RTTP

Server-side RTTP Logging

Contents

1 Introduction

This document describes the server-side logging of RTTP messages between the Liberator and a client communicating over RTTP.

1.1 Readership

This document is intended for system administrators, testers, and developers.

1.2 Related documents

[1] **Liberator Administration Guide**

Contains instructions on how to install and configure Caplin Liberator.

1.3 Acknowledgments

None.

2 Server-side RTTP logging

The server-side RTTP logging feature allows you to record conversations between a Liberator and its users. The logging feature is enabled for individual users, and produces a continuously updated log file for every new session between the Liberator and the user.

Note: It is recommended that in a live system you only turn on RTTP traffic logging for troubleshooting purposes.

To set up RTTP logging:

- First configure Liberator to log the RTTP protocol traffic between clients and the Liberator.

  Do this by defining the naming convention for the log files – see section 2.1. Then specify a list of user names (Liberator login names) whose RTTP traffic is to be logged.

  You can do this in two ways:

  - Through Liberator configuration, as detailed in section 2.3.

    or

  - If JMX monitoring is enabled for the Liberator, dynamically through the Users or Logs tab on the Enterprise Management Console (EMC), as shown in section 2.2.

Tip: By default, the RTTP log files are generated in Liberator's *var/rttp* directory.

2.1 Defining the RTTP log file names

Define the names of the traffic log files by setting the **rttp-log** entry of the Liberator Configuration file *rttpd.conf*.

Example:

```
rttp-log rttp/RTTP_TRAFFIC_%l.%i
```

`%l` is the user name and `%i` is the RTTP session id. So in this case the name of the RTTP traffic log for user JSmith's session would typically be *rttp/RTTP_TRAFFIC_JSmith.0x-ab-9*

It is strongly recommended that the name of the RTTP traffic log file contains at least the user name and RTTP session id markers (`%l` and `%i`), so that a separate log file is generated for each session for each user who has RTTP logging enabled. If these markers are absent, the log entries for all RTTP sessions will be mixed together in the same file, making it difficult to determine which messages came from which sessions and users.

For reference information on the **rttp-log** Liberator configuration entry, see the **Liberator Administration Guide**.

2.2 Configuring user RTTP logging using the EMC

The Enterprise Management Console's Session tab allows you to switch RTTP traffic logging on and off for existing user sessions. You can also enable logging permanently for any user known to the Liberator; each time the user logs in to Liberator their RTTP session will be logged.

To enable RTTP session logging for a user who is logged in to Liberator

Note: Use this EMC facility with caution in live systems as it enables RTTP logging for all the user's subsequent sessions until you turn the logging off.
If RTTP logging is enabled for many users it can adversely affect performance.

- Within the Users tab, right click on the row detailing the user and select the option 'Start RTTP Session Logging'.

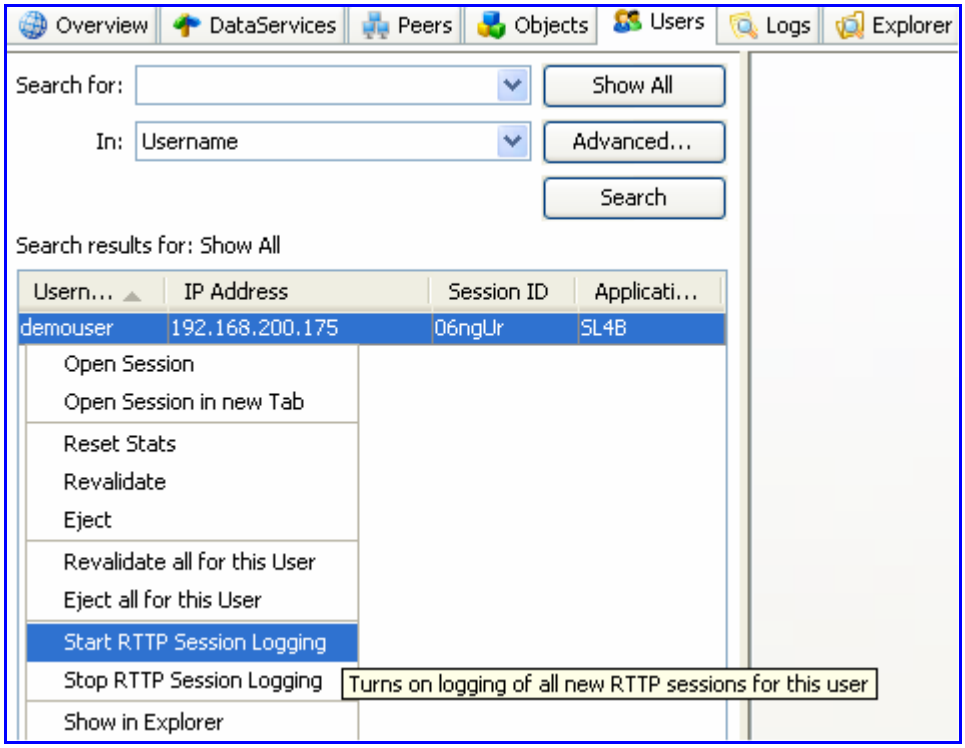
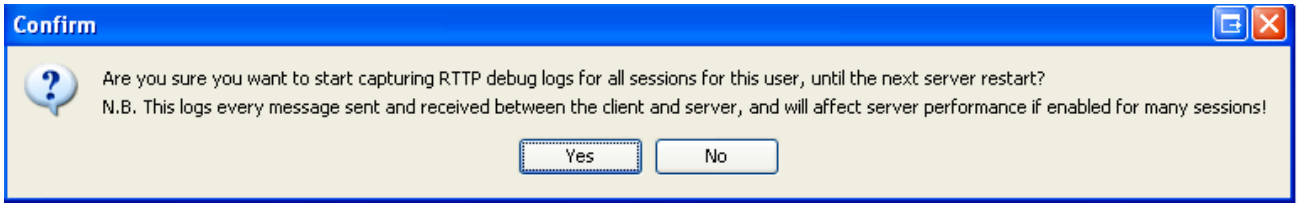


