when making a secure connection bewteen the FTRA, version 2.0 or greater, and the Eagle. Each error code contains a brief description of the error and the suggested recovery action.

This section also contains procedures, following Tables 9 and 10, for testing connectivity and network problems, and to verify that the setup for making secure connections is correct.

If secure connections to the Eagle 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 before performing any of the actions in Tables 9 and 10. 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 9 or Table 10 on page 116 are encountered after the recovery procedure is verified, contact Tekelec Technical Services. See page 3 for the contact information.

**Table 9.** 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 43 on page 50). |
| 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 119 and the "Connectivity Test - II" section on page 120). 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 9.** 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 15) 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 Tekelec Technical Services immediately. See page 3 for the contact information. |
| 596 | The file name is already specified. | Report this issue to Tekelec Technical Services immediately. (Internal SFTP implementation error). See page 3 for the contact information. |
| **SFTP Client Errors** | | |
| 597 | SFTP client packet send failure | Peform these tests:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 598 | The SFTP connection is closed. | |
| 599 | SFTP packet read failure | |

**Table 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 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 121. If the error persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 601 | Undefined | Notify Tekelec Technical Services. See page 3 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 121. If the error persists, report the issue to Tekelec Technical Services. See page 3 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 121. |

**Table 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 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 43 on page 50) is accessible and re-try the connection. |
| 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 121. |
| 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 Tekelec Technical Services immediately. See page 3 for the contact information. |

**Table 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| **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 Tekelec Technical Services immediately. See page 3 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. | |
| 625 | Failure to read the client configuration file. | Report this issue to Tekelec Technical Services immediately. See page 3 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 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. | |

**Table 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 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 is compatible with **openSSH 3.0.2p1**. | Report the issue to Tekelec Technical Services if the problem persists after the SSHD configuration file is verified. See page 3 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 Tekelec Technical Services. See page 3 for the contact information. |
| 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 640 | A bad message was received during the SSH authentication. | |

**Table 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 641 | Missing authentication context, encountered during the SSH user authorization. | Report this issue to Tekelec Technical Services immediately. See page 3 for the contact information. |
| 642 | Failure during the public key read/verification operation. | |
| 643 | Undefined SFTP/SSH error. | |
| 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 645 | A bad option was specified in the SSH client on the Eagle. | |
| 646 | An unsupported escape character was used in the SSH client on the Eagle. | |
| 647 | An unsupported cipher type was used in the SSH client on the Eagle. | Report this issue to Tekelec Technical Services immediately. See page 3 for the contact information. |

**Table 9.** 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. | Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 649 | A bad port was used in the SSH client on the Eagle. | Report this issue to Tekelec Technical Services immediately. See page 3 for the contact information. |
| 656 | Bad forwarding was used in the SSH client on the Eagle. | |
| 657 | Bad forwarding ports were specified in the SSH client on the Eagle. | |
| 658 | A bad dynamic port was specified in the SSH client on the Eagle. | |

**Table 9.** 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. | Verify that the SFTP/SSHD version is compatible with **openSSH 3.0.2p1**. Verify there is no network outage by performing these tests:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 660 | An invalid option or argument was specified in the SSH client on the Eagle. | Report this issue to Tekelec Technical Services immediately. See page 3 for the contact information. |
| 661 | The hostname was not specified in the SSH client on the Eagle. | |
| 663 | The SSH client was unable to load the cipher type on the Eagle. | |
| 664 | Asynchronous IO is not supported on IPSM, SSH client error. | |
| 665 | Compression is already enabled in the SSH client on the Eagle. | |
| 666 | Unknown cipher number on the SSH client on the Eagle. | |
| 667 | The SSH client key length is invalid. | |

**Table 9.** 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. | Report this issue to Tekelec Technical Services immediately. See page 3 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 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 Tekelec Technical Services. See page 3 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 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 674 | The SSH/SFTP client on the Eagle 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 675 | Corrupted check bytes were detected on the SSH/SFTP client on the Eagle. | |
| 676 | Corrupted MAC on input was detected by the SSH/SFTP client on the Eagle. | Verify that the **`sshtools.xml`** file provided with FTRA software has the field as shown:<br><!-- The Message Authentication Code configuration, add or overide default mac implementations --><br><MacConfiguration><br><DefaultAlgorithm>hmac-md5</DefaultAlgorithm><br></MacConfiguration> |
| 677 | Corrupted pad on input was detected by the SSH/SFTP client on the Eagle. | Report this issue to Tekelec Technical Services immediately. See page 3 for the contact information. |
| 678 | SSH/SFTP tried to close a connection that is already closed. | |