Figure 1 – Starting RTTP Logging for a logged in user

- Click Yes on the dialog box that pops up.



Logging of the user's RTTP traffic will start when the user next logs in to the Liberator. (The user's current session is not logged.)

Subsequently, every time the user logs in to Liberator their RTTP traffic is logged until you explicitly disable logging (see "To disable RTTP session logging for a user who is logged in to Liberator" on page 7 and "To disable RTTP session logging for any Liberator user " on page 10).

To disable RTTP session logging for a user who is logged in to Liberator

- Within the Users tab, right click on the row detailing the user and select the option 'Stop RTTP Session Logging'.

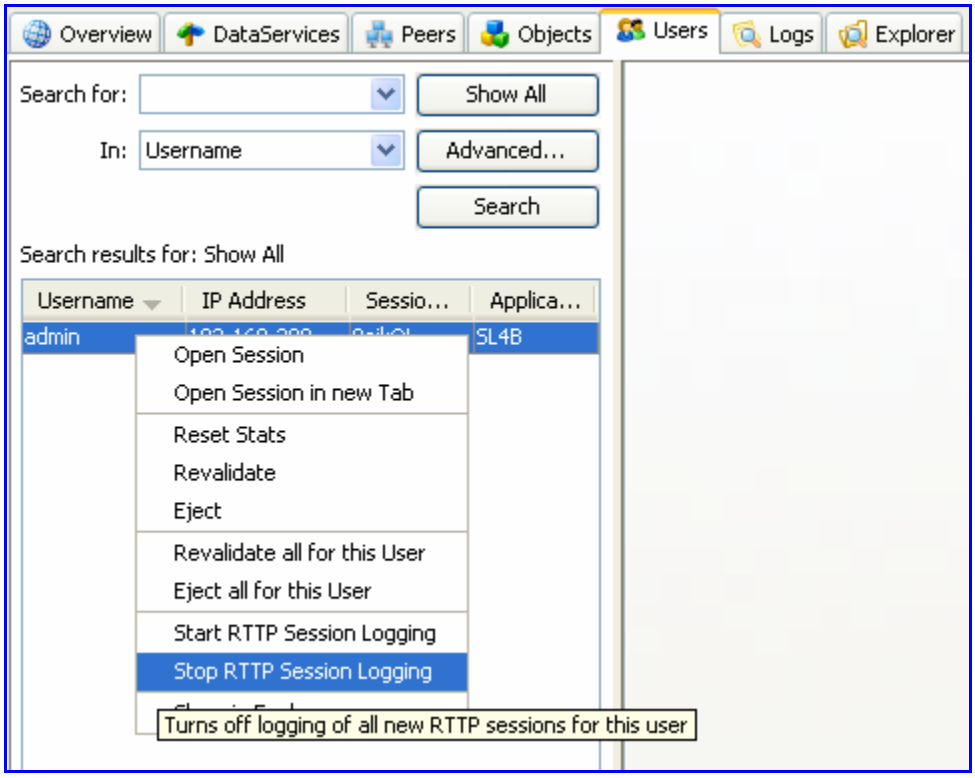


Figure 2 – Stopping RTTP Logging for a logged in user

To enable RTTP session logging for any Liberator user

The following instructions allow you to enable RTTP session logging for a user even if they are not logged in to the Liberator.

Note: Use this EMC facility with caution in live systems, as it enables RTTP logging for all the user's subsequent sessions until you turn the logging off.
If RTTP logging is enabled for many users it can adversely affect performance.

- Go to the Logs tab and enter the name of the user in the box headed 'Log Sessions For Another User'.

  The user name must be a valid Liberator login name.

  Click the Add button.

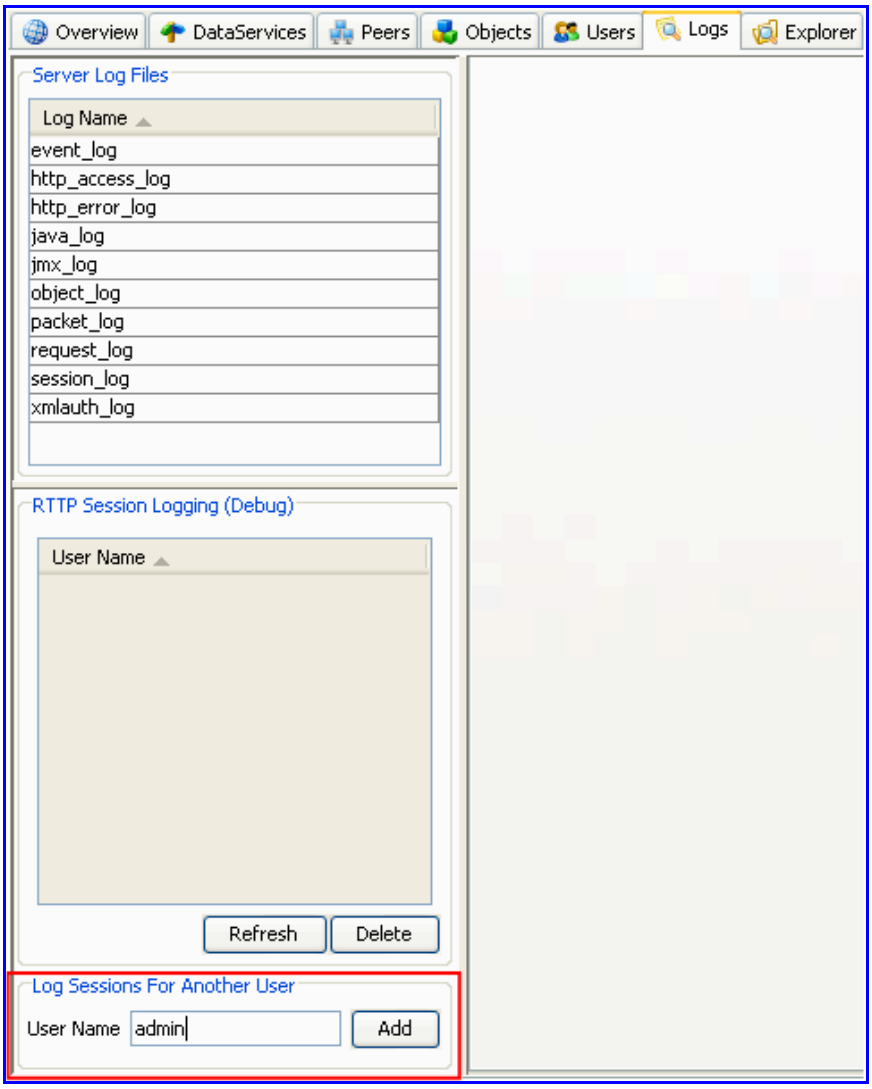
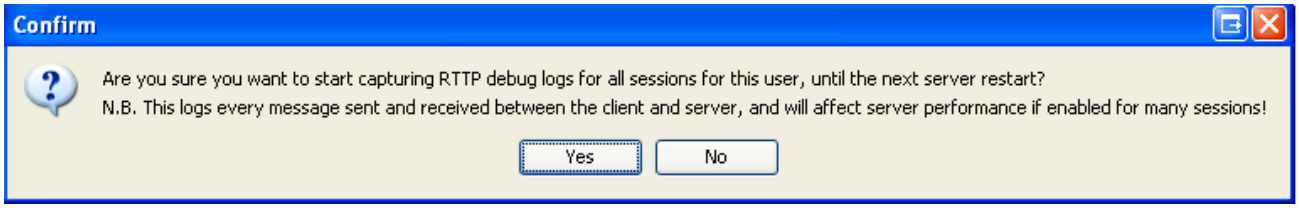


Figure 3 – Starting RTTP session logging for a named user

- Click Yes on the dialog box that pops up.