**Table 9.** FTP/SFTP/SSH Error Codes (Continued)

| SFTP/SSH Generic Network Client Error Code | Description | Action/Recovery |
|---|---|---|
| 679 | The SSH/SFTP client on the Eagle 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 680 | SSH/SFTP tried to set the packet size twice. | Report this issue to Tekelec Technical Services immediately. See page 3 for the contact information. |
| 681 | A bad packet size was detected by the SSH/SFTP client on the Eagle. | |

**Table 9.** 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:<br>• "FTP Server Verification" on page 119<br>• "SFTP /SSHD Server Verification" on page 119<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 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 10.** 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 using the `rtrv-ftp-serv` command, and re-try the connection |
| 41 | Protocol wrong type for socket | Report this issue to Tekelec Technical Services. See page 3 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:<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 52 | The network dropped the connection on reset. | |
| 53 | Software caused the connection to abort. | Report this issue to Tekelec Technical Services. See page 3 for the contact information. |

**Table 10.** 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:<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 for the contact information. |
| 55 | No buffer space available. | Report this issue to Tekelec Technical Services. See page 3 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.<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120 |
| 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 119. |

**Table 10.** 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:<br>• "Connectivity Test – I" on page 119<br>• "Connectivity Test - II" on page 120<br>• "Network Outage Trouble Shooting" on page 121.<br>Make any fixes necessary and retry the connection.<br>If the problem persists, report the issue to Tekelec Technical Services. See page 3 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 Tekelec Technical Services. See page 3 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 43 on page 50).

**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 43 on page 50).

**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 43 on page 50).

**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 and the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 50).

On an Eagle 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 15), and **yy.yy.yy.yy** is the IP address of the FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 50).

**Expected Result:**

**NOTE: The RTT time and data sizes may vary.**

```
> pass:loc=xxxx:cmd="ping yy.yy.yy.yy"
Command Accepted - Processing
    e1110501 13-03-31 13:57:59 GMT  EAGLE5 30.2.0-50.8.0
    pass:loc=xxxx:cmd="ping yy.yy.yy.yy"
    Command entered at terminal #5.
;
    e1110501 13-03-31 13:57:59 GMT  EAGLE5 30.2.0-50.8.0
    PASS: Command sent to card
;
    e1110501 13-03-31 13:57:59 GMT  EAGLE5 30.2.0-50.8.0
    PING command in progress
;
    e1110501 13-03-31 13:57:59 GMT  EAGLE5 30.2.0-50.8.0
;
    e1110501 13-03-31 13:58:01 GMT  EAGLE5 30.2.0-50.8.0
    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 and FTP/SFTP server shown in the **FTP Server Configuration Menu** window (see Figure 43 on page 50).

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 shown in the **STP Connection Configuration Menu** window (see Table 2 on page 15).

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, enter the **`pass:loc=xxxx:cmd="netstat -p tcp"`** command at the Eagle 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 15), 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
    e1110501 13-03-31 19:32:52 GMT  EAGLE5 30.2.0-50.8.0
    pass:loc=3102:cmd="netstat -p tcp"
    Command entered at terminal #5.
;
    e1110501 13-03-31 19:32:52 GMT  EAGLE5 30.2.0-50.8.0
    PASS: Command sent to card
;
    e1110501 13-03-31 19:32:52 GMT  EAGLE5 30.2.0-50.8.0
    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

;

    e1110501 13-03-31 19:32:52 GMT  EAGLE5 30.2.0-50.8.0

    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 11, fix the network problems and retry the connection.

**Table 11.** 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



## Numerics

## A

## B

## C

## D



## E

## F

## G



## H



## I

## J



## K



## L



## M



## N

## S

## T

## U



## V

## W