Subsequently, every time the user logs in to Liberator their RTTP traffic is logged until you explicitly disable logging (see “To disable RTTP session logging for a user who is logged in to Liberator” on page 7 and “To disable RTTP session logging for any Liberator user ” on page 10).

To disable RTTP session logging for any Liberator user

- Go to the Logs tab and select the required user from the list headed 'RTTP Session Logging (Debug)'.
- Click the Delete button.

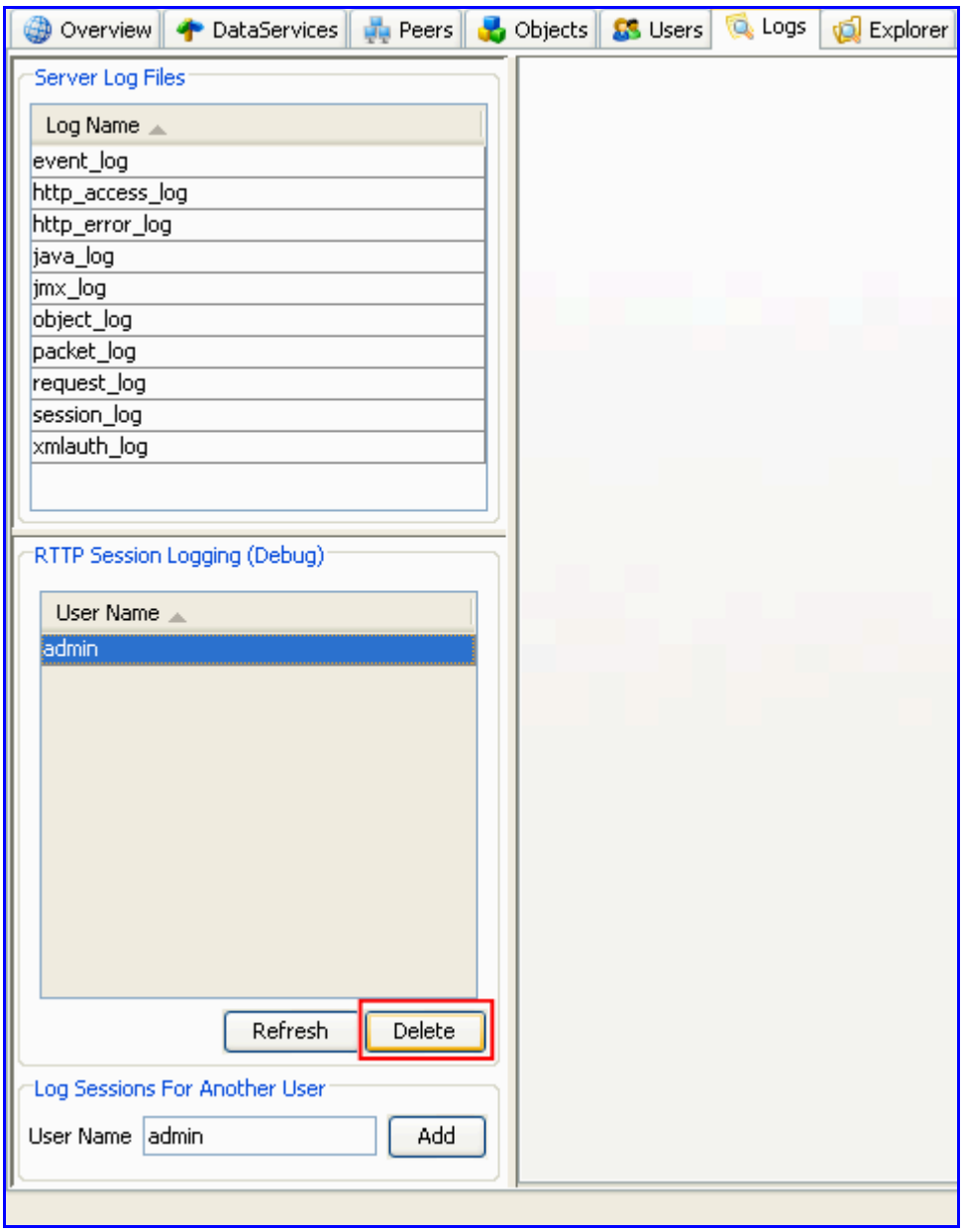
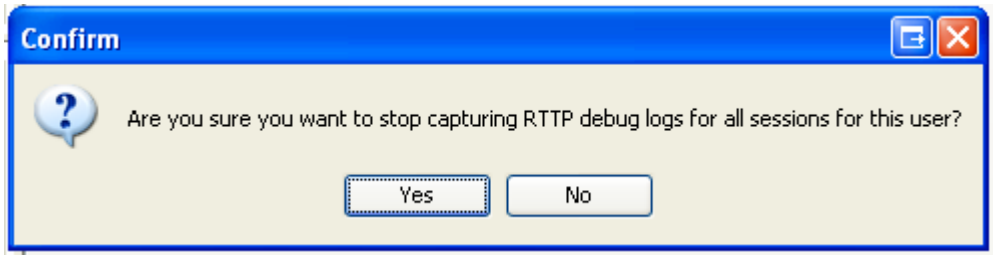


Figure 4 – Stopping RTTP session logging for a named user

- Click Yes on the dialog box that pops up.



2.3 Configuring User RTTP Logging from the Liberator

You can turn on traffic logging for individual users by setting the Liberator configuration option **rttp-log-users** in the Liberator configuration file (*rttpd.conf*).

Note: This option should only be used for debugging test installations.
It permanently enables traffic logging for the specified users. Logging can only be turned off by stopping the Liberator and changing the **rttp-log-users** configuration option.
In a live system you should normally turn RTTP logging on and off using the Enterprise Management Console (see section 2.2).

If the **rttp-log-users** configuration entry is absent or empty, only RTTP traffic logs that have been specified using the Enterprise Management Console will be generated

The user names can be defined as a space separated list, or as individual entries, or a combination of the two.

Examples:

```
rttp-log-users Alf Bill Carl
```

or

```
rttp-log-users Alf
rttp-log-users Bill
rttp-log-users Carl
```

Note: To ensure the RTTP session logs are created, check that the Liberator's *var* directory contains a directory called *rttp*

For reference information on **rttp-log-users**, see the **Liberator Administration Guide**.

2.4 Interpreting server-side RTTP Logs

Separation of log traffic in log files

The default log file naming convention causes an RTTP traffic log file to be generated for each combination of user and RTTP session, so if a user has more than one session established concurrently you can easily analyze the traffic for the individual sessions.

RTTP traffic log format

RTTP traffic log entries have the format:

>>>TIMESTAMP
<RTTP message as text>>

or

<<<TIMESTAMP
<RTTP message as text>>

where:

- **>>>** indicates that the RTTP message has been sent *from the Liberator* to the client
- **<<<** indicates that the RTTP message has been sent *to the Liberator* from the client
- ***TIMESTAMP*** has the format ***dd_mon hh:mm:ss.ss*** (for example 23_Aug 15:22:14.07)

Example 1

The following log is for an RTTP type 5 (Streaming JavaScript) connection, established using StreamLink for Browsers on the client. It shows a "NOOP+OK" being sent by a Liberator. During periods of inactivity, clients regularly send "NOOP" messages to the server. The server responds by sending "NOOP+OK" messages back to clients (if the server is available). This is reminiscent of 'pinging' a server, and receiving "reply" messages back indicating that the server is up and running.

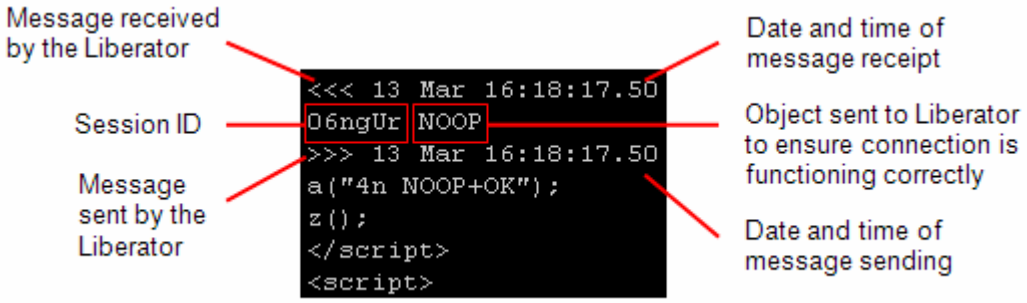


Figure 5 – Sample Log for an RTTP type 5 connection

Example 2

The following log is for an RTTP type 2 (HTTP Tunneled) connection, established using StreamLink for Java on the client. The client has requested one object from the Liberator – "/DEMO/MSFT"

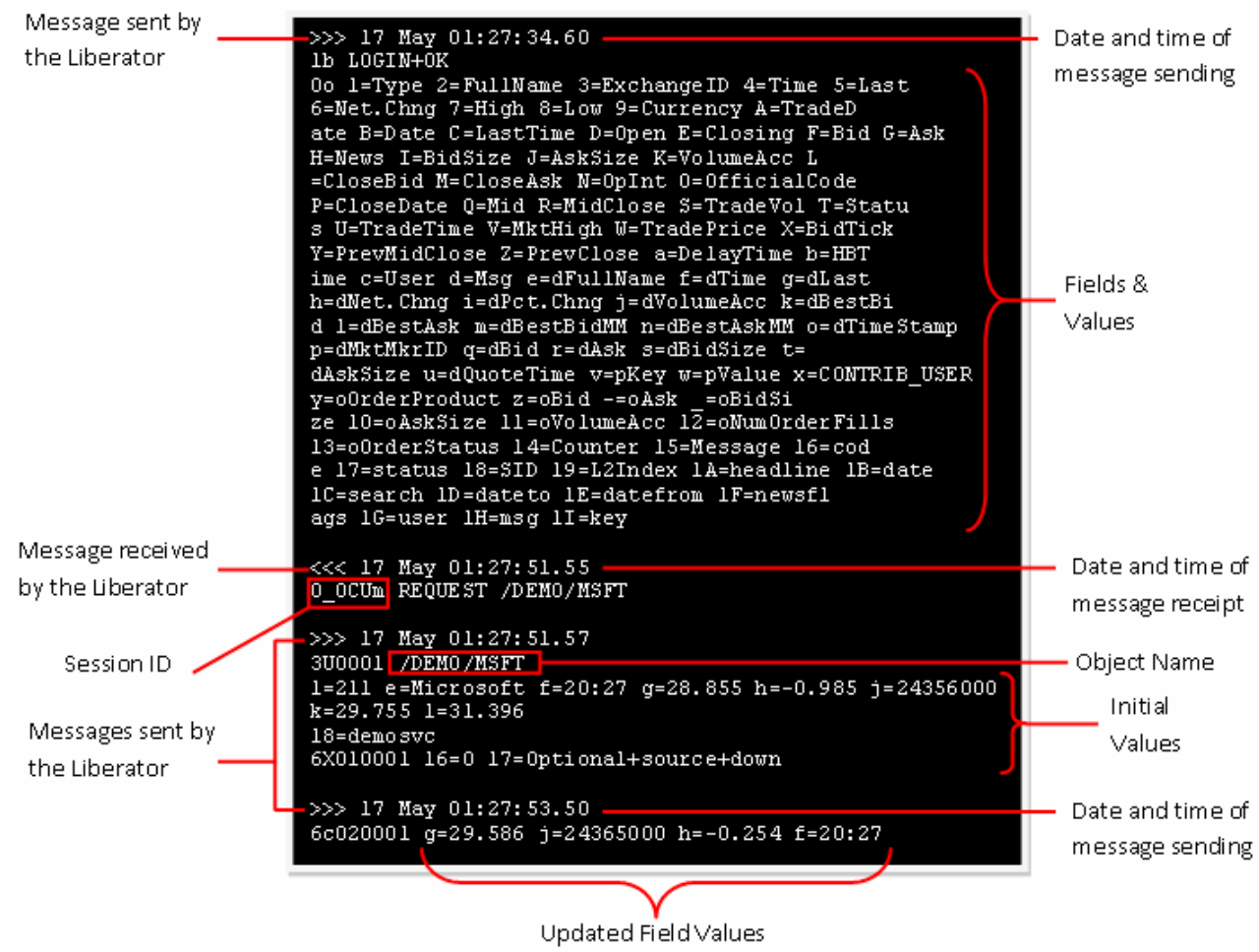


Figure 6 – Sample Log for an RTTP type 2 connection

Contact Us

Caplin Systems Ltd.

Triton Court
14 Finsbury Square
London EC2A 1BR
UK

Telephone: +44 20 7826 9600

Fax: +44 20 7826 9610

www.caplin.com